

EXIGÊNCIAS DO CITI PARA FORNECEDORES

PROPRIETÁRIOS:
Head of Citi Procurement & Risk

DATA DA EMISSÃO:
Janeiro de 2015

REVISADO:
Setembro de 2026

VERSÃO:
9

ÍNDICE

1	VISÃO GERAL.....	3
2	OPORTUNIDADES IGUAIS DE EMPREGO.....	5
3	ANTI-SUBORNO E CORRUPÇÃO (AB&C)	6
4	PRESENTES E ENTRETENIMENTO.....	6
5	ENGAJAMENTO DE FORNECEDORES E PRINCÍPIOS DE FORNECEDORES.....	7
6	PROIBIÇÃO DE ESCRAVIDÃO MODERNA	7
7	PESSOAL DO FORNECEDOR	9
8	GESTÃO DE FRAUDES.....	11
9	INTERAÇÃO COM A MÍDIA E APARIÇÕES PÚBLICAS	13
10	COMUNICAÇÕES ELETRÔNICAS ESCRITAS	13
11	ATIVIDADES E CONTRIBUIÇÕES POLÍTICAS	14
12	ANTILAVAGEM DE DINHEIRO (“AML”)	14
13	GESTÃO DE REGISTROS	16
14	RESILIÊNCIA EMPRESARIAL/CONTINUIDADE DE NEGÓCIOS.....	18
15	NORMAS GLOBAIS DE VERIFICAÇÃO DE ANTECEDENTES	24
16	DESPESAS.....	26
17	SEGURANÇA DA INFORMAÇÃO (IS)	27
18	DIRETRIZES DE LOCAL DE TRABALHO SEGURO	66
19	INTELIGÊNCIA ARTIFICIAL/APRENDIZADO DE MÁQUINA (INCLUINDO IA GENERATIVA/IA AGÊNTICA)	67
20	RECLAMAÇÕES DO CLIENTE	68
21	POLÍTICA DE NEGOCIAÇÃO E INVESTIMENTO PESSOAL.....	69
22	NORMAS DE FATURAMENTO E COBRANÇA.....	69
23	POLÍTICA DE AUSÊNCIA OBRIGATÓRIA.....	70
	APÊNDICE – DEFINIÇÕES.....	71

1 VISÃO GERAL

1.1. Exigências Gerais

Estas Exigências do Citi para Fornecedores (“**Exigências**”) detalham algumas das obrigações que os Fornecedores devem cumprir ao fazer negócios com o Citi. Algumas Exigências são aplicáveis a todos os Fornecedores, enquanto a aplicabilidade de outras Exigências a um Fornecedor específico depende dos tipos de produto(s) e serviço(s) que o Fornecedor fornece ao Citi (estes últimos estão resumidos na Seção 1.2 abaixo e são indicados no início de cada disposição listada no documento). Os termos em letras maiúsculas terão os significados atribuídos a cada um deles neste documento, inclusive no Apêndice anexo, a menos que esse significado não seja indicado neste documento, e nesse caso eles terão os significados atribuídos a eles no Contrato, conforme definido abaixo.

Estas Exigências são obrigações contratuais de acordo com os contratos do Fornecedor com o Citi (incluindo, entre outros, documentos da transação, por exemplo, ordens de serviço, cronogramas de licença) (individualmente “**Contrato**”) e são adicionais a quaisquer obrigações especificadas em qualquer Contrato, quaisquer obrigações de acordo com a Lei Aplicável (conforme o termo é definido abaixo), qualquer notificação ao Fornecedor do Citi informando o Fornecedor sobre suas obrigações nos termos dessa notificação (individualmente “**Notificação**”), ou quaisquer exigências adicionais mais específicas implementadas pelos negócios ou funções do Citi. As obrigações e exigências mais restritivas devem ser aplicadas na medida de qualquer conflito entre qualquer uma das exigências anteriores e estas exigências. Os fornecedores devem assumir uma função proativa e consultar o contato de negócios principal (ou pessoa designada) do Citi em relação a qualquer dúvida que tenham sobre estas exigências, incluindo quaisquer alterações, qualquer isenção solicitada ou qualquer conflito percebido neles ou com a Lei Aplicável.

O Fornecedor deve cumprir imediatamente qualquer solicitação razoável que o Citi possa enviar ao Fornecedor para obter dados que o Citi exige relacionados aos Serviços ou Pessoal do Fornecedor em associação com a obrigação do Citi de cumprir a Lei Aplicável. A falha do Fornecedor em cumprir essas obrigações será considerada uma violação relevante dos termos deste Contrato.

O não cumprimento destas Exigências ou de quaisquer exigências adicionais especificadas por uma unidade do Citi com a qual o Fornecedor faz negócios pode resultar na rescisão do Contrato do Fornecedor com o Citi. Além disso, violações das Exigências também podem ser violações da Lei Aplicável e podem resultar em indenizações civis ao Citi (ou terceiros) ou penalidades criminais para o Fornecedor. O Fornecedor não pode usar a conformidade com suas próprias políticas como um substituto para sua obrigação de conformidade com quaisquer disposições destas Exigências sem o consentimento por escrito do Citi.

1.2. Exigências Aplicáveis a Fornecedores Seletivos

O quadro a seguir lista algumas Exigências que se aplicam a determinados Fornecedores que atendem aos critérios de aplicabilidade nele designados. As seções não mencionadas abaixo são aplicáveis a TODOS os Fornecedores.

Nº da Seção	Título da Seção	Aplicabilidade
2	OPORTUNIDADES IGUAIS DE EMPREGO/AÇÃO AFIRMATIVA	Aplicável a contratos e pedidos de compra necessários para a execução de um contrato do Citi com o governo federal dos EUA; se houver incerteza sobre se o contrato ou pedido de compra constitui um subcontrato ou pedido de compra do governo federal, inclua “Conforme aplicável” no início ou no final da cláusula, conforme apropriado.
12	ANTILAVAGEM DE DINHEIRO	Aplicável a Fornecedores que executam determinados serviços relacionados ao cliente (ou seja, integração, triagem de conta e transação do cliente) ou a entrega de dados/métricas relacionados às atividades anteriores; <u>E/OU</u> Fornecedores que atuam como intermediários com relação a caixa ou instrumentos financeiros (p. ex., serviços de captura de depósito remota, courier, carro blindado ou cofre).
13	GESTÃO DE REGISTROS	Aplicável a Fornecedores que acessam/processam/armazenam Informações do Citi.
14	CONTINUIDADE DE NEGÓCIOS	Aplicável a Fornecedores que fornecem serviços ou hospedam infraestrutura/aplicativos de tecnologia usados pelo Citi. O Citi Business Activity Owner (BAO) é responsável por comunicar a aplicabilidade e os requisitos de COB ao Fornecedor.
15	NORMAS GLOBAIS DE VERIFICAÇÃO DE ANTECEDENTES	Aplicável a Fornecedores que prestam serviços ao Citi.
16	DESPESAS	Aplicável a Fornecedores que são contratualmente qualificados para reivindicar despesas comerciais reembolsáveis.
17	SEGURANÇA DA INFORMAÇÃO (IS)	Aplicável a Fornecedores, incluindo Subcontratados que acessam/processam/gerenciam/armazenam informações do Citi <u>E/OU</u> Fornecedores responsáveis como Host para aplicativos que usam a Internet com a marca do Citi; <u>E/OU</u> Fornecedores com conectividade com os recursos de rede do Citi; <u>E/OU</u> Fornecedores que exigem acesso sem acompanhamento às instalações do Citi.
18	DIRETRIZES DE LOCAL DE TRABALHO SEGURO	
19	INTELIGÊNCIA ARTIFICIAL/APRENDIZADO DE MÁQUINA (incluindo IA Generativa/IA Agêntica)	Aplicável a Fornecedores que utilizam Inteligência Artificial/Aprendizado de Máquina (IA/ML), conforme definido pelo Citi em qualquer parte do produto/serviço que estejam fornecendo.
20	POLÍTICA DE NEGOCIAÇÃO E INVESTIMENTO PESSOAL	Aplicável aos Fornecedores que exigem acesso regular a MNPI como parte de suas responsabilidades de trabalho no Citi.
23	POLÍTICA DE AUSÊNCIA OBRIGATÓRIA	Esta Política é aplicável a Não Funcionários (“Trabalhadores”) em Cargos Sigilosos (conforme definido no Glossário) (“Trabalhadores

Nº da Seção	Título da Seção	Aplicabilidade
		em Cargos Sigilosos”), bem como gestores e supervisores diretos de Funcionários em Cargos Sigilosos (“Gestores”) e Contatos da Unidade do Citi de Não Funcionários “em Cargos Sigilosos.

2 OPORTUNIDADES IGUAIS DE EMPREGO

2.1 Oportunidades Iguais de Emprego.

O Citi desenvolveu políticas concebidas para garantir oportunidades iguais de emprego para todas as pessoas qualificadas, independente de raça, cor, religião, sexo, orientação sexual, identidade de gênero, nacionalidade, cidadania, status de imigração, idade, estado civil, informações genéticas, deficiência, status de veterano protegido ou qualquer outra característica protegida por lei.

Os Fornecedores devem cumprir e fazer com que seu pessoal cumpra as exigências de todas as leis e regulamentos aplicáveis de não discriminação, incluindo, entre outros, quaisquer leis ou regulamentos que o Citi notifique por escrito ao Fornecedor para que sejam cumpridos.

Os Fornecedores revisarão e tomarão as medidas apropriadas consistentes com a Declaração de Política de Oportunidades Iguais de Emprego dos EUA do Citi, que pode ser encontrada em www.citigroup.com/global/eeo-aa-policy.

2.2 Contratos Administrativos

Contratos e pedidos de compra necessários para o cumprimento de um contrato do Citi com o governo federal devem conter literalmente a seguinte cláusula em negrito, conforme exibido abaixo. (Se tiver dúvidas se é um pedido de subcontratação/compra do governo federal, incorpore e adicione “Conforme aplicável” ao início da seção).

[Conforme aplicável,] o Fornecedor cumprirá todas as Leis federais antidiscriminação aplicáveis e certifica que não opera nenhum programa em violação de quaisquer Leis federais antidiscriminação aplicáveis.

2.3 Apêndice de Contratos Administrativos

Contratos e pedidos de compra necessários para o cumprimento de um contrato do Citi com o governo federal devem conter o seguinte aviso no apêndice do subcontrato ou pedido de compra. (Se tiver dúvidas se é um subcontrato/pedido de compra do governo federal, incorpore e adicione “Conforme aplicável” no final do aviso abaixo.)

Como um contratado do governo federal, o Citigroup está fornecendo ao contratado ou fornecedor abaixo assinado uma notificação escrita de nossas obrigações de oportunidades iguais de emprego em nome de veteranos e indivíduos com deficiências protegidos. O Citigroup cumpre plenamente a Seção 503 da Lei de Reabilitação e da Vietnam Era Veterans’ Readjustment Assistance Act (Lei de Assistência ao Reajuste de Veteranos da Era do Vietnã), bem como suas regulamentações aplicáveis, nos termos do 41 C.F.R. § 60-741 e 41 C.F.R. § 60-300, respectivamente. Nossa Declaração de

Política de Oportunidades Iguais de Emprego pode ser encontrada em www.citigroup.com/global/eeo-aa-policy. Quaisquer dúvidas sobre nossa Declaração de Política EEO podem ser direcionadas ao contato fornecido em nossa Declaração de Política.

[Conforme aplicável,] solicitamos que você tome as medidas apropriadas consistentes com nossa Declaração de Política e os regulamentos.

3 ANTISUBORNO E CORRUPÇÃO (AB&C)

O Citi tem políticas, procedimentos e controles internos razoáveis criados para cumprir as leis AB&C e proíbe estritamente pagamentos de suborno ou facilitação de qualquer forma. Os Fornecedores (incluindo Facilitador de Negócios), seu Pessoal ou qualquer pessoa que atue em nome do Citi, direta ou indiretamente, devem realizar suas atividades de acordo com os mais altos padrões éticos e em compliance com a Lei de Práticas Corruptas no Exterior (FCPA) dos EUA, a Lei de Suborno do Reino Unido (UKBA), cada uma conforme alterada e todas as outras leis locais AB&C aplicáveis dos países em que o Citi opera.

Nem o Fornecedor, nem qualquer um de seus Funcionários, operando em nome do Citi, ou em conexão com qualquer contrato ou relacionamento do Fornecedor com o Citi, (i) fará, conferirá, autorizará ou oferecerá quaisquer pagamentos, benefícios, vantagens ou qualquer outra coisa de valor a qualquer pessoa; ou (ii) receberá ou aceitará qualquer pagamento, benefício, vantagem ou qualquer outra coisa de valor de qualquer pessoa, em cada caso (i)-(ii) em violação da FCPA, da UKBA ou de quaisquer outras leis AB&C. O Fornecedor e seu Pessoal devem realizar suas atividades e transações em nome do Citi ou em conexão com qualquer contrato ou relacionamento do Fornecedor com o Citi, em conformidade com as Exigências, incluindo esta Seção. O Fornecedor e seu Pessoal também devem manter um programa de compliance AB&C e políticas e procedimentos projetados e aplicados para garantir compliance com todas as leis AB&C.

Para obter uma visão geral do Programa AB&C do Citi, acesse [Citigroup's Investor Relations](#) (em Políticas do Citi, selecione Programa AB&C).

4 PRESENTES E ENTRETENIMENTO

Os Fornecedores e seu Pessoal não podem oferecer presentes ou qualquer coisa de valor (incluindo entretenimento) aos funcionários do Citi, se isso puder criar um conflito de interesses real ou aparente, quid pro quo, comprometer a integridade ou julgamento do funcionário ou de outro modo influenciar indevidamente a tomada de decisão do funcionário, levar o funcionário a agir de forma contrária às suas funções ou de outra forma violar as leis aplicáveis. Sem limitar o acima exposto, o funcionário deve aderir à Seção de Presentes e Entretenimento Proibidos da Norma G&E. Os Fornecedores e seu Pessoal não devem oferecer presentes de negócios não monetários que excedam, no total, US\$ 300 por pessoa por ano civil, a qualquer funcionário do Citi.

Quando um Fornecedor fornece entretenimento de negócios (por exemplo, um convite para uma refeição, evento esportivo, cultural ou outro evento comparável) a um funcionário do Citi, o Fornecedor deve participar do evento e o entretenimento deve ser apropriado, habitual e razoável, não suntuoso ou excessivamente frequente. Além disso, se o Fornecedor não estiver presente no evento, o entretenimento será considerado um presente de negócios e estará sujeito aos limites de relatório aplicáveis da Norma de Presentes e Entretenimento do Citi. O Fornecedor não pode, em nome do Citi ou supostamente em nome do Citi, fornecer qualquer coisa de valor, incluindo à custa do próprio Fornecedor ou à custa de um funcionário do Citi, a qualquer pessoa, direta ou indiretamente, nem induzir outra pessoa a fazer o mesmo, se isso fosse, ou pudesse ser razoavelmente percebido, como uma ação corrupta, inadequada ou em violação da lei aplicável.

5 ENGAJAMENTO DE FORNECEDORES E PRINCÍPIOS DE FORNECEDORES

<https://www.citigroup.com/citi/suppliers/>O Citi interage com Fornecedores em várias iniciativas e para aumentar a conscientização sobre o programa de aquisição do Citi com possíveis Fornecedores das comunidades que atendemos. Além disso, o Programa procura identificar Fornecedores promissores, especialmente aqueles que promovem soluções inovadoras para abordar questões comerciais emergentes. Informações adicionais sobre as expectativas do Citi para fornecedores estão disponíveis no site [Doing Business with Citi](#) em:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 PROIBIÇÃO DE ESCRAVIDÃO MODERNA

O Citi está comprometido a manter práticas com o objetivo de identificar e tentar prevenir o risco de que a escravidão moderna e o tráfico humano possam ocorrer na organização ou em qualquer uma de suas cadeias de suprimentos. Os Fornecedores do Citi devem aderir às Exigências estabelecidas abaixo e desenvolverão políticas, procedimentos e/ou práticas eficazes em toda a empresa para identificar e tentar prevenir o risco de escravidão moderna e tráfico humano em suas próprias operações e cadeias de suprimentos. Os Fornecedores são obrigados a preencher o Questionário de Responsabilidade Corporativa do Citi a pedido do Citi, incluindo quaisquer informações adicionais necessárias, para permitir que o Citi avalie a exposição ao risco e as possíveis etapas de mitigação, principalmente para fornecedores em setores e regiões geográficas de alto risco. Espera-se que os Subcontratados do Fornecedor sigam o mesmo processo.

6.1 Prevenção de Trabalho Infantil

O Fornecedor não deve empregar mão de obra infantil. O termo “criança” refere-se a qualquer pessoa abaixo da idade mínima para trabalhar estabelecida pela legislação aplicável ou, na ausência de tal legislação, a qualquer pessoa com menos de 15 anos ou abaixo da idade de conclusão do ensino obrigatório, prevalecendo a idade mais

jovem. Sujeito à proibição imperativa da utilização do trabalho infantil, se trabalhadores com menos de 18 anos forem empregados, será dada especial atenção às funções que eles desempenham e às condições em que devem trabalhar para assegurar que não venham a sofrer danos físicos, mentais ou outros como um resultado direto ou indireto de seu trabalho ou condições de trabalho.

6.2 Emprego Escolhido Livremente

O Fornecedor deve garantir que os trabalhadores não sejam forçados, coagidos mental ou fisicamente, presos, escravizados, submetidos a trabalho prisional involuntário, traficados como escravos ou submetidos a trabalho compulsório de qualquer forma, incluindo horas extras forçadas. Todos os trabalhos devem ser realizados voluntariamente. Obrigações do Fornecedor neste instrumento incluem, entre outros, garantir o seguinte:

1. **Contratos, Salários e Horário de Trabalho:** Os trabalhadores devem ter os seus termos de emprego ou contratação descritos em um documento que seja facilmente compreensível para os mesmos e que estabeleça claramente os seus direitos e obrigações. Esse documento escrito deve incluir, entre outros, termos transparentes no que se refere a salários, horas extras, períodos de pagamento, horas de trabalho e direitos relativos a intervalos de descanso e férias. Esses termos escritos devem ser fornecidos ao trabalhador antes do início do trabalho, devem ser honrados pelo empregador e devem atender aos padrões da indústria e às exigências mínimas das leis e acordos coletivos aplicáveis no local onde o trabalho é realizado.
2. **Direito de Rescindir Livremente o Contrato de Trabalho:** Os trabalhadores devem ter o direito de rescindir livremente o seu contrato de trabalho, conforme adequado, após um prazo razoável de notificação, em conformidade com as leis e convenções coletivas aplicáveis e sem a imposição de sanções impróprias.
3. **Tratamento Desumano:** Os trabalhadores, suas famílias e os que estão intimamente ligados a eles não devem ser submetidos a tratamento rude ou desumano, incluindo, entre outros, punição física, violência ou coerção física, psicológica ou sexual, abuso verbal, assédio ou intimidação. Trabalhadores migrantes, suas famílias e as pessoas que estão intimamente ligadas a eles não devem ser objeto de discriminação em razão de sua nacionalidade.
4. **Salários, Benefícios e Horário de Trabalho:** A remuneração deve cumprir todas as leis salariais aplicáveis, incluindo aquelas relativas a salário mínimo, horas extras e benefícios exigidos legalmente. Os funcionários devem ser pagos integralmente, em tempo hábil e com declarações de pagamento transparentes. Não haverá deduções punitivas nem retenção de salários ou benefícios como medida disciplinar. As semanas de trabalho não devem exceder o máximo definido pela legislação local e as horas extras devem ser

voluntárias, dentro dos limites legais, e a recusa de fazer horas extras não deve ser punida.

5. **Sem Confisco de Documentos de Identidade:** Os trabalhadores não devem ter sua identidade ou autorizações de viagem, passaportes ou outros documentos oficiais ou quaisquer outros itens valiosos confiscados ou retidos como condição de emprego, e a retenção de propriedade não deve ser usada, direta ou indiretamente, para restringir as liberdades dos trabalhadores ou para criar escravidão no local de trabalho.
6. **Sem Taxas de Recrutamento ou Servidão por Dívida:** Taxas ou custos associados ao recrutamento de trabalhadores (incluindo, entre outros, taxas relacionadas a vistos de trabalho, despesas de viagem e custos de processamento de documentos) não devem ser cobrados dos trabalhadores, seja direta ou indiretamente. Da mesma forma, os trabalhadores não serão obrigados a fazer pagamentos que tenham a intenção ou o efeito de criar escravidão no local de trabalho, incluindo o pagamento de seguros, ou ser obrigados a reembolsar a dívida por meio do trabalho. Se for determinado que taxas ou custos foram cobrados dos trabalhadores em relação ao processo de recrutamento ou incorridos durante o curso do emprego, o Fornecedor deve tomar medidas razoáveis para obter reembolso imediato desses custos. Sempre que for necessário recrutar trabalhadores contratados por intermédio de terceiros, como uma agência de emprego, só serão contratadas agências de emprego bem conceituadas. Quando os trabalhadores forem contratados para serem empregados diretamente, apenas agências de recrutamento confiáveis devem ser contratadas. A proibição de taxas de recrutamento pagas por funcionários se aplica a todos os recrutadores, agentes e subagentes. Os Fornecedores devem ter controles para garantir compliance. **Liberdade de Movimento:** Os trabalhadores devem ser livres para circular sem restrições desproporcionais e não devem ser confinados fisicamente ao local de trabalho ou a outros locais controlados por empregadores (p. ex., blocos de acomodação). O alojamento em locais controlados pelo empregador não deve ser imposto aos trabalhadores, exceto quando for necessário devido à localização ou natureza do trabalho sendo executado.
7. **Reclamações sem retaliação:** Os trabalhadores devem ser livres para apresentar reclamações aos seus empregadores sobre o tratamento que o empregador lhes dá e os trabalhadores não devem sofrer prejuízos, represálias ou vitimização por ter apresentado uma queixa.

7 PESSOAL DO FORNECEDOR

7.1 Treinamento, Designação, Redesignação e Gestão de Pessoal do Fornecedor
O Fornecedor usará um número adequado de indivíduos com treinamento, educação, experiência e habilidade adequados para executar os Serviços da maneira mais eficaz, consistente com qualquer Contrato e comprovará as qualificações desses indivíduos

mediante solicitação. Após a designação de Pessoal a um Projeto, o Fornecedor não redesignará ou utilizará qualquer Pessoal para outros assuntos que reduzam sua disponibilidade para trabalhar no Projeto sem o consentimento prévio por escrito do Citi e geralmente designará o Pessoal em Projetos de uma maneira que minimize interrupções devido à necessidade de reorientação. O Fornecedor garantirá que seu pessoal não se fará passar por funcionário ou agente do Citi, nem esperará ser tratado como funcionário do Citi para nenhuma finalidade, incluindo alegações de direito a benefícios indiretos fornecidos pelo Citi ou para renda por invalidez, impostos ou benefícios de seguro social, imposto Federal de desemprego, benefícios de seguro-desemprego Estadual ou imposto Federal retido na fonte. O Fornecedor é o único responsável por todas as responsabilidades relacionadas ao empregador quanto ao seu Pessoal, incluindo, entre outros, manter todas as coberturas exigidas, preencher todas as declarações fiscais aplicáveis e fazer todos os pagamentos e depósitos de impostos necessários de maneira consistente com o status do Fornecedor como um Contratante independente.

7.2 Substituição do Pessoal do Fornecedor

O Fornecedor removerá e substituirá qualquer Pessoal designado pelo Fornecedor a um Projeto se o Citi notificar o Fornecedor de que essa pessoa é inaceitável para o Citi por qualquer motivo não discriminatório. O Fornecedor concorda ainda em remover e substituir qualquer Pessoal designado a um Projeto e impedi-lo de fornecer Serviços ao Citi (ou de qualquer responsabilidade com relação à entrega ou supervisão dos Serviços) imediatamente quando não puder ou não quiser fornecer os Serviços de forma oportuna e profissional.

7.3 Políticas de Pessoal do Fornecedor

O Fornecedor declara, garante e concorda que mantém e administra efetivamente políticas e procedimentos abrangentes para qualificar seu Pessoal que é pessoa física e está designado para fornecer Serviços no local ao Citi, e que essas políticas e procedimentos incluem verificação de autorização de trabalho, verificação de antecedentes profissionais e condenações criminais, conforme estabelecido neste documento, e exames toxicológicos antes da contratação, tudo na medida permitida pela Lei Aplicável e qualquer acordo coletivo de trabalho aplicável. Sem limitar a generalidade do exposto, o Fornecedor também declara, garante e concorda que possui controles e procedimentos para garantir a total conformidade do Fornecedor com toda a Lei Aplicável relacionada à imigração, incluindo a validação de que todo o Pessoal do Fornecedor designado ao Citi está autorizado a trabalhar durante toda a designação em total conformidade com toda a Lei Aplicável relacionada à imigração. Mediante solicitação, o Fornecedor fornecerá imediatamente ao Citi uma prova por escrito de autorização de trabalho para todo e qualquer Pessoal do Fornecedor designado ao Citi e sua conformidade com a Lei Aplicável relacionada à imigração e substituirá qualquer Pessoal que não tenha autorização de trabalho consistente com a Lei Aplicável por funcionários substitutos devidamente qualificados, incluindo o fornecimento de todo o treinamento e orientação necessários para garantir a prestação oportuna e eficaz dos Serviços, em cada caso, sem custo adicional para o Citi.

7.4 Propriedade do Fornecedor

Para cumprir as leis e regulamentos aplicáveis nas jurisdições em que o Citi faz negócios, mediante solicitação do Citi, os Fornecedores são obrigados a fornecer os detalhes de proprietários, que é uma pessoa natural e/ou uma entidade, incluindo proprietários imediatos do Fornecedor, até e inclusive o beneficiário efetivo que é proprietário ou controla direta ou indiretamente por meio de influência ou outros meios o contrato, produto ou serviço.

8 GESTÃO DE FRAUDES

Em conexão com os esforços do Citi para identificar e mitigar o risco de fraude (“Gestão de Fraudes”).

8.1 Todos os Fornecedores devem:

1. Cooperar com qualquer investigação do Citi em relação à suspeita ou alegação de roubo, fraude ou outra atividade criminal ou delito potencial e processar qualquer comportamento fraudulento ou criminal em toda a extensão permitida por lei.
2. Garantir informação e encaminhamento em tempo hábil de quaisquer possíveis eventos de fraude ao Citi por meio da [Ethics Hotline](#). Isso inclui, entre outros, tentativa, suspeita, alegação ou ocorrência real de roubo, fraude (por exemplo, enviar intencionalmente informações falsas, imprecisas ou equivocadas sobre o Fornecedor, esquemas de faturamento, desaparecimento de fundos e valores mobiliários etc.), atividade criminal ou delito envolvendo o Citi, um funcionário do Citi, um Fornecedor ou agente do Citi ou um não funcionário do Citi (por exemplo, funcionários e contratados temporários).
3. Permitir monitoramento e supervisão pelo Citi e seus representantes e apoiar investigações conduzidas pelo Citi e Agências de Aplicação da Lei relativas a atividades potencialmente fraudulentas envolvendo esse Fornecedor.
4. Informar, em tempo hábil, qualquer conflito de interesses (incluindo conflitos de interesses entre Fornecedores/Funcionários do Fornecedor e/ou Funcionários do Citi) de que os Fornecedores tenham conhecimento; e
5. Apoiar os processos de prevenção de fraudes do Citi durante a configuração ou atualização da conta bancária de um fornecedor no sistema de pagamento de Fornecedores do Citi.

8.2 Além disso, os Fornecedores que prestam serviços que são inerentemente mais expostos ao risco de fraude são **obrigados** a:

1. Documentar e seguir um Programa de Gestão de Risco de Fraude que identifique os riscos de fraude relevantes para os serviços que prestam ao Citi e os controles e procedimentos implementados para reduzir esses riscos.
2. Completar o treinamento de conscientização sobre fraude (no prazo de 90 dias corridos da contratação e anualmente depois disso) e treinar o pessoal sobre elementos específicos de risco de fraude que estão relacionados com os serviços específicos prestados ao Citi.

3. Monitorar casos de tentativa de fraude e manter controles eficazes para reduzir o risco de fraude em relação aos serviços que prestam ao Citi, documentar procedimentos para controles e testar continuamente a eficácia dos controles, reportando as deficiências ao Business Activity Owner (BAO).
4. Fornecer ao Business Activity Owner (BAO) quaisquer informações necessárias para a auditoria/monitoramento/avaliação contínuos da exposição ao risco de fraude.
5. A Auditoria inclui o Modelo de Avaliação de Impacto de Fraude de Terceiros ("TP-FIAT"), que foi criado para realizar avaliações de controle das capacidades dos Fornecedores relacionadas à mitigação de riscos de fraude. Este procedimento operacional descreve um conjunto de etapas a serem realizadas pelo Business Activity Owner (BAO) ou Third-Party Officer (TPO) e pelo Fraud Risk Management Officer ("FRMO") para identificar e gerenciar o risco de fraude.

8.3 Fornecedores com maior risco de fraude inerente incluem, entre outros, aqueles que:

1. Têm acesso a dados classificados como Confidenciais ou acima (quando não estiverem sob controle ou supervisão direta do Citi), que podem ser usados para possibilitar fraude, como acesso a contas internas, transações financeiras, transações em dinheiro.
2. Têm conectividade a redes/sistemas do Citi; e
3. Fornecem, apoiam ou têm acesso a serviços e recursos que podem ser visados para cometer ou possibilitar fraude, incluindo:
 - a) Identificação, integração ou solicitações de processamento de novos clientes;
 - b) Atividades de Pagamento/Transferência de Fundos do Citi ou do Cliente e/ou autenticação de acesso dos clientes do Citi a esses serviços;
 - c) Fazer, verificar ou completar alterações em dados do Citi ou de clientes do Citi (por exemplo, dados demográficos);
 - d) Fornecimento, manutenção ou autorização de instrumentos transacionais (por exemplo, cartões de débito/crédito, carteiras eletrônicas, talões de cheques etc.);
 - e) Provisão ou suporte de atividades de gestão de fraude operacional ao Citi, relativamente à prevenção detecção ou resposta a eventos de fraude;
 - f) Fornecimento de acesso físico a dinheiro, instrumentos financeiros e ativos/bens físicos;
 - g) Acesso sem escolta ou fora do horário de funcionamento nas instalações do Citi;
 - h) Demonstrações Financeiras: atividades contábeis, como lançar entradas no GL/SL;
 - i) Ganhar e gastar Recompensas por atividades incentivadas.

9 INTERAÇÃO COM A MÍDIA E APARIÇÕES PÚBLICAS

O departamento de Serviços Empresariais e Assuntos Públicos do Citi é o único departamento autorizado a emitir comunicados à imprensa ou declarações públicas em nome do Citi. Os Fornecedores não podem emitir qualquer comunicado de imprensa que, direta ou indiretamente, identifique o Citi, qualquer Contrato ou arranjo entre um fornecedor e o Citi ou qualquer produto ou serviço adquirido de um Fornecedor pelo Citi. Os Fornecedores não podem consentir ou se envolver em qualquer atividade de relações públicas relacionada ao Citi com Clientes, funcionários do Citi, outros Fornecedores do Citi, outros clientes de Fornecedores ou quaisquer outros terceiros sem a aprovação prévia por escrito de seu respectivo contato de negócios principal do Citi.

Os Fornecedores não podem publicar qualquer material por escrito ou em formato eletrônico (incluindo livros, artigos, podcasts, webcasts, blogs, publicações em sites, fotos, vídeos, mídia social ou outras mídias), conduzir ou fazer discursos, dar entrevistas ou fazer aparições públicas que mencionem o Citi, as operações, Clientes, produtos ou serviços do Citi sem a aprovação prévia por escrito de seu respectivo contato de negócios principal do Citi e o diretor sênior de assuntos públicos do país.

Estando ou não em conexão com a provisão de serviços ou produtos do Citi, os Fornecedores não podem usar símbolos exclusivos, marcas registradas, marcas de serviço, nomes comerciais, logotipos, símbolos ou nomes de marcas, sem, em cada caso, garantir o consentimento prévio por escrito do Citi. Os Fornecedores não podem usar o nome, logotipo ou marcas registradas, instalações ou relacionamentos do Citi para benefício ou para trabalho fora do Citi (incluindo timbre ou sites pessoais, blogs ou outros sites de redes sociais). Além disso, os Fornecedores não podem fazer qualquer uso do nome, instalações ou relacionamentos para fins de caridade ou pro bono.

10 COMUNICAÇÕES ELETRÔNICAS ESCRITAS

Ao interagir com o pessoal do Citi, ou no desempenho de suas obrigações para ou em nome do Citi, os fornecedores têm permissão para usar apenas os Equipamentos, Sistemas e Serviços de Comunicação Eletrônica Escrita aprovados pelo Citi. Canais de Comércio Eletrônico novos, expandidos ou modificados do Citi, seja como ferramentas independentes ou integrados em uma plataforma mais ampla, fornecidos pelo Citi ou de terceiros, devem ser aprovados de acordo com as Exigências do Citi aplicáveis, das quais o Fornecedor foi notificado por escrito por seu BAO. É proibido falar sobre os negócios do Citi com o pessoal do Citi em plataformas de mensagens não aprovadas pelo Citi, como WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber e qualquer outra plataforma eletrônica interativa.

Além disso, os Fornecedores não devem ter expectativas de privacidade em relação às Comunicações Eletrônicas escritas criadas, descobertas, usadas, acessadas, baixadas, armazenadas, transmitidas, recebidas ou excluídas por meio de Equipamentos, Sistemas e Serviços de Comunicação fornecidos pelo Citi. O Citi pode monitorar Equipamentos, Sistemas e Serviços de Comunicações Eletrônicas e Comunicações

Eletrônicas. Essas Comunicações Eletrônicas são propriedade do Citi e podem ser mantidas de acordo com as exigências de retenção de registros aplicáveis (sujeito à legislação e regulamentação local).

<https://policydirectory.citi.net/cpd/layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 ATIVIDADES E CONTRIBUIÇÕES POLÍTICAS

Diversas leis, como aquelas relacionadas a: influência estrangeira; financiamento de campanhas; presentes e entretenimento; lobby legislativo, de mobilização de base (grassroots), de promoção de imagem (goodwill) e regulatório; contratações públicas e práticas de “pay-to-play”; bem como valores mobiliários; e a regulamentação de atividades políticas e das divulgações relacionadas a tais atividades, envolvendo o Citi e seus fornecedores. É proibida qualquer atividade política por parte de Fornecedores que não esteja em conformidade com as políticas ou normas relevantes do Citi, com a legislação ou com regulamentações.

A atividade política inclui, entre outros:

1. Fazer contribuições políticas corporativas ou pessoais, solicitar contribuições políticas, usar fundos ou recursos da empresa (como instalações, equipamentos, software ou pessoal) ou oferecer serviços pessoais como voluntário durante o horário da empresa em nome de um candidato concorrendo a um cargo público, um comitê de partido político ou um comitê político.
2. Fazer lobby ou contatar autoridades públicas, seja diretamente ou por intermédio de terceiros, incluindo tentativas de influenciar autoridades, a legislação e, dependendo da jurisdição, podem incluir tentativas de influenciar as autoridades regulamentadoras ou a concessão de contratos administrativos; ou
3. Buscar, aceitar ou ocupar qualquer cargo político associado a um governo, incluindo qualquer conselho governamental, comissão ou outra organização similar.

Nenhuma atividade política pode ser realizada ou conduzida por qualquer Fornecedor em nome do (ou supostamente em nome do) Citi, ou de seus clientes, sem autorização prévia por escrito do Controle de Operações Globais (ggacontrol@citi.com) de Assuntos Governamentais do Citi. Embora o Citi possa pagar uma tarifa e/ou reembolsar os custos diretos dos serviços contratados e permitidos de atividade política fornecidos pelo Fornecedor, como lobby, o Citi não reembolsará Fornecedores ou qualquer um de seus funcionários por contribuições políticas pessoais ou corporativas de qualquer tipo.

12 ANTILAVAGEM DE DINHEIRO (“AML”)

Aplicável a Fornecedores que executam determinados serviços relacionados ao cliente (ou seja, integração, triagem de contas e transações de clientes) ou a entrega de dados/métricas relacionados às atividades anteriores; E/OU que atuam como intermediários em relação a

transações ou instrumentos financeiros (por exemplo, serviços de captura remota de depósitos, courier, carro blindado ou cofre, transferências eletrônicas, ativos digitais).

12.1 Obrigações de AML:

1. Conformidade com os Processos do Citi e as Leis Aplicáveis:

- Manter e cumprir os processos e procedimentos do Citi, projetados para atender às exigências das leis aplicáveis, incluindo (i) a Lei Gramm-Leach-Bliley e os regulamentos promulgados em seu âmbito; (ii) A Lei PATRIOTA dos EUA e os regulamentos promulgados em seu âmbito; (iii) qualquer lei ou regulamento que trata de lavagem de dinheiro; e (iv) qualquer lei ou regulamento relacionado a sanções econômicas. Essas políticas e procedimentos abordarão as funções e responsabilidades em procedimentos antilavagem de dinheiro, incluindo a obrigatoriedade de reportar imediatamente qualquer atividade observada que pareça incomum ou potencialmente incomum relacionada a atividades financeiras, transações e entrada de caixa.

2. Treinamento Anual e Elementos do Programa para o Pessoal:

- Garantir que os Funcionários que prestam os Serviços para o Citi recebam treinamento anual em relação às funções e responsabilidades em procedimentos antilavagem de dinheiro, incluindo a obrigatoriedade de reportar imediatamente qualquer atividade observada que pareça incomum ou potencialmente incomum relacionada a atividades financeiras, transações e entrada de caixa. O treinamento incluirá, entre outros, os seguintes componentes:
 - a. Relatório e encaminhamento de atividades suspeitas.
 - b. Um programa “Know Your Customer” (KYC), incluindo um Customer Identification Program (CIP), verificação de sanções e nome, customer due diligence (CDD), enhanced due diligence (EDD) e a identificação e verificação de **Ultimate Beneficial Owners (UBOs)**.
 - c. Monitoramento de transações em todos os instrumentos e atividades financeiras relevantes.
 - d. Relatórios/métricas periódicos, incluindo relatório de alterações legais e regulatórias e alterações relevantes ao programa AML.
 - e. Testes e controles de eficácia do programa AML, incluindo visitas ao local.

3. Cumprimento das Disposições Contratuais:

- Cumprir quaisquer disposições do Contrato que definam qualquer programa que deva ser instituído pelo Fornecedor.

4. **Relato Imediato de Suspeitas de Violação:**

- Informar imediatamente o Citi, por escrito, sobre qualquer suspeita de violação da lei, incluindo qualquer atividade observada que pareça incomum ou potencialmente incomum relacionada a entrada de caixa, atividades financeiras ou transações que envolvam o Citi ou seus clientes.

5. **Prevenção e Denúncia de Sonegação/Evasão Fiscal:**

- Cumprir todas as leis e regulamentos tributários aplicáveis nos países onde operam.
- Em nenhuma circunstância os Fornecedores devem se envolver em sonegação/evasão fiscal deliberada ou facilitar essa evasão em nome de terceiros, o que pode incluir atividades que ajudem a evitar o pagamento de impostos devidos e a pagar ou ocultar informações das autoridades fiscais.
- Portanto, os Fornecedores devem adotar procedimentos de prevenção razoáveis relacionados à sonegação/evasão fiscal de impostos e informar imediatamente ao Citi por escrito quaisquer violações ou suspeitas de violações relacionadas ao Citi.

12.2 **Políticas e Procedimentos Internos do Fornecedor:**

Os Fornecedores também devem manter políticas e procedimentos internos adequados para cumprir todas as leis e regulamentos de AML já existentes ou que venham a entrar em vigor no futuro.

13 **GESTÃO DE REGISTROS**

Aplicáveis a Fornecedores que acessam/processam/armazenam Informações do Citi.

O Citi exige que todos os Fornecedores com custódia de informações do Citi trabalhem com seu Business Activity Owner (“**BAO**”) ou contato de negócios principal do Citi para (i) identificar e classificar as informações, como Registros ou Informações Transitórias para fins de gestão de registros do Citi, (ii) classificar Registros de acordo com o Master Record Catalogue (“**MRC**”) do Citi, (iii) reter informações com base nas exigências de retenção do Citi e (iv) quando não houver indicação para Reter Informações, descartar as Informações adequadamente no final do Ciclo de Vida das Informações.

O BAO ou o contato de negócios principal do Citi deve trabalhar com o Fornecedor para garantir que o Fornecedor tenha identificado e classificado os registros de acordo com os códigos de registro do Citi no MRC e que seja atualizado pelo menos anualmente. O Fornecedor tem a obrigação de cumprir as exigências de Gestão de Registros comunicadas pelo BAO. Os registros que atendem aos critérios de qualificação para descarte devem ser adequadamente descartados o mais rápido possível, mas não mais de seis meses após o cumprimento dos requisitos de retenção, a não ser que estejam sujeitos à Retenção de Informações. Informações Transitórias devem ser destruídas não mais de dois anos após seu último uso, a menos que sujeitas à Retenção de Informações. Informações Transitórias que incluem informações pessoais devem ser excluídas assim que a finalidade para a qual foram coletadas for cumprida, a não ser que estejam sujeitas à Retenção de Informações. O Fornecedor deve suspender a destruição ou alteração de Informações do Citi quando for notificado de uma Retenção de Informações. Em caso de dúvida, o Fornecedor deve verificar com seu contato de negócios principal do Citi ou o BAO.

Trimestralmente, as regras de retenção listadas nos Cronogramas de Retenção do País são revisadas e atualizadas conforme necessário para estarem em conformidade com as mudanças regulatórias e internas do DRIM. Caso haja uma alteração que afete o Fornecedor, o BAO informará o Fornecedor. O Fornecedor deve avaliar o impacto e implementar alterações nos respectivos sistemas, processos e inventários. Tipos de registro que ele detém e gerencia, no prazo de 90 dias a contar da notificação do BAO.

Os fornecedores que mantêm documentos em nome do Citi são responsáveis por preservar (“manter”), coletar e produzir todas as Informações que sejam consideradas relevantes para um processo legal ou outro dentro do prazo exigido, conforme solicitado pelo BAO. O Fornecedor deverá, mediante solicitação, devolver as informações do Citi conforme exigido pelos termos contratuais aplicáveis. Os Fornecedores não devem descartar Informações do Citi, independentemente de sua classificação (por exemplo, Confidencial, não Confidencial) sem a aprovação do contato de negócios principal do Citi ou BAO, o que deve incluir uma confirmação de que nenhuma Retenção de Informações ativa se aplica às Informações prestes a serem destruídas. As exigências de Gestão de Registros e de retenção e todas as exigências de manuseio de informações devem sobreviver ao término ou vencimento do Contrato, salvo acordo expresse em contrário.

Os Fornecedores devem manter documentação listando todo o Pessoal do Fornecedor responsável por supervisionar a gestão de Informações do Citi sob custódia do Fornecedor e realizar reuniões periódicas com seu contato de negócios principal do Citi ou Records Management Officer para revisar e atualizar nomes de contatos, detalhes de procedimentos, funções e responsabilidades e o Inventário de Registros do Fornecedor do Citi.

14 RESILIÊNCIA EMPRESARIAL/CONTINUIDADE DE NEGÓCIOS

Aplicável a Fornecedores que fornecem serviços ou hospedam infraestrutura/aplicativos de tecnologia usados pelo Citi. O Citi Business Activity Owner (BAO) é responsável por comunicar a aplicabilidade e os requisitos de COB ao Fornecedor.

14.1 Recursos de Recuperação

O Plano de Recuperação de Desastres do Fornecedor deve fornecer recursos alternativos capazes de fornecer todos os produtos e serviços ao Citi caso os locais principais do Fornecedor sejam desativados. Os recursos de recuperação devem estar localizados em locais separados geograficamente dos locais principais com separação suficiente para minimizar ou eliminar a ameaça do mesmo desastre poder afetar os locais principal e de recuperação.

1. Os recursos de recuperação não estão limitados aos Sistemas de Informação, mas incluem todos os recursos necessários para a entrega contínua de produtos e serviços para o Citi e podem incluir equipe, prédios, equipamentos de negócios, centro de dados, redes de dados e voz e serviços de transporte.
2. Fornecedores de aplicativos podem implementar um tipo de arquitetura Hot/Hot para garantir uma configuração de Alta Disponibilidade (HA). Essa arquitetura requer que existam dois (no mínimo) sistemas igualmente configurados que estão em operação e disponíveis para clientes/usuários. A característica mais importante oferecida por este modelo é que o(s) ambiente(s) alternativo(s) está(ão) funcionando simultaneamente com o datacenter primário (produção).

14.2 Níveis de Serviço de Recuperação

A continuidade dos negócios dos fornecedores deve atender aos níveis de serviço estabelecidos para ser eficaz para o Citi. No mínimo, o Plano de Recuperação de Desastres do Fornecedor deve estabelecer valores específicos para:

1. Objetivo de Tempo de Recuperação
2. Objetivo de Ponto de Recuperação;
3. Recursos de Recuperação/Capacidade de Tecnologia
4. Duração da Recuperação

14.3 Plano de Recuperação de Desastres

O Fornecedor manterá um Plano de Recuperação de Desastres para a continuidade dos negócios (e fornecerá evidências de seus testes atuais e periódicos, se solicitado pelo Citi) para que, apesar de qualquer interrupção na capacidade do Fornecedor para fornecer os Produtos/Serviços ou cumprir suas outras obrigações aqui contidas de qualquer local específico ou por meio dos esforços de qualquer indivíduo em particular, o Fornecedor possa prontamente fornecer os Produtos/Serviços e cumprir suas obrigações a partir de um local alternativo ou com Pessoal substituto. Uma cópia do Plano de Recuperação de Desastres deve ser fornecida ao Citi no prazo de dez (10) dias

corridos a partir da Data Efetiva de cada Ordem de Serviço celebrada entre o Citi e o Fornecedor e, posteriormente, anualmente, enquanto cada Ordem de Serviço estiver em vigor. O Fornecedor fornecerá ao Citi quaisquer instruções ou outras informações necessárias para que o Citi continue a receber Produtos/Serviços do Fornecedor em circunstâncias em que o Fornecedor invoca seu Plano de Recuperação de Desastres. O Fornecedor declara, garante e concorda que seu Plano de Recuperação de Desastres incluirá, no mínimo:

1. Procedimentos e estratégias de recuperação, incluindo realocação, transferência de trabalho e/ou acesso remoto para mitigar os efeitos de interrupções, incluindo indisponibilidade de tecnologia (Negação de Serviço/DoS), indisponibilidade do local principal de trabalho (Negação de Acesso/DoA) e indisponibilidade da equipe (inclusive de subcontratados);
2. Manutenção pelo Fornecedor (incluindo, entre outros) de um local secundário de recuperação de desastres separado dos locais do Produto/Serviço, o armazenamento de mídia de backup em um local separado dos locais do Produto/Serviço, o uso de linhas e servidores de comunicação redundantes;
3. Procedimentos para backup/restauração da operação e aplicação dos Produtos/Serviços, incluindo um plano detalhado e documentado para responder a uma interrupção prolongada dos Produtos/Serviços causada por falha de energia, falha do sistema, desastre natural ou outras circunstâncias imprevistas que envolvam processos e procedimentos para retomar as operações no prazo mutuamente acordado;
4. Procedimentos para a proteção de todo o Conteúdo;
5. Procedimentos e quaisquer acordos de terceiros para equipamentos de substituição (por exemplo, equipamentos de computador);
6. Procedimentos para quaisquer instalações de produção fora do local; e
7. O plano de Recuperação de Desastres do Fornecedor estabelecerá que:
 - a. O Fornecedor notificará imediatamente o Citi sobre qualquer desastre que possa afetar negativamente os Produtos/Serviços;
 - b. O Fornecedor fornecerá ao Citi, no prazo de 24 horas do referido aviso, um plano para continuar a fornecer os Produtos/Serviços em uma instalação de processamento alternativa;
 - c. Os Produtos/Serviços devem estar totalmente operacionais dentro do Objetivo de Tempo de Recuperação (RTO) necessário, que, se não for definido de outra forma no Contrato aplicável, é de no máximo 4 horas para processos aos quais o Citi atribui a classificação de criticalidade “Crítico para a Empresa” ou “ALTA”, no máximo 24 horas para processos aos quais o Citi atribui a classificação de criticalidade “MÉDIA” e no máximo 72 horas para processos aos quais o Citi atribui a classificação de criticalidade “BAIXA”; e
 - d. Se partes das instalações do Fornecedor estiverem inoperantes, o Fornecedor tratará o Citi de forma não menos favorável do que o Fornecedor trata seus outros clientes comerciais.

14.4 Exigências do Plano de Recuperação de Desastres Aplicáveis aos Serviços Hospedados.

À medida que o Fornecedor gerencia e fornece um Serviço Hospedado ao Citi, as disposições a seguir também se aplicam. O Plano de Recuperação de Desastres incluirá, no mínimo:

1. Procedimentos para backup/restauração da operação e aplicação dos Serviços Hospedados, incluindo um plano detalhado e documentado para responder a uma interrupção prolongada nos serviços causada por falha de energia, falha do sistema, desastre natural ou outras circunstâncias imprevistas que incluam processos e procedimentos para retomar as operações no prazo mutuamente acordado;
2. Além disso, o Plano de Recuperação de Desastres do Fornecedor estabelecerá que: (a) O Fornecedor notificará o Citi por escrito no prazo de duas (2) horas sobre qualquer desastre que possa afetar negativamente os Serviços Hospedados; (b) o Fornecedor fornecerá ao Citi, no prazo de 24 horas do referido aviso, um plano para continuar a fornecer os Serviços Hospedados em uma instalação de processamento alternativa, e (c) os Serviços Hospedados devem estar totalmente operacionais no prazo de 48 horas do aviso inicial;
3. O Fornecedor concorda, mediante solicitação, em divulgar as informações necessárias para permitir que o Citi desenvolva um plano de recuperação de desastres e um plano de continuidade de negócios, que funcionará em conjunto com o Plano de Recuperação de Desastres e o plano de continuidade de negócios do Fornecedor; e
4. Se partes das instalações do Fornecedor estiverem inoperantes, o Fornecedor tratará o Citi de forma não menos favorável do que o Fornecedor trata seus outros clientes comerciais.

14.5 Mudanças no Plano de Recuperação de Desastres

O Fornecedor pode alterar seu Plano de Recuperação de Desastres, desde que as alterações não rebaixem o Plano de Recuperação de Desastres de maneira que possa afetar adversamente os serviços (por exemplo, prolongando seus RTOs). O Fornecedor comunicará imediatamente quaisquer alterações em seu Plano de Recuperação de Desastres ao Citi e, a pedido do Citi, explicará as alterações para que o Citi entenda completamente e seja capaz de responder às alterações.

14.6 Plano de Recuperação de Desastres de Subcontratados

O Fornecedor garantirá que qualquer Subcontratado do Fornecedor mantenha um Plano de Recuperação de Desastres e controles de Continuidade de Negócios relacionados consistentes com as Exigências do Citi para Fornecedores. O Fornecedor deve fornecer supervisão apropriada dos Subcontratados, incluindo a revisão periódica desses controles e resultados dos testes e garantir a correção oportuna de quaisquer lacunas identificadas.

14.7 Invocação do Plano de Recuperação de Desastres e Notificação de Crise

O Fornecedor notificará imediatamente o principal contato comercial do Citi:

1. Quando o Fornecedor invocar seu Plano de Recuperação de Desastres e;
2. Com relação a qualquer crise, ameaça, aviso ou evento cibernético contra o Fornecedor ou seus Subcontratados que tenha probabilidade razoável de impactar adversamente os Serviços ou Produtos fornecidos ao Citi.

14.8 Testes

Todos os recursos e planos de recuperação do Fornecedor devem ser testados no prazo de 120 dias após a implementação na produção (90 dias no caso de aplicativos classificados pelo Citi como Críticos para a Empresa) e ser testados anualmente (a cada 12 meses) no mínimo. O teste deve demonstrar a capacidade do Fornecedor de cumprir os níveis de serviço de recuperação para todos os produtos e serviços fornecidos ao Citi. Esses testes devem ser abrangentes e incluir todo o escopo dos Serviços fornecidos ao Citi. Os Fornecedores devem informar o Citi sobre o teste de recuperação dos produtos/serviços fornecidos ao Citi com pelo menos 30 dias corridos de antecedência. O Citi pode participar ou observar o teste de recuperação do Fornecedor de aplicativos usados pelo Citi para validar a funcionalidade comercial do aplicativo no ambiente de recuperação. Se o Citi desejar participar, o Fornecedor fornecerá ao Citi os objetivos do teste, o plano de teste e os procedimentos para se conectar ao local do teste antes de realizar o teste. No prazo de (10) dias úteis após a conclusão de cada teste, o Fornecedor fornecerá ao Citi um resumo dos objetivos do teste, o plano de teste e os resultados do teste, incluindo os prazos necessários para recuperação e evidências dos resultados do teste (por exemplo, capturas de tela).

14.9 Validação de Volume

Um fornecedor que hospeda aplicativos classificados pelo Citi como Críticos para a Empresa deve demonstrar que os volumes de Produção podem ser processados em seu ambiente de recuperação de desastres/COB. O Citi e o Fornecedor devem concordar com a metodologia a ser usada para validação.

14.10 Uso dos Sistemas do Citi para Fornecer Serviços

Se solicitado pelo Citi ou por Afiliadas do Citi, os Fornecedores que utilizam os Sistemas do Citi participarão, sem custo ou encargo para o Citi, dos exercícios de recuperação de desastres do Citi.

14.11 Como Lidar com os Resultados dos Testes

Se qualquer resultado de teste do Fornecedor mostrar que não atendeu qualquer objetivo do teste ou RTO aplicável, o Fornecedor realizará uma análise da causa raiz e corrigirá imediatamente as deficiências identificadas. Após a implementação da correção, o Fornecedor conduzirá um novo teste no máximo dentro de cento e vinte (120) dias corridos (90 dias corridos no caso de aplicativos classificados pelo Citi como Críticos para a Empresa) após a falha do teste inicial (ou o período de tempo especificado na Ordem de Trabalho relevante).

14.12 Gestão de Crises

Em conjunto com seu plano de continuidade de negócios, o Fornecedor deve manter um plano de gestão de crises para controlar as operações de recuperação. No mínimo, o

plano de gestão de crises do Fornecedor deve identificar pessoas específicas com autoridade suficiente para ativar uma operação de recuperação, definir protocolos de comunicação e encaminhamento para coletar e divulgar informações da crise e incluir protocolos de notificação e encaminhamento para comunicação com o Citi no caso de uma crise.

14.13 Avaliações de Continuidade de Negócios

Os Fornecedores estão sujeitos ao Processo de Avaliação de Continuidade de Negócios de Terceiros do Citi para avaliação das políticas, procedimentos e controles do Fornecedor em relação ao compliance com os requisitos do Citi e quaisquer requisitos legais e/ou regulatórios (aplicáveis ao Citi ou ao Fornecedor) que dizem respeito à continuidade de negócios. A avaliação consiste em questionários que exigem respostas do Fornecedor com evidências comprobatórias e pode incluir visitas aos locais do Fornecedor. Se as descobertas de uma avaliação revelarem ou indicarem problemas ou preocupações, o Citi documentará as descobertas e trabalhará com o Fornecedor para identificar um meio para corrigir os problemas. Os fornecedores devem fazer rapidamente as correções necessárias e/ou adicionar controles compensatórios para atender às preocupações do Citi de forma satisfatória.

14.14 Resiliência Operacional

Serviços Comerciais Críticos são aqueles serviços que, se a entrega foi interrompida, podem causar impacto adverso significativo no Citi, em seus clientes ou no sistema financeiro. O Fornecedor deve garantir que qualquer interrupção na entrega de elementos dos serviços que representem serviços comerciais críticos ou apoiem a prestação de serviços comerciais críticos por parte do Citi, conforme especificado pelo Citi periodicamente (“Serviços Comerciais Críticos”) não exceda a duração definida pelo Citi nem viole qualquer métrica relevante definida pelo Citi (“Tolerâncias de Impacto”) conforme notificado ao Fornecedor periodicamente. As Tolerâncias de Impacto serão expressas como uma métrica clara com prazo definido, correspondente ao período de tempo durante o qual a prestação do serviço pode sofrer interrupção. O Citi e o Fornecedor revisarão as Tolerâncias de Impacto anualmente como parte do processo contínuo de governança do contrato. Quando o Citi for obrigado a definir mais de uma Tolerância de Impacto para um Serviço Comercial Crítico individual devido às exigências de mais de um Órgão Regulador, o Citi poderá especificar Tolerâncias de Impacto separadas para esse Serviço Comercial Crítico. O Fornecedor deve:

1. Notificar o Citi assim que tomar conhecimento de que falhou (ou é razoavelmente provável que venha a falhar) na prestação de qualquer serviço dentro das Tolerâncias de Impacto correspondentes definidas pelo Citi, juntamente com uma explicação dos motivos de qualquer falha potencial ou real e as medidas tomadas para mitigar o impacto dessa falha;
2. Quando solicitado, fornecer assistência razoável ao Citi para permitir que sejam identificados as pessoas, os processos, as tecnologias, as instalações e as informações necessárias para que o Fornecedor forneça o serviço para apoiar Serviços Comerciais Críticos;
3. Fornecer assistência razoável ao Citi para permitir que o Citi conduza:
 - a. qualquer teste de cenário interno da capacidade do Fornecedor de

- permanecer dentro da(s) Tolerância(s) de Impacto para cada Serviço Comercial Crítico no caso de uma interrupção grave, mas plausível, de suas operações ou das operações do Fornecedor; e
- b.** quaisquer lições aprendidas exercidas após um teste de cenário para permitir que o Citi identifique pontos fracos e quaisquer ações necessárias para melhorar a capacidade do Fornecedor de responder e se recuperar de interrupções futuras.

Quando qualquer teste de cenário interno do Citi identificar vulnerabilidades ou limitações na capacidade do Fornecedor de fornecer serviços dentro das Tolerâncias de Impacto correspondentes definidas pelo Citi e após qualquer falha do Fornecedor em entregar qualquer serviço dentro das Tolerâncias de Impacto correspondentes definidas pelo Citi, as partes acordarão um plano (incluindo um cronograma para implementar o plano), para garantir que o Fornecedor tome as medidas necessárias para resolver ou mitigar tais vulnerabilidades ou limitações ou remediar a causa da falha em permanecer dentro das Tolerâncias de Impacto (conforme aplicável) assim que for razoavelmente praticável.

14.15 Contrato de Depósito em Caução

A pedido do Citi, os Fornecedores (i) que licenciam o software para o Citi para operação no ambiente do Citi ou (ii) que fornecem um Serviço Hospedado ao Citi devem garantir que os Materiais de Depósito sejam depositados com o terceiro depositário designado do Citi e executar um cronograma de registro de depositantes ou outros formulários exigidos pelo terceiro depositário com relação aos Materiais de Depósito de acordo com o contrato de caução aplicável. Posteriormente, durante o restante do prazo do contrato aplicável com relação à licença ou Serviço Hospedado, o Fornecedor depositará versões atualizadas dos Materiais de Depósito com o terceiro depositário para garantir que o Código-Fonte em depósito e outros Materiais de Depósito permaneçam atualizados com a versão mais recente do software aplicável à versão do software ou Serviços Hospedados sendo usados pelo Citi. O Código-Fonte ou outras atualizações do Material de Depósito devem ser entregues ao terceiro depositário dentro de 30 (trinta) dias após a data de qualquer atualização do software licenciado para o Citi ou modificações aos Serviços Hospedados que estão sendo usados pelo Citi. O Fornecedor cumprirá totalmente todas as obrigações e exigências de um depositante, conforme estabelecido no contrato de caução. O Fornecedor é o único responsável por todos os custos e taxas de caução, incluindo, entre outros, taxas de configuração, taxas anuais, taxas de depósito, taxas de serviços e quaisquer outras taxas e custos de caução. No caso de um Evento de Liberação, o Terceiro Depositário liberará os Materiais de Depósito para o Citi ou pessoa designada pelo Citi, de acordo com os termos do contrato subjacente e do contrato de caução.

Se o Código-Fonte (ou outros Materiais de Depósito) for entregue ao Citi ou ao designado do Citi (diretamente pelo Fornecedor ou pelo Terceiro Depositário em cumprimento de suas obrigações sob um contrato de caução aplicável), o Código-Fonte e os Materiais de Depósito estão sujeitos à licença existente nos termos do contrato relevante entre o Fornecedor e o Citi; desde que se considere que cada licença dá ao Citi o direito de usar e modificar o Código-Fonte e outros Materiais de Depósito conforme razoavelmente necessário para: (i) integrar e garantir a compatibilidade do software e outros Materiais de Depósito com os sistemas do Citi, (ii) fazer com que o software ou

outros Materiais de Depósito cumpram a Lei Aplicável, as normas do setor ou a prática de mercado, (iii) permitir que o software ou outros Materiais de Depósito permaneçam atualizados com inovações tecnológicas e (iv) permitir que o software e outros Materiais de Depósito cumpram os objetivos de negócios do Citi e de suas Afiliadas no escopo da Licença existente. Quaisquer versões do Software que incluam uma modificação desenvolvida por ou em nome do Citi usando o Código-Fonte estão sujeitas a todas as disposições desta Seção e ao acordo subjacente; desde que o Fornecedor não tenha direito, título ou interesse em ou a quaisquer modificações, e todos os direitos de propriedade intelectual a quaisquer modificações serão exclusivos do Citi.

O Fornecedor envidará esforços comercialmente razoáveis com terceiros que forneceram qualquer software usado no Software para permitir que o Fornecedor coloque o código-fonte desse software de terceiros no Depósito do Código-Fonte. Se o terceiro se recusar a conceder ao Fornecedor esse direito, o Fornecedor envidará esforços comercialmente razoáveis para ter o contrato de licença de software de terceiros aplicável transferido para o Citi em um Evento de Liberação.

O Código-Fonte entregue ao Citi de acordo com esta Seção estará sujeito à Licença existente para o Software licenciado aplicável ou Serviços Hospedados aplicáveis, *desde que* o Citi possa usar e modificar o Código-Fonte e o Software em conexão com seus requisitos comerciais e operacionais, para permitir que o Software permaneça atualizado com inovações tecnológicas e para cumprir a Lei Aplicável. Quaisquer versões do software que incluam uma modificação desenvolvida por ou em nome do Citi usando o Código-Fonte estão sujeitas a todas as disposições do contrato aplicável; desde que o Fornecedor não tenha direito, título ou interesse em ou a quaisquer modificações, e todos os Direitos de Propriedade Intelectual a quaisquer modificações serão exclusivos do Citi.

15 NORMAS GLOBAIS DE VERIFICAÇÃO DE ANTECEDENTES

Aplicável a todos os Fornecedores Terceirizados que prestam serviços ao Citi.

15.1 Visão Geral – Verificação de Antecedentes

A verificação de antecedentes deve ser realizada de acordo com todas as leis e regulamentos locais aplicáveis. Todas as informações e autodivulgações descritas neste documento devem ser fornecidas pelos representantes do Fornecedor e Subcontratados, conforme apropriado. Falsificação ou omissão das informações, quer seja no currículo, durante uma entrevista, em um formulário de integração ou durante o processo de integração, não importa quando for descoberto, pode constituir motivos de recusa ou término da atribuição no Citi de acordo com a lei local. Resultados adversos de qualquer verificação realizada, não importa quando for descoberto, também podem constituir motivos de recusa ou término da atribuição no Citi de acordo com a lei local. Informações adicionais sobre a conclusão da verificação de antecedentes podem ser encontradas em

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Coleta de Informações Básicas e Verificação de Identidade

Antes de qualquer funcionário do Fornecedor começar uma atribuição no Citi, os Fornecedores devem coletar o nome e sobrenome, endereço de correspondência e endereço permanente (se diferente), número de telefone e e-mail (se aplicável) das pessoas. O Pessoal do Fornecedor também deve fornecer documentação que confirme sua identidade. Isso pode incluir fornecer informações e/ou documentação de um número de identificação nacional, cartão de identificação emitido pelo governo com foto ou um passaporte.

15.3 Verificação de Sanções

Todo o pessoal do Fornecedor que realiza trabalho em nome do Citi ou de um proprietário com participação de 25% ou mais em um Fornecedor do Citi, incluindo Subcontratados, independentemente do acesso aos dados/sistemas/redes do Citi E/OU acesso às instalações do Citi, deve ser analisado com base na lista de Cidadãos Especialmente Designados e Pessoas Bloqueadas (a “Lista SDN”) do Office of Foreign Assets Control (“OFAC”) do Departamento do Tesouro dos Estados Unidos e na lista de regiões e jurisdições sujeitas a sanções impostas pelos Estados Unidos (“Sanções dos EUA”), bem como em relação a qualquer lista emitida e aos nomes de jurisdições sujeitas a sanções impostas por autoridades fora dos Estados Unidos, incluindo a Lista Consolidada de Sanções Financeiras da União Europeia (UE), à Lista Consolidada do Conselho de Segurança das Nações Unidas (ONU), a Lista de Sanções do Reino Unido (RU) e às listas em conformidade com as leis e regulamentos aplicáveis à jurisdição local (“Sanções não Relacionadas aos EUA”).

As listas do OFAC estão disponíveis publicamente neste site: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Compliance com a Imigração

O Fornecedor deve demonstrar que mantém e implementa protocolos para verificar se todo o pessoal está autorizado a trabalhar nos países de atribuição. Além disso, o Fornecedor deve: (1) garantir que todo o pessoal esteja autorizado a trabalhar e (2) cumprir todas as leis, regulamentos e políticas aplicáveis (incluindo requisitos de qualificação e verificação de emprego). O Fornecedor deve ainda demonstrar e manter protocolos para assegurar que seu pessoal cumpre todas as leis e regulamentos de imigração aplicáveis e tem o status/classificação apropriada de visto para as atribuições e atividades nas quais eles estão envolvidos.

15.5 Histórico Profissional

Os Fornecedores devem confirmar o histórico profissional de seu pessoal dos últimos sete (7) ou 10 anos, se exigido por regulamento local. O histórico profissional da pessoa deve ser confirmado para garantir que empregadores, cargos, datas e obrigações foram descritos com precisão. O pessoal do Fornecedor também deve divulgar qualquer emprego ou atribuição prévia como consultor ou trabalhador temporário no Citi ou qualquer de suas empresas predecessoras (incluindo, entre outros: Citibank, Citicorp, Travelers, Salomon Brothers e/ou Smith Barney).

15.6 Histórico Escolar

Os Fornecedores devem confirmar o nível mais alto de formação concluído por seu pessoal. As informações confirmadas devem incluir as datas de participação, nomes das instituições, endereços e graduações obtidas.

15.7 Antecedentes Criminais

Onde for legalmente permitido, os funcionários dos Fornecedores e subcontratados devem divulgar ao Citi se estiverem sujeitos a prisão, citação, intimação, audiência preliminar, denúncia ou condenação por qualquer crime, incluindo confissão judicial ou confissão judicial sem efeitos civis e qualquer participação em uma suspensão condicional do processo ou programa similar. A análise administrativa de registros criminais e/ou verificações de impressões digitais deve ser concluída antes da data de início da tarefa, onde for permitido legalmente e estiver disponível. Condenações criminais por infrações relacionadas a roubo, fraude, desonestidade ou a violações de confiança ou crimes semelhantes definidos de forma diferente na legislação local, exceto onde proibido por lei, podem resultar em recusa e/ou desqualificação para a tarefa com o Citi. Outras condenações podem resultar em recusa e/ou desqualificação para a tarefa com base nas leis e regulamentos locais aplicáveis.

15.8 Novo Exame

Os Funcionários do Fornecedor cuja atribuição termina devem passar por novo exame no caso de serem designados novamente ao Citi. Para obter informações adicionais sobre exigências de novo exame, consulte https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Transferências Internacionais

Todo exame deve ser feito de acordo com os regulamentos do país em que a atribuição da tarefa está localizada. Se um funcionário do Fornecedor for transferido para um novo país, a pessoa deve ser examinada novamente de acordo com as exigências do novo país.

16 DESPESAS

Fornecedores que são contratualmente qualificados para reivindicar despesas comerciais reembolsáveis.

16.1 Visão Geral

O Citi reembolsará apenas despesas de negócios razoáveis que tenham sido aprovadas previamente por escrito pelo Citi e tenham sido incorridas pelo Fornecedor em conexão com a provisão de produtos e serviços para o Citi e estejam de acordo com os termos

do Contrato ou Política de Governança de Despesas Operacionais do Citi aplicável e suas Normas e Procedimentos, quando apropriado, e sejam adequadamente comprovadas por meio de recibos, faturas, itinerários ou outras formas de documentação, conforme considerado aceitável pelo Citi.

16.2 Reembolsos

Essas despesas devem ser documentadas e faturadas para o Citi de maneira adequada de acordo com as exigências de faturamento do Citi. Despesas de Fornecedor não podem ser incorridas por um funcionário do Citi em nome de um Fornecedor. Qualquer despesa enviada ao Citi para reembolso de itens de despesas válidos e aprovados deve incluir (além de todos os outros requisitos de faturamento):

1. O objetivo comercial da despesa;
2. O valor e a descrição da despesa;
3. O local e a data da despesa;
4. O nome/descrição do projeto para o qual o fornecedor está fornecendo serviços;
5. O nome e o relacionamento comercial do representante do Citi que solicita os serviços para os quais tais despesas foram incorridas; e
6. Número do Pedido de Compra, se aplicável.

Para obter informações sobre despesas de negócios reembolsáveis permitidas, fale com seu contato de negócios principal do Citi. Recibos, faturas, itinerários ou outras formas de documentação comprobatória consideradas aceitáveis pelo Citi devem ser enviadas com o pedido de reembolso. As solicitações de reembolso devem estar em conformidade com as disposições do Contrato aplicável ou com a Política de Governança de Despesas Operacionais do Citi e suas Normas e Procedimentos relevantes, quando apropriado, aprovadas pelo patrocinador de negócios apropriado e/ou contato de negócios principal do Citi e aprovadas por um indivíduo devidamente autorizado e com valor suficiente para a commodity correspondente. Não serão reembolsados pedidos fora de compliance.

17 SEGURANÇA DA INFORMAÇÃO (IS)

Aplicável a Fornecedores, incluindo Subcontratados, que acessam, processam, armazenam ou gerenciam quaisquer Informações do Citi conforme classificadas e definidas no Apêndice; ou Hospedam aplicativos que usam a Internet da marca do Citi; ou têm conectividade com os recursos de rede do Citi; ou requerem acesso sem acompanhamento às instalações do Citi.

17.1 Visão Geral

Esta seção fornece exigências mínimas para os Fornecedores do Citi, incluindo fornecedores e subprocessadores ou subcontratados que armazenam, processam, gerenciam ou acessam Informações do Citi ou hospedam aplicativos do Citi ou que têm conectividade de rede com o Citi, com relação aos controles de proteção da informação que são esperados pelo Citi. Essas exigências garantem que as informações sejam protegidas de acordo com as exigências legais e regulatórias aplicáveis e os mais altos padrões do setor (por exemplo, ISO/IEC 27001/2) nos locais em que o Citi e seus

Fornecedores fazem negócios. Se as leis ou regulamentos locais ou normas relevantes do setor estabelecerem um padrão mais alto do que o fornecido aqui, os Fornecedores devem cumprir tais leis, regulamentos ou normas. Além disso, pode ser exigido que os Fornecedores incorporem práticas e procedimentos de segurança da informação adicionais como parte do compliance deles com outras políticas do Citi e termos e condições contratuais. Se um Fornecedor decidir implementar práticas de segurança ou procedimentos adicionais para segurança da informação, o Fornecedor deverá garantir que essas práticas e procedimentos não entrem em conflito com os controles mínimos definidos nesta seção.

17.2 Política e Governança de Segurança da Informação

Os fornecedores devem ter documentado as políticas e normas de segurança da informação. A governança de políticas deve incluir funções e responsabilidades claramente definidas e revisão/atualização anual de políticas e normas para consistência com o estado atual da tecnologia, normas do setor, requisitos legais e regulatórios.

17.3 Segregação de Funções

Os fornecedores devem ter processos implementados para garantir que nenhuma pessoa possa realizar duas funções de negócio ou duas funções de TI nem duas funções do Sistema de Informações Controladas com acesso contínuo para a mesma atividade, mudança, Sistema de Informação ou transação sem autorização ou detecção, a menos que controles adequados de compensação estejam presentes para mitigar o risco.

Tabela A

Funções	Descrição da Função
Desenvolvimento/Engenharia	Projetar, criar ou modificar software, hardware e configurações; exemplos podem incluir: - Projetar e criar novo código do aplicativo e esquemas de banco de dados relacionados - Projetar produtos de infraestrutura e componentes de aplicativos - Personalizar produtos de tecnologia para integrar com software e serviços
Aprovação	Aprovar a promoção de mudanças de código a serem implementadas
Implementação/administração de sistemas	Instalar, implementar ou administrar mudanças de software, hardware e configuração. Exemplos podem incluir: - Realizar a liberação de código, de forma automatizada ou manual, para a infraestrutura de produção - Instalar um produto ou aparelho de tecnologia

	- Iniciar ou interromper serviços para apoiar a solução de problemas e correção de sistemas com dados de produção
Revisão da Atividade de ID Privilegiada	Verificação da atividade de gestão de mudanças ou eventos de sistemas relacionados a segurança (por exemplo, trilhas de auditoria)
Administração de IDs	Adicionar, modificar e excluir IDs (Usuário, FIDs e Bots), direitos ou senhas
Função de Negócios	Descrição da Função
Iniciar Transação Comercial	Iniciar (também conhecido como inserir, realizar ou criar) transações comerciais e alterar informações de clientes
Aprovar Transação Comercial	Aprovar (também conhecido como autorizar ou verificar ou liberar) transações comerciais
Função de IT	Descrição da Função
Operações de Rede	Gestão de dispositivos e suporte operacional de produtos que fornecem serviços de infraestrutura de rede. Roteadores de rede, switches, Firewalls e Domain Name Services (DNS) são exemplos
Operações Fora da Rede	Gestão de dispositivos e suporte operacional de produtos que não fornecem serviços de infraestrutura de rede. Servidores, telefones e computadores são exemplos

17.4 Compromisso da Administração com a Segurança da Informação

Os Fornecedores que hospedam um aplicativo que utiliza a Internet com marca Citi e/ou têm acesso a Informações do Citi com classificação de Confidencial ou acima, estão sujeitos ao Processo de Avaliação de Segurança da Informação de Terceiros (Third Party Information Security Assessment, TPISA) do Citi para avaliação das políticas, procedimentos e controles do Fornecedor relativamente ao compliance com as exigências do Citi e quaisquer exigências legais e/ou regulatórias (aplicáveis ao Citi ou ao Fornecedor) que dizem respeito à segurança da informação.

A avaliação consiste em questionários de segurança que exigem respostas do Fornecedor com evidências comprobatórias e pode incluir visitas aos locais do Fornecedor onde as Informações Confidenciais ou acima do Citi são armazenadas, processadas, gerenciadas ou acessadas por terceiros. Além disso, a Equipe de Monitoramento Contínuo de Terceiros da TPISA pode monitorar o Fornecedor usando ferramentas de monitoramento de Segurança Cibernética que utilizam informações publicamente disponíveis para identificar sistemas, hosts, aplicativos e servidores vulneráveis baseados na Internet para coisas como software em fim de vida, portas abertas exploradas, vulnerabilidades ou outros comprometimentos. Se as descobertas de um TPISA revelarem ou indicarem deficiências de segurança, o Citi documentará as descobertas em um aviso para o Fornecedor e trabalhará com o Fornecedor para identificar meios de corrigir as deficiências. Os Fornecedores devem fazer rapidamente as correções necessárias e/ou controles compensatórios para abordar as preocupações do Citi a exclusivo critério do Citi e cumprir os prazos exigidos de 180 dias corridos para problemas de Alto Risco, 240 dias corridos para problemas de Risco Médio e antes da próxima data de compliance para problemas de Baixo Risco, já que esses problemas são classificados como risco pelo Citi.

1. O Fornecedor deve realizar com regularidade avaliações de suas operações de negócios e controles relacionados em comparação às suas próprias normas, políticas e procedimentos de segurança da informação. As avaliações periódicas devem incluir, no mínimo:
 - a) Avaliação dos processos que o Fornecedor usa para garantir compliance com a própria política e normas de IS do Fornecedor;
 - b) Avaliação dos recursos de apoio, como aplicativos e infraestrutura usada pelo Fornecedor e processos de IS usados pelos subcontratados do Fornecedor (se aplicável) que apoiam suas operações comerciais, ou permitir que o Citi realize essas avaliações. É exigida conformidade quando um terceiro assina um novo contrato ou renova um contrato existente com um subcontratado que acessa, processa, gerencia ou descarta informações do Citi classificadas pelo Citi como Confidenciais ou acima.
2. Os problemas que forem identificados como resultado de qualquer Avaliação de Risco da Segurança da Informação (por exemplo, TPISA), devem ser documentados e acompanhados até a conclusão com evidência de remediação fornecida ao Citi.
3. Se a função de Gestão de Segurança da Informação do Fornecedor for realocada para além das fronteiras do país, o Fornecedor deve obter aprovação documentada do Citi para essa realocação.
4. Se o Fornecedor adquirir uma nova entidade, deve completar uma avaliação da entidade adquirida para compliance com essas Normas.
5. O Fornecedor não deve terceirizar as funções de gestão de segurança incluindo, entre outros, gestão de firewall, de configuração de segurança, de patch ou funções de Administração da Segurança da Informação (Information Security Administration, ISA), nos sistemas usados para armazenar, processar e/ou transmitir informações do Citi, a menos que tenha sido previamente aprovado por escrito pelo Citi.

6. Se o Fornecedor hospeda um software ou site que contém Informações do Citi ou tem a marca do Citi, avaliações de vulnerabilidade periódicas devem ser realizadas de acordo com o System Security Testing Standard (SSTS) do Citi e quaisquer questões relevantes identificadas durante a avaliação devem ser corrigidas dentro dos prazos especificados nesse Padrão. Como a SSTS não é aprovada para distribuição externa, os Fornecedores devem trabalhar com seu Gerente de Relacionamento do Citi para garantir compliance com a documentação de referência. Além disso, o Fornecedor deve cumprir as normas relevantes de gestão de Segurança da Informação ISO/IEC 27001 (ou normas sucessoras de gestão de segurança da informação que estabeleçam padrões e protocolos mais altos) e cumprir as disposições de segurança da informação contidas nesta Seção (17).
7. Se for necessária conectividade com servidores e/ou Sistemas de Informação na rede interna do Citi, o Fornecedor deve notificar o contato de negócios principal dele no Citi, de modo que o processo de provisionamento de conectividade atual possa ser seguido.
8. O fornecedor deve notificar imediatamente o contato apropriado do Citi (Business Activity Owner ([BAO])) sobre qualquer acesso, aquisição, perda, corrupção ou exclusão não autorizada de Informações do Citi ou qualquer outro comprometimento dos Sistemas de Informação usados para armazenar, processar ou transmitir Informações do Citi.
9. O Fornecedor deve garantir que toda atividade de alto risco ou alterações a dados sigilosos tenham trilhas de auditoria que possibilitem atribuir essas ações aos indivíduos que as realizaram.
10. O Fornecedor deve garantir que dados confidenciais ou acima sejam mascarados na tela e em documentos impressos, incluindo, por exemplo, relatórios de monitoramento, de exceção e regulatórios e outros relatórios.
11. O Fornecedor deve limitar a impressão, registro e cópia de dados sigilosos, inclusive pelos seus dispositivos próprios. O Fornecedor deve devolver ou destruir todas as informações do Citi em um momento acordado durante ou no final do contrato, a menos que seja proibido por lei ou regulamento.
12. O Fornecedor deve garantir que todo o pessoal do fornecedor (funcionários, contratados, temporários, subcontratados) com acesso às informações do Citi assine um acordo de não divulgação ou confidencialidade.
13. Os funcionários do Fornecedor devem receber um manual do funcionário ou documento semelhante que contenha processo disciplinar por não conformidade no que se refere a violações do código de conduta do Fornecedor e das políticas de recursos humanos que devem ser reconhecidos como parte de seu processo de integração.
14. O Fornecedor tem um processo implementado para recuperar todos os ativos quando um funcionário ou não funcionário é demitido ou pede demissão.
15. Se quaisquer Informações Confidenciais forem mantidas ou armazenadas de qualquer forma em um site ou sistema acessível pela web, o Fornecedor deve divulgar essas informações ao Citi. Essa divulgação pode ser incluída na descrição dos Serviços. Se o Fornecedor mantiver ou armazenar Informações Confidenciais do Citi, o Fornecedor fará com que uma auditoria SSAE 18 (ou qualquer avaliação oficial sucessora aprovada pelo Citi) seja realizada uma vez por ano durante a vigência deste Contrato e fornecerá ao Citi, no mínimo uma

vez por ano, uma cópia dos relatórios documentando os resultados dessa auditoria SSAE 18 ou qualquer avaliação oficial sucessora aprovada pelo Citi.

16. Se o Fornecedor for adquirido ou adquirir outra entidade em qualquer fusão ou aquisição ou transação semelhante, e essa transação puder afetar os Serviços, o Fornecedor deverá notificar imediatamente o Citi por escrito e o Fornecedor deverá realizar uma avaliação de segurança da informação na entidade resultante em consonância com estas Exigências para garantir que a aquisição ou fusão não afete o cumprimento das Exigências.

17.5 Risco de Segurança da Informação do Subcontratado

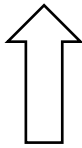
O Fornecedor deve exigir que os subcontratados com acesso a dados confidenciais ou acima do Citi sejam submetidos a avaliações de Segurança da Informação (IS) pré-contrato e pós-contrato periódicas realizadas por pessoal qualificado de Segurança da Informação. Essas avaliações devem ser feitas de acordo com um processo aprovado pela administração que aborde todas as etapas do processo de avaliação desde o início até a gestão de pontos de auditoria. A avaliação de IS do subcontratado deve utilizar um questionário ou ferramenta equivalente que avalie a postura do subcontratado nos domínios de IS que se alinham com aqueles incluídos no Questionário de Avaliação de IS de Terceiros (TPAQ) do Citi e deve incluir um método lógico para calcular o risco de IS associado ao envolvimento do subcontratado. O Fornecedor deve monitorar a conclusão da avaliação e gerenciar os pontos de auditoria observados e os planos de ação corretiva para o encerramento.

17.6 Responsabilidade pelos Ativos

1. O Fornecedor deve garantir a manutenção de um inventário de todos os aplicativos e hardware sob seu controle que são usados para armazenar, processar e/ou transmitir Informações do Citi.
2. O Fornecedor deve garantir que um inventário de ativos de Informação do Citi seja mantido sob seu controle de acordo com um processo usado para manter adequadamente a precisão e a completude desse inventário.
3. O Fornecedor deve ser responsável por proteger todas as Informações do Citi sob seu controle.
4. O Fornecedor deve garantir a responsabilidade pela atividade de seus usuários de maneira consistente com as práticas do setor.
5. O acesso dos usuários a contas externas pessoais de armazenamento de e-mail na Internet e armazenamento em nuvem deve ser restrito na rede global do fornecedor onde as Informações do Citi residem.

17.7 Classificação e Manuseio de Informações.

O Citi classifica as informações de acordo com a tabela de Classificação de Informações seguinte: Consulte o Apêndice para definições e exemplos de cada classificação de informação listada abaixo.

RESTRITAS	Mais Sigilosas
PII SIGILOSA	
PII CONFIDENCIAL	
CONFIDENCIAIS	
PII INTERNA	
INTERNAS	
PÚBLICAS	Menos Sigilosas

1. Com base na classificação de Informações do Citi, o Citi deve trabalhar com o Fornecedor para especificar o nível de segurança necessário para proteger tais informações, e o Fornecedor deve garantir que controles suficientes estão implementados, em conjunto com qualquer nível intensificado ou modificado que o Citi pode exigir.
2. Informações com classificação de internas ou acima devem ser armazenadas em dispositivos gerenciados por terceiros que estão sujeitos a um contrato entre o Terceiro e o Citi que contém cláusulas de confidencialidade consistentes com as políticas e normas do Citi.
3. Se o Fornecedor permitir o uso de dispositivos não pertencentes à empresa para armazenar dados do Citi (ou seja, dispositivos gerenciados por uma quarta parte), o Fornecedor precisa ter uma política em vigor que exija aprovação específica da administração, bem como diretrizes e procedimentos de monitoramento específicos para uso e descarte de Informações do Citi.
4. O Fornecedor sempre deve proteger as Informações do Citi contra acesso, modificação ou exclusão não autorizada.
5. As Informações do Citi classificadas como Confidenciais ou acima transferidas por meio de Mídia Eletrônica Transportável (Electronic Transportable Media, ETM) devem ser criptografadas usando um algoritmo de criptografia aprovado, e a entrega deve ser confirmada. O Fornecedor deve confirmar que a ETM foi recebida pelo pretendido. Se a confirmação de recebimento não for recebida até a data esperada de entrega, o Fornecedor deverá notificar o Citi.

17.8 Configuração Segura

1. O Fornecedor deve manter um padrão de configuração seguro documentado para todos os ativos com potencial para armazenar, processar, acessar ou transmitir Informações do Citi.
2. O Fornecedor deve incorporar controles de segurança da informação em seus processos e procedimentos para a seleção, desenvolvimento e implementação de aplicativos, produtos e serviços.
3. O Fornecedor deve ter um procedimento de compilação segura para todos os sistemas onde as Informações do Citi são armazenadas, processadas e/ou transmitidas.
4. O fornecedor deve manter uma imagem ou modelo seguro para todos os sistemas.
5. Todas as contas de usuário e senhas padrão devem ser removidas e/ou alteradas dos sistemas, dispositivos de rede e aplicativos que contam com suporte do fornecedor.

6. Qualquer sistema ou serviço que tenha sido comprometido deve ser reconstruído e configurado usando uma imagem ou modelo que tenha integridade comprovada.
7. Qualquer mudança a ser feita em uma configuração segura deve ser aprovada pela administração por meio de um processo de gestão de mudanças do Fornecedor.
8. O Fornecedor deve notificar o Citi sobre quaisquer alterações na configuração segura.
9. O procedimento de compilação seguro deve incluir ferramentas para apoiar verificações de configuração automatizada das configurações de compilação de segurança/padrão no momento da implantação da produção e monitoramento contínuo para compliance e desvios da configuração de linha de base.

17.9 Requisitos de Criptografia

O Fornecedor não deve transmitir informações classificadas como Confidenciais ou acima sem criptografia. Informações classificadas como Confidenciais ou acima devem ser criptografadas **ponta a ponta** com ferramentas ou soluções aprovadas pelo Citi. Os protocolos aprovados e os respectivos números de versão para a transmissão criptografada de dados são os seguintes:

1. Em trocas de informações de autenticação e autorização: SAML v2.0, OAuth v2.0 (somente autorização),
2. Para proteger os canais de comunicação e a troca de chaves associada, somente os seguintes Protocolos de Segurança da Rede são permitidos:
 - a) TLS v1.3 é o preferido e todos os pacotes TLS v1.3 são permitidos. Se o TLS v1.3 for o único protocolo habilitado, nenhuma revisão adicional é necessária.
 - b) Se o TLS v1.3 não for viável do ponto de vista técnico e o TLS 1.2 for utilizado, atualmente uma nota B ou superior do SSLabs é aceitável, não sendo necessária nenhuma análise adicional.

Os dados armazenados de forma persistente no ambiente de Terceiros do Citi ou quando trocados devem ser totalmente criptografados usando ferramentas ou soluções aprovadas pelo Citi. Os algoritmos e tamanhos de chave aprovados para criptografar dados são os seguintes:

1. **Advanced Encryption Standard (AES):** Tamanhos de chave aprovados: 256 ou mais bits. Modos Restritos: O modo Electronic Codebook (ECB) é proibido, exceto quando a quantidade de texto simples for menor ou igual ao tamanho do bloco. Criptografia da unidade de disco: AES com chave de 256 bits é recomendado. O AES com chave de 128 bits é permitido como opção de TLS Cupher; no entanto, essa opção deixará de ser permitida em favor de níveis de segurança de 256 bits ou superiores até 31 de dezembro de 2028 para viabilizar o alinhamento do Citi com cronogramas internacionais (Ref.: NIST 8547 IPD).
2. **ChaCha20 (uma criptografia de fluxo para casos de uso associados):** Tamanhos de chave aprovados: 128 ou 256 bits, com nonce de 96 bits e

contagem de blocos de 32 bits ou nonce de 64 bits e contagem de blocos de 64 bits. Tamanho máximo dos dados: 16 petabytes.

Os criptossistemas de chave pública, troca de chaves, mecanismos de acordo, resumo de mensagem e funções de derivação de chave aprovados são os seguintes:

Comunicado Referente à Prontidão do Fornecedor para Computação Quântica: Os Fornecedores devem apresentar seu plano de cobertura da *tabela 2* e *tabela 4* do NIST IR 8547 (ipd) à equipe do Programa de Prontidão para Computação Quântica do Citi por meio de ([survey link](#)).

1. **Criptossistemas de Chave Pública e tamanhos mínimos de chave:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 bits.
 - b) Algoritmo de Assinatura Digital (DSA): 2048 bits. O DSA não deve ser usado para proteger dados do Citi processados ou armazenados fora do Citi.
 - c) Elliptic Curve Digital Signature Algorithm (ECDSA): 256 bits e conforme especificado no ANSI X9.62 com curvas recomendadas pelo NIST.
2. **Mecanismos de Acordo e Troca de Chaves e tamanhos mínimos de chave:**
 - a) Diffie-Hellman (DH)/Ephemeral Diffie-Hellman (DHE): 2048 bits.
 - b) Elliptic-curve Diffie–Hellman (ECDH) /Ephemeral Elliptic-curve Diffie–Hellman (ECDHE): 256 bits e conforme especificado no ANSI X9.63 com curvas recomendadas pelo NIST¹.
3. **Funções de Compreensão de Mensagens:** É proibido criar uma chave de criptografia de tamanho maior que o número de bits aleatórios no material usado para gerar o hash.
 - a) SHA-1 Aceitável apenas para aplicativos de assinatura não digital. Família SHA-2, família SHA-3 e POLY-1305: Aceitável para todos os aplicativos de função hash criptográfica.
4. **Funções de Derivação de Chave baseadas em senha e requisitos mínimos:**
 - a) PBKDF2 Contagem mínima de iteração de 10.000 com pelo menos 16 bytes salt.
 - b) HKDF: Deve ter salt, e o valor de entrada de informações deve ser incluído.
 - c) SCRYPT: Número mínimo de rodadas/fator de custo de 10.
 - d) O uso do NIST SP800-108 KDF para Criptografia de Fluxo é proibido. Os modos NIST SP 800-108 KDF, ou seja, Iteração de Contador, Feedback e Duplo Pipeline, são aceitáveis.
 - e) Argon2 é recomendado.
5. **Funções de hash de senha e requisitos mínimos:**
 - a) Bcrypt (para armazenamento local de material de autenticação): Número mínimo de rodadas/fator de custo de pelo menos 10.
 - b) Argon2 ou PBKDF2 são recomendados para hash de senha ao armazenar senhas localmente em qualquer ambiente ou sistema implantado de produto do Fornecedor.

¹ ECDHE é a preferência.

17.10 E-mail Externo

O requisito de criptografia para e-mails individuais contendo Informações do Citi classificadas pelo Citi como confidenciais ou de classificação mais alta, em que o fornecedor não tem permissão de usar ferramentas ou software de criptografia de ponta a ponta aprovados pelo Citi conforme regulamento e/ou política do Fornecedor, pode ser cumprido ainda através de criptografia de transporte [por ex., criptografia gateway a gateway por meio da segurança da camada de transporte (Transport Layer Security, TLS)]. Os protocolos de e-mail seguros aprovados são:

1. **Identify-Based Encryption (IBE)** dispõe de e-mail criptografado e pode ser usada em soluções voltadas para o cliente do Citi e sistemas seguros de e-mail e entrega eletrônica.
2. **Mandatory TLS (MTLS)** dispõe de criptografia de sessão (não criptografa carga útil de e-mail) e pode ser usado com fornecedores, parceiros e clientes que têm acordos pré-negociados para seu uso.
3. **Domain Keys Identified Mail (DKIM)** dispõe de autenticação de fonte e gestão de chave e pode ser usado com fornecedores, parceiros e clientes.

17.11 Redes Privadas

Redes privadas que são regulamentadas independentemente por uma autoridade reconhecida e que atendem normas do Setor de Serviços Financeiros para efetuar transações entre partes licenciadas ou credenciadas (por exemplo, a SWIFT ou um banco central) podem ser consideradas isentas do requisito de criptografia em trânsito de PII Confidenciais até que essas redes forneçam a infraestrutura necessária para compatibilidade completa com transmissões criptografadas.

17.12 Chamadas de Voz e Fax

Informações com uma classificação do Citi de Confidenciais ou acima enviadas por fax ou discutidas em chamadas de voz (incluindo VOIP) podem ser enviadas sem criptografia. Quando necessário, o Fornecedor deve desenvolver procedimentos e orientações específicos para proteger informações classificadas como Confidenciais ou acima enviadas por meio desses canais.

17.13 Gestão de Chaves e Certificados de Criptografia

O termo limite seguro usado nesta seção refere-se a um Programa de Validação de Módulo Criptográfico (CMVP), como o Federal Information Protection Standard (FIPS), limite validado (FIPS 140-2/3 Nível 2 é o nível de segurança mínimo aceitável). (Enclaves de Computação Confidenciais, como AWS Nitro Enclaves, são aceitáveis. Outros casos exclusivos de limite de segurança devem ser aprovados pelo Citi).

1. O fornecedor deve implementar algoritmos criptográficos atuais padrão do setor e os comprimentos mínimos de chave para criptografia e assinatura (incluindo chaves SSH). O fornecedor deve fornecer garantia por meio de seu Processo de Gestão de Mudanças quando esses algoritmos e tamanhos de chave são atualizados para se alinhar com os padrões do setor.
2. O Fornecedor deve ter um processo de ciclo de vida de gestão de chaves documentado formalmente com controles implementados para proteger material sigiloso contra uso ou exposição não autorizados. Todos os

segredos criptográficos e principais eventos do ciclo de vida devem ocorrer apenas dentro de um limite seguro. Todo o acesso a limites privilegiados e seguros deve ser documentado. O Fornecedor deve fornecer um diagrama de sequência para todos os principais eventos do ciclo de vida destacando os atores, entidades e limites envolvidos.

3. As chaves criptográficas devem ter uma finalidade exclusiva e nunca devem ser usadas para nenhuma outra finalidade, como usar a mesma chave de criptografia para criptografia de disco e criptografia de dados ou a mesma chave de criptografia para criptografia de carga útil e criptografia de banco de dados. A reutilização de chaves criptográficas entre vários *tenants* por um fornecedor SaaS é proibida por padrão e pode ser permitida apenas para casos de uso não críticos e de baixo risco envolvendo informações do Citi classificadas abaixo de PII Confidenciais, PII Sigilosas e Restritas, sujeitos à aprovação explícita do Conselho de Arquitetura de Segurança.
4. Para todas as chaves criptográficas (simétricas ou assimétricas), a chave privada ou material de chave privada (como sementes ou parte de uma chave privada) não deve ser exibida em texto não criptografado em nenhum momento. Chave privada ou material de chave privada (como semente ou parte de uma chave privada) nunca deve sair do limite seguro, com a exceção de chaves efêmeras, como chaves de sessão dinâmica. Se o projeto exigir que uma chave simétrica ou uma chave privada ou material de chave privada seja transmitido entre enclaves seguros/limites de acesso privilegiado, deve ser transmitido de forma criptografada usando apenas uma Chave de Encapsulamento de Chave Simétrica ou Chave de Transporte de Chave Pública somente por meio de túneis criptografados TLS mútuos, e essa transmissão deve ser aprovada pelo Citi por escrito. Nesses casos, a Chave de Transporte de Chave Privada nunca deve sair do limite seguro de acesso privilegiado onde foi gerada.
5. A Chave de Encapsulamento de Chave Simétrica deve ser dividida em dois ou mais componentes de chave e passar por XOR antes de distribuir e para entrada/carregamento manual de chave. A Chave de Encapsulamento de Chave Simétrica deve ter Listas de Controle de Acesso (ACLs) adequadas associadas dentro do limite seguro, como módulos validados pelo CMVP e a Chave de Encapsulamento de Chave Simétrica não deve ser armazenada fora do limite seguro.
6. O acesso humano ou agente de serviço ou automatizado a keystores ou limites seguros contendo chaves privadas ou segredos ou material de chaves privadas (como sementes ou parte de uma chave privada) deve ser devidamente segregado com controles que limitem o acesso apenas a pessoal ou sistemas autorizados.
7. Toda solicitação de acesso aos keystores contendo chaves privadas ou simétricas deve ser registrada e documentada com detalhes como quem, quando e a finalidade do acesso para fins de auditoria.
8. O fornecedor não deve usar certificados autoassinados e curinga ou certificados SSL padrão.
9. Todas as chaves criptográficas devem ter um intervalo de tempo de criptografia definido conforme sugerido no NIST SP800-57 parte 1, revisão 6. As chaves devem ser atualizadas ou rotacionadas antes da expiração para

acomodar períodos de mudança, conflitos de agendamento e congelamentos do sistema.

a) Ao substituir um certificado vencido, é proibido o uso do antigo par de chaves assimétricas.

10. As chaves criptográficas devem ser tratadas como comprometidas assim que for estabelecida uma suspeita de comprometimento da integridade da chave, do meio em que a chave é armazenada ou compartilhada ou da confidencialidade da chave simétrica ou privada. Todas as chaves comprometidas devem ser removidas do uso operacional e todos os certificados correspondentes devem ser revogados.
11. Redes sem fio devem ser criptografadas com algoritmos criptográficos padrão do setor.
12. Fornecedores utilizando qualquer forma de mecanismo criptográfico devem usar ferramentas e técnicas de gestão de chaves padrão do setor. A função principal de gestão de chaves deve ser segregada da gestão operacional.
13. Os fornecedores podem utilizar serviços de KMS e PKI nativos da nuvem apenas quando a interoperabilidade com os serviços de PKI e KMS provisionados pelos Serviços de Segurança de Dados do Citi estiver assegurada e o controle criptográfico não for delegado para fora da governança criptográfica do Citi.

17.14 Responsabilidade pelo Controle de Acesso

Para proteger todos os Sistemas de Informações Controladas usados para armazenar, acessar, gerenciar, processar ou transmitir Informações Confidenciais ou acima do Citi contra acesso não autorizado, o Fornecedor é responsável por aplicar o princípio de privilégio mínimo, limitando os direitos do usuário ao nível mínimo de acesso necessário para cada função de trabalho e gerenciando o fornecimento de acesso lógico a todos os sistemas e aplicativos. Os controles devem ser totalmente documentados e auditáveis. O provisionamento e desprovisionamento de acesso, incluindo redefinição e ativação de senhas, devem ser realizados por meio de um processo automatizado sempre que possível para garantir a mitigação de riscos associados a possíveis erros humanos causados por excesso de direitos e para alinhamento com os padrões do setor.

1. O fornecedor é responsável pelos direitos de acesso de todos os usuários em sua organização.
2. O fornecedor deve implementar controles de acesso que garantam que os usuários recebam somente os privilégios e direitos estritamente necessários para executar suas respectivas funções.
3. O Fornecedor deve implementar um processo para garantir que todas as capacidades de acesso padrão sejam removidas, desabilitadas ou protegidas para impedir o uso não autorizado.

17.15 Gestão de Acesso do Usuário

O Fornecedor deve gerenciar o fornecimento de acesso lógico a sistemas e aplicativos que processam, armazenam e/ou transmitem informações classificadas como Confidenciais ou acima do Citi. Isso inclui:

1. Identificação e inventário de sistemas de autenticação aprovados.
2. Exigência de que todo acesso aos dados do Citi requeira a aprovação de um gerente ou representante do gerente e do proprietário do sistema. O Fornecedor é responsável por garantir que qualquer um de seus funcionários com acesso aos dados do Citi receba esse acesso de acordo com a necessidade de conhecimento.
3. Exigência de que qualquer combinação de privilégios/funções para um usuário individual não possa ser fornecida se apresentar um conflito de interesses ou uma violação das regras do executante-verificador.
4. Um processo de monitoramento para supervisionar e gerenciar os direitos de acesso concedidos/revogados a cada usuário do sistema.
5. As solicitações de acesso não devem basear-se na replicação ou clonagem dos direitos de outro usuário; elas devem especificar funções ou direitos explícitos, acompanhados de justificativa de negócio, para evitar a expansão indevida de privilégios e garantir a aplicação do princípio do privilégio mínimo.

17.16 Identificação e Autenticação de Usuários

Todos os sistemas de informações controladas do fornecedor devem autenticar a identidade dos usuários ou sistemas que acessarem essas plataformas antes de iniciar uma sessão ou transação nas quais as informações do Citi podem ser acessadas.

1. Os usuários precisam ser exclusivamente identificados ou mapeados para a plataforma tecnológica por uma ID de Usuário.
2. Os usuários devem ser autenticados na plataforma de tecnologia usando um método de autenticação aprovado. O fornecedor deve entrar em contato com seu contato comercial principal (BAO) para obter os métodos aprovados atuais.
3. O uso de infraestrutura de autenticação compartilhada [por exemplo, Single Sign-On (logon único), Reduced Sign-On, e outros serviços de autenticação compartilhados) deve estar de acordo com os requisitos de autenticação do Citi; o Fornecedor deve entrar em contato com seu BAO principal para obter os métodos aprovados atuais.
4. Os Dados de Verificação de Identidade (IVD) que são usados para autenticar um usuário em um Sistema de Informação devem ser criptografados na transmissão e armazenamento. Consulte a seção 17.9 sobre os requisitos de criptografia.
5. Todas as contas utilizadas pelo pessoal do Fornecedor para acessar os sistemas do Citi devem estar vinculadas a um identificador exclusivo atribuído pelo Citi (por exemplo, GEID); IDs de usuário genéricos/compartilhados para usuários humanos são proibidos para garantir a rastreabilidade, aplicação de SOD e a prontidão para auditoria.

17.17 Identificação de Acesso Privilegiado e Acesso Privilegiado Temporário

O Fornecedor deve manter um inventário de todas as identidades e identificar aquelas que têm acesso privilegiado ou têm acesso a repositórios eletrônicos (conjuntos de dados ou bancos de dados que dão suporte para aplicativos comerciais) que contêm informações classificadas como PII Confidenciais ou Acima. O Fornecedor deve implementar controles que protejam contra o uso não autorizado dessas Identidades. Se um funcionário exigir acesso a uma ID privilegiada ou aos repositórios eletrônicos mencionados antes, o acesso deve ser concedido por meio de um processo temporário de gestão de acesso que:

1. Exija que o solicitante esteja em uma lista de usuários autorizados pré-aprovada ou obtenha uma aprovação no momento do uso.
2. Exige uma justificativa documentada em um tíquete de mudança/problema antes de o acesso ser concedido.
3. Inclui uma análise independente da atividade realizada com o acesso.
4. Inclui um processo para iniciar a revogação/remoção do acesso ao final do período de liberação de acesso temporário.
5. Permite acesso a produção e estabilização após implementação, como após um upgrade importante ou resolução de assistência/reparo, de modo que o acesso seja estendido por até sete (7) dias consecutivos.

17.18 Revisão dos Direitos de Acesso do Usuário

1. O Fornecedor deve implementar um processo documentado para revisar, verificar e excluir direitos de usuário desnecessários para os Sistemas de Informações Controladas usados para armazenar, processar, gerenciar e/ou transmitir informações do Citi pelo menos semestralmente.
2. Os usuários não devem rever ou aprovar os próprios direitos ou os direitos de uma pessoa que delegou a responsabilidade de revisão a eles.
3. Quando ocorre uma mudança de função de um funcionário de um Fornecedor que realiza trabalho para o Citi, o Fornecedor tem 14 dias corridos para realizar uma revisão de acesso e direitos e remover o acesso aos dados do Citi se não for mais necessário para sua nova função.

17.19 Procedimentos Seguros de Logon

1. IDs de logon de usuários bloqueadas devem ser habilitadas novamente por meio de um serviço de redefinição padrão do setor ou outra função autorizada. Um texto em banner, quando compatível com o sistema operacional ou aplicativo, deve ser exibido em todos os pontos de entrada da rede quando um usuário entra inicialmente ou é autenticado.

17.20 Sistema de Gestão de Senhas

1. As senhas fixas de usuários nunca devem ser exibidas na tela em texto não criptografado. A funcionalidade de ativação/desativação da visibilidade da senha está isenta deste requisito, desde que:
 - (1) A entrada de senha seja mascarada por padrão,
 - (2) A visibilidade da senha pode ser iniciada apenas por uma ação explícita do usuário;
 - (3) A senha é remascarada automaticamente dentro de no máximo 15 segundos após a ação do usuário ser descontinuada.

2. Senhas de IDs Funcionais com Privilégios não devem ser inseridas no código em texto não criptografado.
3. As senhas estáticas devem conter no mínimo oito (10) caracteres, que devem conter letras e números, e diferenciam maiúsculas de minúsculas. A diferenciação entre maiúsculas e minúsculas em senhas estáticas deve ser validada em cada ponto de autenticação. Senhas estáticas de IDs Funcionais (FID) devem conter no mínimo 15 caracteres nos aplicativos implementados após 31 de agosto de 2026.
4. Podem ser usados PINs como único método de autenticação para acessar os sistemas de informação apenas se os PINs forem necessários para satisfazer restrições dos dispositivos físicos (por exemplo, teclado, telefone, cartão inteligente).
5. Todas as senhas fixas devem ser modificadas a cada 90 dias corridos no mínimo.
6. Todas as senhas fixas devem ser bloqueadas após no máximo seis (6) tentativas de login consecutivas fracassadas ou seis (6) tentativas de redefinição de senha consecutivas. As senhas devem ser desbloqueadas por meio de uma função de administrador de ID ou desbloqueadas automaticamente após pelo menos 30 minutos.
7. Todos os sistemas de autenticação devem impor um controle de inatividade/não uso de login que não pode exceder 100 dias corridos. Se tecnicamente viável, os logins desativados podem ser habilitados novamente pelo usuário ou outra função autorizada.
8. O processo de autenticação deve garantir que a mesma senha não foi usada pelo menos nas últimas seis (6) mudanças.

17.21 Uso de Utilitários do Sistema

O fornecedor deve garantir que o uso de programas utilitários que podem substituir os controles de sistemas e aplicativos (por exemplo, inicialização de dispositivos periféricos) seja restrito e controlado.

17.22 Sessão Expirada

1. Login e nova autenticação devem ocorrer para todos os usuários de um Sistema de Informações Controladas usado para armazenar, processar e/ou transmitir informações do Citi.
2. Os usuários devem autenticar novamente depois de um período de inatividade que não excede 30 minutos. Atividade inclui qualquer entrada em um terminal (mouse, teclado, tela sensível ao toque etc.). Quando a imposição for providenciada pela proteção de tela protegida por senha, a imposição de Aplicativo/Single Sign-on não é necessária.

17.23 Rescisão do Acesso do Usuário

1. Após rescisão ou renúncia, o acesso do usuário ou direitos que podem permitir o acesso a dados classificados como Confidenciais ou acima do Citi, incluindo login do usuário para Desktop/Active Directory, Single Sign-On (SSO), e-mail, tokens de Senha Única (OTP) e acesso remoto, deve ser removido imediatamente.

2. Se um funcionário tiver acesso a sistemas pertencentes e administrados pelo Citi, o suporte do gerente de relacionamentos comerciais do Citi, BAO ou suporte ao BAO deve ser notificado imediatamente após a mudança de função ou rescisão desse funcionário para garantir que o gerente de negócios do Citi inicie a remoção do acesso para trabalhadores demitidos no fim do prazo de rescisão.
3. O Fornecedor tem um processo documentado em vigor para recuperar o acesso de todos os ativos de acordo com os prazos estabelecidos na seção 17.23.2 quando um funcionário ou não funcionário é demitido ou pede demissão.
4. Se alguma anomalia for descoberta pelo Fornecedor em relação a 17.23.1-17.23.3, o Fornecedor deve informar imediatamente o Gerente de Relacionamentos Comerciais do Citi, BAO ou suporte ao BAO, com uma justificativa e controles sólidos provisionados.

17.24 Acesso Remoto

O Fornecedor deve ter controles de acesso remoto implementados para proteger o acesso a redes que podem armazenar, processar ou transmitir dados Confidenciais ou acima do Citi, que incluem:

1. O acesso remoto a Sistemas de Informação usados para armazenar, processar e/ou transmitir informações do Citi deve ser protegido contra uso não autorizado.
2. Todos os notebooks e computadores de mesa gerenciados pelo Fornecedor e usados para armazenar, processar e/ou transmitir informações do Citi usando acesso remoto onde há armazenamento/processamento local de informações com uma classificação de Informações do Citi de Confidencial ou acima devem ser criptografados usando uma ferramenta de criptografia que satisfaça as normas do setor.
3. As conexões remotas devem ser estabelecidas apenas por meio de soluções de acesso remoto aprovadas que utilizem autenticação multifator (MFA).
4. Computadores gerenciados pelo fornecedor devem ter um firewall pessoal ativo quando conectados diretamente (ou seja, não por meio de um firewall ou proxy gerenciado pelo Fornecedor) na Internet.
5. Os dispositivos gerenciados pelo fornecedor devem estar regularmente conectados à rede do Fornecedor para receber e instalar atualizações regulares de software/ferramentas antivírus como um requisito para acesso total à rede. O acesso limitado pode ser permitido para a finalidade expressa de atualizar o dispositivo.
6. Se dispositivos não pertencentes ao Fornecedor e gerenciados pela empresa estiverem em uso para acessar informações Confidenciais ou acima do Citi, eles devem ser configurados para usar uma solução autorizada que não permita o download para o computador local. Os seguintes controles precisam estar implementados:
 - a) Dados do Citi não podem ser baixados para dispositivos fora de uma solução gerenciada pela empresa.
 - b) O Fornecedor deve garantir que esse acesso seja protegido por autenticação com base em token ou com base em certificado usando

tecnologias de acesso remoto padrão [ou seja, Interface de Desktop Virtual (VDI)].

- c) Soluções de acesso remoto, como Terminal Services e VMware Horizon, devem ser configuradas para desativar o compartilhamento da área de transferência e mapeamento de unidade via protocolos Blast, PCoIP e desativar protocolos RDP e SSH
7. Se os soft tokens forem usados para MFA, como para acessar um aplicativo de software em um dispositivo móvel, o software de autenticação de soft token deverá autenticar o usuário (por exemplo, por senha, biometria etc.) e impedir seu uso se o telefone celular estiver com jailbreak ou root (usando um sistema operacional diferente daqueles certificados e fornecidos pelo fornecedor do dispositivo móvel).
 8. Todo o Pessoal do Fornecedor, incluindo, entre outros, funcionários permanentes/temporários, contratados e subcontratados, exigindo acesso especial, privilegiado e/ou de nível administrativo a sistemas, repositórios de dados, aplicativos e/ou infraestrutura, incluindo, entre outros, administradores de sistema, administradores de banco de dados, administradores de controle de acesso, administradores de firewall, administradores de sites etc., que estejam relacionados direta ou indiretamente aos Serviços fornecidos para o Citi, só deve ser autenticado usando MFA e esse acesso será registrado e monitorado de forma independente pelo Fornecedor para atividade suspeita e/ou acesso não autorizado de acordo com estas Exigências.
 9. Para dispositivos de propriedade pessoal e dispositivos de propriedade de um terceiro, o Fornecedor deve ter uma solução eficaz para garantir que esses dispositivos tenham uma versão do sistema operacional aprovada, níveis de patch, soluções antivírus e antimalware, antes que esses dispositivos sejam autorizados a fazer login na rede.
 10. O Fornecedor deve garantir que todo o seu pessoal:
 - a) Mantenha um espaço de trabalho remoto dedicado e privado que não contém dispositivos de assistência de voz (por exemplo, Siri, Alexa), dispositivos de gravação de vídeo e/ou qualquer outro dispositivo de escuta/gravação de foto, vídeo ou áudio. Nenhum pessoal não autorizado terá permissão para visualizar quaisquer dados, sistemas, aplicativos que possam aparecer na(s) tela(s) dos sistemas de computação remotos.
 - b) Bloqueie o dispositivo de computação ao deixar o dispositivo sem vigilância para garantir que o acesso não autorizado para visualizar a tela seja adequadamente mitigado.

17.25 Política de Mesa Limpa

O pessoal do Fornecedor deve proteger as Informações do Citi em todas as formas, incluindo informações físicas usadas ou armazenadas no espaço de trabalho da equipe. Os Fornecedores devem comunicar essa exigência a todos os seus funcionários pelo menos anualmente por meio de treinamento sobre a IS ou outro canal.

17.26 Segurança contra Incêndios

1. O Fornecedor deve cumprir as exigências legais e regulatórias aplicáveis que regulamentam a segurança física e o estabelecimento de um ambiente de trabalho seguro, incluindo os códigos locais a respeito de incêndios.
2. O Fornecedor deve utilizar sistemas de detecção, alarme e contenção de incêndios. Os sistemas devem ser inspecionados e testados semestralmente.

17.27 Segurança Física

1. As Informações do Citi devem ser armazenadas em áreas com controles que restrinjam o acesso apenas a pessoal autorizado.
2. O Fornecedor deve ter um sistema de controle de acesso físico documentado e auditável em vigor.
3. O Fornecedor deve utilizar uma combinação de sistemas de alarme de segurança/de invasão que inclua um alarme de segurança monitorado por terceiros, seguranças e vigilância por vídeo, conforme apropriado para o ambiente e para os serviços prestados.
4. O Fornecedor deve ter uma política de visitantes documentada que inclua o requisito de todos os visitantes fornecerem identificação verificável na chegada e assinarem uma lista de entrada e saída.

17.28 Procedimentos e Responsabilidades de Segurança Operacional

1. O processo de gerenciamento de mudanças de Fornecedores deve incluir controles de pontos de verificação principais sobre registro, revisão, teste, aprovação, implementação e encerramento de mudanças. O Fornecedor também deve ter um processo de mudança de emergência que exija todas as etapas listadas sobre a inclusão de uma hierarquia de aprovações obrigatórias.
2. O Fornecedor deve ter um processo auditável relacionado à gestão de capacidade que inclua (entre outros) métricas/indicadores de disponibilidade, capacidade e desempenho; avaliação de impacto nos negócios; monitoramento proativo, investigação e abordagem de problemas de desempenho e capacidade.
3. Quando for aplicável, o Fornecedor deve garantir que os ambientes de Laboratório, Desenvolvimento, Testes e Produção sejam todos separados física e/ou logicamente uns dos outros.

17.29 Requisitos de Desenvolvimento de Software

Aplicáveis a Fornecedores que fornecem software desenvolvido para uso exclusivo do Citi. Os Fornecedores devem cumprir esses requisitos ou demonstrar um processo documentado e aprovado do Ciclo de Vida de Desenvolvimento de Software ("SDLC") com abordagem equivalente e de qualidade igual.

17.30 Iniciação e Planejamento

O Fornecedor deve definir o escopo e os objetivos da solução em alinhamento com as exigências e as obrigações contratuais do Citi. Isso inclui:

1. Documentar requisitos funcionais e não funcionais;
2. Fornecer estimativas de esforço e cronograma; e
3. Identificar todos os componentes ou dependências de terceiros.

As atividades de compliance, incluindo avaliações de risco de segurança, devem ser iniciadas no início do projeto. Funções, responsabilidades e pontos de verificação de aprovação devem ser claramente comunicados.

Todos os ambientes devem ser classificados como Desenvolvimento (DEV), Testes (TEST) ou Produção (PROD) e devem permanecer estritamente segregados ao longo do ciclo de vida. A classificação do ambiente determina as permissões de acesso e o tipo de dado que pode ser processado. O Fornecedor deve restringir o acesso com base na designação do ambiente e alinhar as implantações com a conclusão da fase SDLC apropriada para evitar o acesso não autorizado ou a exposição de dados.

17.31 Projeto

O Fornecedor deve documentar uma abordagem de projeto que garanta que a solução entregue atenda a todos os requisitos declarados (um “Plano de Teste”). No mínimo, um Plano de Teste deve incluir e descrever:

1. Todos os testes a serem executados pela equipe de desenvolvimento, incluindo testes unitários, testes funcionais e não funcionais, e testes de aspectos de desempenho, com rastreabilidade aos requisitos;
2. Identificação do(s) aprovador(es) que confirmará(ão) a conclusão;
3. Requisitos de testes de segurança, como avaliações de vulnerabilidade e modelagem de ameaças; e
4. O ambiente de teste, a abordagem, o processo e o caminho de promoção.

Uma estratégia de lançamento deve ser preparada descrevendo os pré-requisitos e processo para implantação em ambientes de TESTE e PRODUÇÃO, incluindo critérios de preparação para lançamento, conteúdo e frequência de entrega ao longo do ciclo de vida do projeto.

Quando especificado no Contrato, as distribuições de software devem ser empacotadas em um formato aprovado pelo Citi, utilizando ferramentas e fluxos de trabalho aprovados pelo Citi.

17.32 Testes

Os testes devem ser planejados e executados em um ambiente controlado para confirmar que a solução atende aos requisitos e critérios de sucesso definidos. Os casos de teste devem ser rastreáveis até os requisitos e os *commits* de código.

O Fornecedor deve preparar um relatório resumindo os resultados de aprovação/reprovação, testes adicionais realizados durante o desenvolvimento e quaisquer testes não concluídos (com motivos) (um “Relatório de Conclusão do Teste”). Defeitos e funcionalidades postergados devem ser documentados, juntamente com planos de mitigação para pontos de auditoria não resolvidos.

Mediante solicitação do Citi, o Fornecedor deve fornecer evidência de:

1. Um Plano de Teste detalhado;
2. A conclusão e os resultados do teste detalhados em um Relatório de Conclusão do Teste; e
3. Rastreabilidade dos resultados do teste aos requisitos e *commits* de código.

17.33 Implantação

Antes da implantação, o Fornecedor deve concluir todos os testes de segurança necessários, incluindo verificações de vulnerabilidade e modelagem de ameaças. O

processo de lançamento deve ser estruturado com registros de alteração documentados, estratégias de reversão e aprovações necessárias. Os planos de implementação e os runbooks de implantação devem incluir protocolos de monitoramento e encaminhamento.

Após a implantação, o Fornecedor deve finalizar os identificadores do sistema e atualizar todos os artefatos relacionados para garantir a prontidão para auditoria.

17.34 Segurança

1. Uma avaliação estruturada realizada durante a fase de projeto do SDLC para identificar e abordar riscos de segurança potenciais, vulnerabilidades e deficiências arquitetônicas antes que o código seja escrito (uma “Revisão de Projeto de Segurança”) deve ser incorporada no SDLC com controles preventivos e detectivos alinhados a padrões do setor, como OWASP.
2. Devem ser aplicadas práticas de codificação seguras.
3. O Fornecedor deve incorporar controles de segurança da informação em seus processos e procedimentos para a seleção, desenvolvimento e implementação de aplicativos, produtos e serviços.
4. O Fornecedor deve ter um procedimento de compilação seguro para todos os sistemas onde as Informações do Citi são armazenadas, processadas e/ou transmitidas e deve manter uma imagem ou modelo seguro para todos os sistemas.

17.35 Controles Contra Malware

O Fornecedor deve garantir a implementação de controles para prevenir e detectar a introdução de qualquer código mal-intencionado (por ex., vírus, worms, vírus Cavalo de Troia, adware, spyware, ransomware ou outros ataques cibernéticos similares em que os dados podem ser comprometidos). O Fornecedor deve:

1. Implementar, atualizar e manter tecnologia antivírus e anti-spyware em todos os computadores pessoais e tecnologia em todos os servidores de Rede Local (LAN), servidores de e-mail e outros dispositivos que armazenam, processam e/ou transmitem informações do Citi.
2. Implementar as configurações de segurança para evitar que os usuários finais desativem as ferramentas antivírus/antimalware e as verificações programadas.
3. Ter procedimentos automatizados e gerenciados centralmente para configurar e atualizar o software antivírus e antimalware.
4. Assegurar que haja processos implementados para identificar e abordar computadores fora de conformidade, nos quais as assinaturas de antivírus ou os mecanismos de varredura estão desatualizados.
5. Controlar o acesso a portas/interfaces de comunicação que permitem conexão a dispositivos externos, incluindo, entre outros, mídia de armazenamento.

17.36 Controles Contra Código Móvel

Os fornecedores devem garantir a implementação de controles relacionados a práticas seguras de código móvel. Quando o uso do código móvel for autorizado, a configuração deve, no mínimo, satisfazer todas as normas relevantes do setor e obrigações contratuais com o Citi, e o Fornecedor deve garantir que o código móvel autorizado opere de acordo com uma política de segurança claramente definida e documentada, bem como impedir a execução de código móvel não autorizado.

Para código móvel que possa afetar o sistema ou plataforma operacional subjacente (ou seja, fora da “área restrita”), o fornecedor deve garantir o seguinte:

1. O código móvel publicado pelo fornecedor deve ser assinado por uma autoridade de certificados aprovada pelo Citi e o ciclo de vida do certificado deve ser gerenciado pelo fornecedor para tratar do vencimento ou rotação da certificação.
2. O código móvel assinado com certificados vencidos deve ser removido da produção.

17.37 Registro de Auditoria

O Fornecedor deve garantir que todos os Sistemas de Informações Controladas usados para armazenar, processar, gerenciar e/ou transmitir dados do Citi usem trilhas de auditoria em nível de infraestrutura ou aplicativo para registrar os seguintes itens:

1. Ações relevantes de segurança de infraestrutura para a plataforma associada
2. Todos os alarmes do sistema associados a um firewall ou evento de segurança gerado por IDS/IPS
3. Todas as tentativas de violações da segurança do sistema (por exemplo, tentativas fracassadas de login de Usuário)
4. Tentativas não autorizadas de acesso a recursos (software, dados, processos etc.)
5. Ações do Administrador
6. Informações relacionadas ao recebimento de informações específicas de um usuário ou outro sistema
7. Todos os eventos significativos relacionados a transações financeiras e Informações do Citi que incluem especificamente os itens seguintes:
 - a. Atualizações em transações financeiras
 - b. Atualizações em dados de PII Confidenciais ou Sigilosas
 - c. Atualizações em dados Restritos
 - d. Atualizações em dados de Autenticação
8. Todas as sessões estabelecidas
9. Artefatos de sessão, como identificação de dispositivo único, devem ser capturados, quando tecnicamente viável, e registrados para aplicativos para o Citi (aplicativos de sites e móveis) para apoiar as investigações de fraude. Esses artefatos devem conter, no mínimo, endereços IP. Esses dispositivos devem ser capturados para as transações do Citi e para atividade de abertura de contas do Citi. As informações devem ser registradas de maneira que o dispositivo da sessão possa ser vinculado à transação ou abertura de conta.
10. As trilhas de auditoria devem documentar a atribuição de uma atividade específica a um indivíduo específico para evitar repúdio.

11. Eventos significativos da Administração de Segurança da Informação (Information Security Administration, ISA) devem ser registrados especificamente, incluindo os itens seguintes:
- a) Criação de usuário
 - b) Modificação dos direitos de acesso do usuário
 - c) Exclusão, criação e modificação de perfis nos Sistemas de Informações Controladas.
 - d) Redefinição de senhas
 - e) Mudanças na configuração de segurança do sistema
 - f) Todas as atividades interativas de IDs Funcionais com privilégios devem
 - g) Os registros de segurança devem conter pelo menos as informações abaixo, independentemente do sistema que gera o registro, a menos que essa inclusão não seja viável tecnicamente:
 - I. Data e hora do evento (horário em formato UTC)
 - II. ID de usuário do indivíduo realizando a ação
 - III. Tipo de evento
 - IV. Nome do ativo ou recurso afetado
 - V. Tipo de acesso (excluir, modificar etc.)
 - VI. Sucesso ou falha do evento
 - VII. Fonte (terminal, porta, local, IP, nome do host etc.)

17.38 Proteção de Informações do Registro

O Fornecedor deve garantir a implementação de controles de acesso para preservar a integridade das trilhas de auditoria durante o início, desligamento, armazenamento e transmissão.

1. Para evitar modificações não autorizadas nos registros de auditoria, o Fornecedor deve garantir que os registros não possam ser substituídos ou modificados pelos usuários do sistema cuja atividade eles rastreiam.
2. O Fornecedor deve apresentar ao Citi um procedimento de retenção de registro para os dados de registro que defina como os dados são mantidos e inclua medidas de compliance referentes a todos os requisitos legais e regulatórios aplicáveis.
3. Os relógios de todos os sistemas de processamento de informações relevantes em uma organização ou domínio de segurança devem ser sincronizados em uma fonte de tempo precisa.

17.39 Uso do Sistema de Monitoramento

Os Fornecedores devem garantir que os eventos seguintes sejam capturados, registrados e revistos diretamente ou por meio de um processo de revisão automatizado:

1. Todos os alarmes do sistema associados a um firewall ou evento de segurança gerado pelos Sistemas de Detecção de Invasão (Intrusion Detection Systems, IDS)/Sistema de Prevenção de Invasão (Intrusion Prevention System, IPS).
2. Todas as atualizações dos recursos críticos como identificadas na compilação padrão segura.

3. Todas as atividades interativas realizadas por quaisquer IDs (funcional, privilegiado, sistema, temporário etc.) com acesso a informações classificadas como PII Confidenciais ou acima.
4. Eventos ISA significativos listados na seção registro de Auditoria acima, com a seguinte exceção:
 - a) Remoção de direitos de usuário, função ou perfil quando a atividade de administração de segurança da informação for executada por um sistema de fluxo de trabalho automatizado/de cumprimento que tem controles de integridade ponta a ponta.

17.40 Correlação de Registro e Revisão

1. Quando um evento registrado dispara um alerta e o evento é revisado, o Fornecedor deve iniciar ações de acompanhamento e uma investigação deve ser realizada se houver indicação de que um incidente de segurança da informação potencialmente prejudicial possa ter ocorrido.
2. O Fornecedor deve garantir que os registros de auditoria sejam agregados a um sistema central de gerenciamento de registros, como um sistema de Gerenciamento de Informações e Eventos de Segurança (SIEM) ou ferramenta analítica de registro para análise e revisão de correlação de registros.
3. Os Fornecedores devem revisar e ajustar periodicamente a configuração de seu SIEM ou ferramenta de análise de registros para melhorar a identificação de eventos acionáveis.

17.41 Controle de Software Operacional

O Fornecedor deve garantir que usará apenas sistemas operacionais e software atualmente aceitos por um prestador de serviços comerciais aceito pelo setor ou que disponibilizem, de forma ativa e adequada, patches e atualizações de configuração para tratar questões de segurança.

O Fornecedor deve garantir a implementação de um processo documentado que especifique os prazos de remediação para a aplicação de todos os patches de segurança e configurações aprovados.

O Fornecedor deve garantir que, independentemente de qualquer contrato de manutenção separado entre o fornecedor e o Citi, o Fornecedor deverá garantir que o software desenvolvido para o Citi e regido por um acordo de licença não permita o uso de versões de software não compatível com vulnerabilidades conhecidas e que esse software foi atualizado e corrigido conforme necessário em tempo hábil.

O software aplicativo usado para processar as Informações do Citi deve ser adquirido de Fornecedores estabelecidos e deve ser licenciado, catalogado e aceito.

17.42 Gestão de Vulnerabilidade e Ameaças

1. O fornecedor deve implementar um processo de gestão de vulnerabilidades e ameaças que aborde e/ou inclua, de forma abrangente, todos os itens a seguir:

- a. Ferramentas e procedimentos para a descoberta e gestão de vulnerabilidades em todos os ativos que podem ser usados para processar, armazenar, acessar ou transmitir dados Confidenciais ou mais sigilosos do Citi.
- b. Uma exigência de que sejam realizadas verificações pelo menos semanalmente utilizando ferramentas de vulnerabilidade e metodologia de relatório reconhecidas pelo setor.
- c. Classificação de vulnerabilidades de acordo com a versão mais atual do “Sistema de Pontuação de Vulnerabilidade Comum (Common Vulnerability Scoring System, CVSS)” (consulte <https://www.first.org/cvss>), com cronogramas de correção com base na gravidade.
- d. O requisito de testar correções de vulnerabilidade antes da implantação de produção completa.
- e. Um processo operacional documentado e repetitivo para acelerar a correção de vulnerabilidades críticas.
- f. O Fornecedor deve monitorar os ativos ao longo de seu ciclo de vida passível de suporte para se preparar para os status de Fim de Vida (End of Life, EOL) ou Fim de Suporte do Fornecedor (End of Vendor Support, EOVS), bem como manter processos estabelecidos para atualizar ou substituir proativamente tais ativos.
- g. Quaisquer vulnerabilidades com pontuação crítica de acordo com o CVSS, identificadas por meio de coleta de inteligência, verificações de vulnerabilidade ou testes de penetração devem ser priorizadas e corrigidas dentro de um prazo bem definido compatível com o risco de vulnerabilidade.

17.43 Aplicativos Hospedados por Terceiros

Se o Fornecedor mantiver ou armazenar Informações Confidenciais ou dados mais sigilosos do Citi em um site ou sistema acessível pela Internet, ou um site que seja da marca Citi, o Fornecedor deverá cumprir, como forma de se proteger contra uma vulnerabilidade ou ameaça que envolva produtos ou serviços que afetem o Citi (cada um deles uma “vulnerabilidade”), as seguintes exigências:

1. Nomear um funcionário do Fornecedor para responder às perguntas do Citi sobre segurança da informação.
2. Utilizar as melhores práticas reconhecidas pelo setor para monitorar, no mínimo semanalmente, fontes respeitáveis de informações sobre vulnerabilidades de segurança do computador, como FIRST, CERT/CC, e o Catálogo de Vulnerabilidades Exploradas Conhecidas da CISA e listas de correspondência de fornecedores, e tomar as medidas apropriadas para obter, testar completamente, aplicar e fornecer ao Citi serviços relevantes pacotes, patches, atualizações e soluções alternativas.

3. Testar, pelo menos trimestralmente, a implementação de suas medidas de segurança da informação usando ferramentas de verificação de vulnerabilidade de rede, sistema e aplicativo e/ou testes de penetração.
4. Permitir que o Citi, ou um terceiro aprovado pelo Citi, execute, com intervalos de tempo razoáveis, avaliações de vulnerabilidade, hacks éticos ou outras avaliações de segurança, para verificar o compliance do Fornecedor com suas obrigações sob qualquer contrato e estas Exigências, incluindo, entre outros, revisão de políticas, processos e procedimentos, avaliações no local de acordos de segurança física, varredura de vulnerabilidade de rede, sistema e aplicativo e teste de penetração, usando ferramentas comercialmente disponíveis e/ou práticas padrão do setor para realizar essas inspeções.
5. Qualquer contratado que forneça ao Fornecedor serviços de avaliação de vulnerabilidade deve constar na lista aprovada pelo Citi de provedores de avaliação de vulnerabilidade. Quando o Fornecedor utilizar contratados ou subcontratados para fornecer os Serviços, o Fornecedor deverá, à sua própria custa, garantir que quaisquer avaliações de vulnerabilidade exigidas sejam concluídas da mesma maneira oportuna como se o Fornecedor estivesse fornecendo esses Serviços diretamente e garantirá que a exigência para qualquer contratado ou subcontratado para facilitar essas avaliações seja registrada no contrato entre o Fornecedor e o contratado/subcontratado referente ao Serviço, incluindo cláusulas que autorizem o Citi a realizar tais avaliações.
6. **Notificação.**
 - a) Ao identificar uma vulnerabilidade que envolva um produto ou serviço que afete o Citi, o Fornecedor deverá notificar o Citi por escrito no prazo de 24 horas após a identificação e incluirá uma descrição das ações corretivas tomadas pelo Fornecedor.
 - b) Ao tomar conhecimento de uma vulnerabilidade que envolva um produto ou serviço que afete o Citi após a divulgação pública responsável dos canais de processo (publicação da Vulnerabilidade no National Vulnerability Database (NVD) ou por meio do catálogo de ameaças fornecido a fornecedores de segurança externos), o Fornecedor notificará o Citi por escrito no prazo de 24 horas a partir de tal publicação. Cada notificação incluirá informações sobre a vulnerabilidade, a utilidade do sistema para serviços relacionados ao Citi (ou seja, se ele hospeda informações do Citi ou é usado na prestação de serviços ou ambos), se pode ser explorado remotamente; e a pontuação de Common Vulnerabilities and Exposures (CVE). O fornecedor continuará a fornecer atualizações ao Citi até que a vulnerabilidade seja remediada. Nos casos em que o Citi identificar uma vulnerabilidade, o Citi poderá notificar o Fornecedor sobre isso, e o Fornecedor deverá remediar imediatamente a vulnerabilidade de acordo com esta Seção.

7. **Remediação.** Para cada notificação de Vulnerabilidade fornecida nesta seção, a parte notificante avaliará o nível de risco e o impacto dessa vulnerabilidade com base na gravidade e risco para o Citi e atribuirá um nível de prioridade de risco com base no Sistema de Pontuação de Vulnerabilidade Comum (CVSS) conforme estabelecido no Apêndice A (ver <https://www.first.org/cvss>). Assim que um nível de risco for atribuído e acordado entre as partes, o Fornecedor remediará qualquer vulnerabilidade média, alta ou crítica identificada. Sempre que possível, a correção para qualquer vulnerabilidade será disponibilizada em um pacote de segurança para a versão atualmente implementada.

Se o Fornecedor não puder ou não quiser remediar a vulnerabilidade a contento do Citi, o Citi poderá rescindir a licença aplicável sem qualquer responsabilidade ou obrigação financeira adicional (para a parte rescindida), e o Fornecedor deverá reembolsar imediatamente ao Citi a parte proporcional das tarifas de licença pagas.

17.44 Controles de Rede de Segurança de Comunicação

1. As redes do fornecedor usadas para acessar, armazenar, processar e/ou transmitir Informações do Citi devem ser protegidas de ameaças, e a segurança deve ser mantida para os Sistemas de Informação usando pontos de execução na rede.
 - a. Informações com uma Classificação de Informações do Citi Confidenciais ou acima não devem ser armazenadas de forma persistente em um sistema em zona desmilitarizada (Demilitarized Zone, DMZ) para a internet. Redes usadas para acessar, armazenar, gerenciar, processar e/ou transmitir Informações do Citi usando Redes Locais sem Fio (WLANs) ou outras soluções de dispositivos sem fio que incluam controles razoáveis para proibir o acesso não autorizado (PEAP-TLS, EAP-TTLS etc.) podem estar conectadas a redes que contêm Informações do Citi.
 - b. Todas as conexões de IP externo para a rede global do fornecedor são protegidas por um firewall administrado pelo Fornecedor.
 - c. Um Sistema de Detecção de Invasão (Intrusion Detection System, IDS) e um Sistema de Prevenção de Invasão (Intrusion Prevention System, IPS) estão implementados e monitoram e protegem em tempo real conexões de Internet à rede do Fornecedor onde as Informações do Citi são acessadas, gerenciadas, armazenadas, processadas ou transmitidas.
2. Para todos os aplicativos de internet com a marca Citi, o Fornecedor deve garantir que:

- a. Os serviços hospedados em sites do Fornecedor estão protegidos por serviços anti-DDoS (Distributed Denial of Service) aprovados pelo Citi ou controles comparáveis validados pelo Citi.
- b. Firewalls externos devem ser configurados com uma regra de negação por padrão. As regras de firewall devem ser configuradas com base no princípio de privilégio mínimo e todas as tentativas de conexão negadas pelo firewall (por exemplo, eliminar pacotes) devem ser registradas/gravadas.
- c. O tráfego de comunicações de rede deve ser negado por padrão e permitido por exceção nas interfaces gerenciadas. As exceções devem ser muito limitadas a fontes, destinos e serviços específicos.
- d. O tráfego de aplicativos da Web deve ter controles adequados e ser filtrado, por exemplo, por meio de Web Application Firewalls.

17.45 Segregação em Redes

O Fornecedor deve garantir que todos os Sistemas de Informação e aplicativos que são usados para acessar, armazenar, processar e/ou transmitir Informações do Citi e que podem ser acessados por meio da Internet, somente possam ser acessados por meio da zona desmilitarizada (DMZ) do Fornecedor.

Durante um evento de emergência, o fornecedor deve ser capaz de filtrar o acesso entre as partes da rede para reduzir o impacto de eventos de segurança da rede (por exemplo, filtragem de porta durante um surto de vírus).

Acesso remoto e segurança de host devem implementar controles de acesso com base em grupos (por exemplo, equipe, subcontratados) para limitar o acesso aos recursos da rede na rede do fornecedor. No nível do host, o controle de acesso pode ser feito em nível de grupos ou de pessoas.

17.46 Identificação de Equipamentos nas Redes

As plataformas de tecnologia devem identificar e autenticar as plataformas de tecnologia de pares compatíveis com os níveis de risco de IS da interação e outros controles atenuantes.

1. Apenas dispositivos do fornecedor (ou seja, hardware, incluindo, entre outros, computadores e notebooks) que cumpram estas exigências e que sejam autorizados pelo Fornecedor podem acessar a Rede do Fornecedor onde as Informações do Citi são armazenadas, processadas ou transmitidas.
2. Apenas dispositivos do Fornecedor (ou seja, hardware, incluindo, entre outros, desktops, laptops, mídia de armazenamento de dados removível) que cumpram esses requisitos e que sejam autorizados pelo Citi podem acessar a rede do Citi.

17.47 Análise e Especificação de Requisitos de Segurança

O Fornecedor deve incorporar procedimentos de segurança da informação em seus processos e procedimentos para a seleção, desenvolvimento e implementação de aplicativos, produtos e serviços.

17.48 Transações On-Line

1. Quando aplicável, o Fornecedor deve ter sistemas de informação que utilizam

senhas dinâmicas ou certificados digitais para validar credenciais.

2. Todos os certificados de entidade final devem ser substituídos pelo menos uma vez a cada 13 meses.
3. Os aplicativos de Fornecedores que armazenam, processam, gerenciam ou acessam informações do Citi, hospedam aplicativos com uso da Internet da marca do Citi ou têm conectividade com os recursos de rede do Citi devem:
 - a. Utilizar um método de autenticação baseado nos tipos de dados/funções acessados;
 - b. Executar uma avaliação de conformidade de Autenticação Multifator (Multifactor Authentication, MFA) e implementar as recomendações, se necessário;
 - c. Realizar uma avaliação de integração do Monitoramento de Atividades Suspeitas (Suspicious Activity Monitoring, SAM) e implementar recomendações se necessário;
 - d. Em todos esses casos, o Fornecedor deve entrar em contato com o contato comercial principal para obter as exigências atuais do Citi.

17.49 Procedimentos de Controle de Mudanças

1. O Fornecedor deve garantir que as mudanças de configuração de firewall, Sistemas de Detecção de Invasão (Intrusion Detection Systems, IDS) e Sistemas de Prevenção de Invasão (Intrusion Prevention Systems, IPS) passem pelo processo de gestão de mudanças do Fornecedor.
2. O acesso concedido à produção por meio de IDs temporárias deve ser registrado e monitorado para acompanhar as mudanças feitas no ambiente.
3. Para Sistemas de Informações Controladas contendo Informações do Cliente com uma classificação do Citi de Confidencial ou acima ou com valor de componente de risco de IS para “Integridade” ou “Disponibilidade” de “Alto”, os registros capturados de acordo com a seção 17.32 (Registro de auditoria) devem ser revistos pelo Fornecedor. Essas revisões podem ser baseadas em uma metodologia de amostragem com base em riscos apropriada.
4. A revisão deve validar que as alterações que fazem parte do acesso com privilégios temporário foram feitas conforme o planejado.
5. O Fornecedor deve documentar todas as alterações, incluindo o armazenamento de evidências do processo de revisão.

17.50 Vazamento de Informações

O Fornecedor deve ter uma norma de codificação segura implementada que previna vazamento de informações, incluindo:

1. Informações detalhadas do sistema (por exemplo, tipo e tecnologia do servidor).
2. Rastreamentos de pilha e erros de exceção que revelam a estrutura de árvore de diretórios e o tipo de banco de dados subjacente.

17.51 Dados de Testes

Informações confidenciais ou acima, conforme definido pelo Citi, não devem ser usadas ou armazenadas pelo Fornecedor em ambientes ou Laboratórios de teste ou desenvolvimento de aplicativos de software, a menos que essas informações sejam

desidentificadas, mascaradas e/ou ofuscadas usando ferramentas e métodos que atendam aos padrões do setor, para que esses dados não sejam mais sigilosos ou o Fornecedor deve implementar controles de produção em tempo real nos ambientes de desenvolvimento ou teste.

17.52 Aceitação do Sistema

O fornecedor deve ter processos de Gestão do Escopo do Projeto e Aceitação do Sistema documentados e implementados que satisfaçam as normas relevantes do setor.

17.53 Comunicação de Pontos Fracos de Segurança da Informação

O Fornecedor deve ter um Processo para garantir que as vulnerabilidades de aplicativos e infraestrutura que resultam em um comprometimento de ativos de informação do Citi sejam **comunicadas ao Citi imediatamente**.

17.54 Responsabilidades e Procedimentos de Incidentes de Segurança

1. Um SIRT é um evento de segurança que compromete qualquer um dos seguintes itens, independentemente de como ou onde o incidente de segurança ocorreu ou quem pode ter causado o comprometimento:
 - A Confidencialidade, Integridade ou Disponibilidade dos dados do Citi.
 - A Confidencialidade, Integridade ou Disponibilidade de quaisquer dados (incluindo Informações Pessoais) em relação aos quais o Citi está sujeito a obrigações contratuais, legais ou regulatórias.
 - Integridade ou Disponibilidade dos sistemas de informação do Citi que armazenam, processam ou transmitem quaisquer dados do Citi.
2. Para nossos fins, um comprometimento de confidencialidade refere-se à exposição de dados a uma pessoa não autorizada ou a cenários em que o Citi perde a custódia e o controle dos dados. Todos os incidentes de segurança devem ser reportados imediatamente.
3. Se o Fornecedor tiver experimentado um SIRT, o Fornecedor deve cooperar com o Citi no fornecimento de informações solicitadas pelo Citi de acordo com os processos de resposta a incidentes do próprio Citi, analisar os dados comprometidos de maneira suficiente para permitir que o Citi cumpra os requisitos legais, regulatórios e/ou de governança interna; fazer quaisquer/todas as notificações exigidas por lei, norma ou regulamento, ou desejadas pelo Citi a seu critério, mediante solicitação do Citi e à custa do Fornecedor, e somente depois que o Citi tiver tido a oportunidade de revisar e alterar a linguagem do modelo de notificação proposto; e o Fornecedor não deve mencionar o Citi em tais notificações,

a menos que o Citi solicite expressamente, por escrito, que seu nome seja incluído.

17.55 Proteção contra Vazamento de Dados (DLP)

O Fornecedor deve implementar controles de prevenção de vazamento de dados (DLP), incluindo conteúdo e monitoramento de terminais, que cubra todos os funcionários com acesso a dados Confidenciais ou acima do Citi.

O Fornecedor deve ter controles implementados para detectar e impedir que ocorrências de dados Confidenciais ou acima do Citi sejam movidos para fora de sua rede por meio dos seguintes canais:

- a. E-mails não criptografados.
- b. Anexos de e-mail criptografados.
- c. Impressão de dados do Citi.
- d. Transferências de dados do Citi para locais fora da rede (por exemplo, via FTP).
- e. Tentativas de copiar dados confidenciais ou acima do Citi para mídias removíveis, como unidades USB, discos rígidos removíveis, unidades de CD/DVD e outros dispositivos removíveis com recursos de armazenamento de dados. Esse privilégio deve ser evitado por padrão.
- f. A solução DLP deve registrar e alertar o Fornecedor de todos os eventos que representam tentativas (bem-sucedidas ou bloqueadas) de mover, transportar ou copiar dados Confidenciais ou acima do Citi de sua rede para outros destinos. Esse privilégio deve ser evitado por padrão.
- g. Upload de dados do Citi para sites externos, incluindo sites de compartilhamento de arquivos/SaaS. Esse privilégio deve ser evitado por padrão.

17.56 Navegação na Web

1. O Fornecedor deve ter controles de acesso à web implementados para evitar o compartilhamento de informações Confidenciais ou acima do Citi e a exposição a malware ou ataque para os funcionários com acesso aos dados do Citi.
2. Para funcionários que têm acesso a dados Confidenciais ou acima do Citi:
 - a. Todas as solicitações de URL devem ser registradas.
 - b. Tentativas de acesso a sites que podem ser usados para compartilhamento não autorizado de dados do Citi (ou seja, webmail, chat, mídias sociais, armazenamento on-line, IA Generativa etc.) precisam ser bloqueadas.
 - c. O acesso a sites que podem expor o ambiente a malware ou ataque precisa ser bloqueado.
 - d. Tentativas de acesso a sites considerados não relacionados aos negócios devem ser bloqueadas.
 - e. O Fornecedor deve assinar um serviço de categorização de URL que seja atualizado regularmente; todas as URLs não categorizadas

- precisam ser bloqueadas por padrão ou todas as URLs precisam ser bloqueadas por padrão e aprovadas caso a caso.
- f. Os Navegadores da Web que estão em uso pelo Fornecedor precisam contar com suporte total e com as atualizações de segurança mais recentes do fornecedor do software.

17.57 Mensagens Eletrônicas

Mensagens eletrônicas, redes ponto a ponto ou outras ferramentas colaborativas de internet não podem ser usadas para transmitir ou armazenar Informações do Citi fora da rede do Fornecedor ou de redes que contêm Informações do Citi, a menos que criptografia apropriada esteja implementada para todos os dados do Citi conforme a Seção 17.9 (Política sobre o uso de controles criptográficos).

17.58 E-mail

O Fornecedor precisa ter controles de e-mail para evitar o compartilhamento de Informações do Citi e a exposição a malware ou ataque. Isso inclui:

1. Os anexos de arquivos recebidos que entram no gateway de e-mail são verificados e bloqueados se representarem um risco para o sistema.
2. O software de filtragem de e-mail (Antispam, Antiphishing) está em uso e atualizado.
3. Quaisquer dados Confidenciais ou acima do Citi devem ser criptografados quando enviados para fora da organização do Fornecedor.
4. Os clientes de e-mail que estão em uso pelo Fornecedor contam com suporte total e com as atualizações de segurança mais recentes do fornecedor do software.

17.59 Mídias Removíveis

1. O fornecedor deve proteger as Informações do Citi, independentemente da mídia em que são mantidas. Esta norma aplica-se, entre outros, aos seguintes tipos de mídia nos quais as informações estão armazenadas: cartão, cassete, disco compacto (CD), disquete ou outro dispositivo de armazenamento removível, saída de cópias impressas, disco magnético, fita magnética, microfilme, microficha, disco óptico ou documento impresso.
2. A configuração padrão para acessar mídia portátil/dispositivos de armazenamento para os sistemas nos quais as Informações do Citi são armazenadas não deve ser acessível. Se exceções forem concedidas e assim o acesso de leitura e gravação for permitido, os dados devem ser criptografados no dispositivo de mídia portátil.
3. Se o uso de mídia removível for permitido, esse uso deve ter um processo de aprovação da administração, incluindo a justificativa comercial para exigir o uso de mídia removível. A mídia removível deve ser inventariada pela administração. Mídia removível que contenha dados Confidenciais ou acima do Citi deve ser criptografada automaticamente, sem nenhuma ação necessária do usuário.

17.60 Descarte de Mídia

1. Quando Informações do Citi com uma classificação do Citi de confidencial ou acima se qualificarem para descarte de acordo com as instruções fornecidas

pelo Citi (ou seja, no ponto em que as informações não são mais exigidas ou úteis para o Citi e qualquer período adicional de retenção exigido por lei, regulamento e/ou políticas do Citi expirou), o fornecedor deve destruir tais informações de maneira a torná-las inutilizáveis e irrecuperáveis.

2. Uma ferramenta aprovada que substitui aleatoriamente os setores da unidade com caracteres específicos e diferentes deve ser usada para apagar com segurança a mídia montável com base nas seguintes regras:
 - a. Para mídias que armazenam informações classificadas como Confidenciais ou acima, a ferramenta deve concluir três aprovações da mídia.
 - b. Desmagnetize a mídia (se aplicável).
3. Destrua a mídia fisicamente para torná-la ilegível (ou seja, trituração, esmagamento das unidades).
4. Papel e outras mídias de armazenamento não eletrônico que contenham Informações Confidenciais ou acima devem ser coletados de forma segura e armazenados em uma “Caixa Confidencial” segura antes do descarte final. As Caixas Confidenciais devem estar sempre trancadas e só podem ser abertas por pessoal autorizado.
 - a. Copiadoras, impressoras, aparelhos de fax e qualquer outro dispositivo que tenha memória/armazenamento que possa conter informações Confidenciais do Citi ou acima também devem ser higienizados.

17.61 Treinamento e Gestão de Segurança da Informação

1. Manter um programa adequado de conscientização e educação sobre segurança cibernética/da informação que inclua, entre outros, prevenção de phishing e outros ataques de engenharia social, tratamento adequado de informações confidenciais e relatórios de incidentes de segurança e gerenciamento de respostas.
2. O Fornecedor deve garantir que todos os funcionários, incluindo contratados e funcionários temporários, recebam educação e treinamento de conscientização sobre as políticas e procedimentos organizacionais relevantes para suas funções.
3. O Fornecedor deve garantir que o programa de treinamento e conscientização seja revisado e atualizado anualmente para abordar riscos e ameaças emergentes, melhores práticas atuais e novas tecnologias no cenário de segurança cibernética.
4. No mínimo, os seguintes tópicos devem ser incluídos:
 - b. Rotulagem e tratamento de informações
 - c. Transmissão Segura (e-mail seguro, armazenamento seguro do SharePoint, não enviar dados de propriedade do Citi para e-mail pessoal)
 - d. Relatório de incidentes de segurança da informação
 - e. Local de trabalho seguro (por exemplo, uso apropriado da internet, software não autorizado, proibições de baixar software não aprovado)
 - f. Gerenciamento de Senhas (por exemplo, senhas fortes, proibição de compartilhamento de senhas)
 - g. Engenharia Social (phishing, spear fishing, vishing, SMishing)
 - h. Trabalho Remoto (por exemplo, Conexão Protegida/Segura, Segurança de Dispositivo Pessoal)
5. Os funcionários do Fornecedor devem receber o treinamento após ou antes de receber acesso a sistemas que hospedam dados do Citi e concluir o treinamento até a data de vencimento na notificação da atribuição.
 - a. O treinamento de IS deve ser administrado a todo o pessoal pelo menos anualmente, quando não for proibido por lei.
6. O treinamento deve incluir um mecanismo para registrar a medição de sua eficácia (por ex., um questionário após a conclusão com critérios de aprovação/reprovação), onde a legislação local permitir.

17.62 Programa de Gerenciamento de Risco Cibernético

O Fornecedor também precisa, no mínimo, manter um programa apropriado de gerenciamento de risco cibernético que inclua no mínimo o seguinte:

1. Manter um programa de Gestão de Risco de Segurança da Informação bem definido, documentado e/ou um programa de gerenciamento de risco operacional que tenha um componente de gerenciamento de risco cibernético/da informação claramente definido, que defina o apetite de risco cibernético do fornecedor e garanta que seu risco cibernético residual se alinha com esse apetite.

2. Manter um programa robusto de governança de gestão de riscos de segurança que inclua, entre outros, a coleta e/ou o desempenho de auditorias e revisões de segurança que avaliam o estado geral de segurança dentro da organização e relatam pelo menos anualmente à sua liderança executiva para revisão e garantia de que o apetite ao risco cibernético do Fornecedor não tenha sido violado.
3. Manter compliance com quaisquer PCI Data Security Standards (PCI-DSS) aplicáveis ao Fornecedor onde o Fornecedor está processando, armazenando e/ou transmitindo transações, pagamentos e/ou informações de cartão de crédito/débito.
4. Manter um plano e manual de gestão de crises e um plano da Equipe de Resposta a Incidentes de Segurança consistente com os padrões do setor para garantir que o Fornecedor tenha capacidade suficiente e adequada para detectar, conter, investigar, responder e se recuperar de qualquer tentativa, suspeita e/ou incidente de segurança cibernética.

17.63 Segurança de Aplicativos, API, Código, Sistema e Infraestrutura

Quando o Fornecedor estiver hospedando, desenvolvendo, codesenvolvendo, fornecendo ambientes de desenvolvimento e/ou fornecendo (a) um aplicativo ou aplicativos de software, o Fornecedor deverá realizar revisões de código do referido software e/ou patches para o software quanto a falhas de segurança, prevenção de acesso não autorizado, modificação e/ou inserção de malware ou outras formas de código malicioso e testes de vulnerabilidade para garantir que o aplicativo (incluindo APIs), juntamente com serviços de sistema subjacentes, sistemas operacionais e as redes estejam livres de vulnerabilidades e defeitos conhecidos que possam resultar em um incidente de segurança, violação de privacidade, fraude, acesso não autorizado e/ou divulgação de Informações Confidenciais, perda de integridade das informações que estão sendo processadas, armazenadas ou transmitidas pelo(s) aplicativo(s) e/ou perda de disponibilidade que possa afetar a qualidade dos produtos e/ou serviços que o Fornecedor fornece ao Citi.

17.64 Segurança Móvel

Quando o Fornecedor estiver fornecendo uma solução de aplicativos móveis, o Fornecedor deve cumprir os seguintes requisitos:

1. O aplicativo móvel deve oferecer suporte apenas às versões geralmente disponíveis (GA)/estáveis e não EOL² do Google Android (excluindo Android Go) e/ou das plataformas Apple iOS/iPadOS. Se a solução móvel estiver equipada com suporte para outras, os sistemas operacionais/versões aceitos serão configuráveis pelo Citi.
2. A solução móvel não deve aceitar plataformas/dispositivos móveis que não estejam equipados com conjuntos de instruções regulares para aceitar

² Versões de produtos que contam com suporte ativo e recebem atualizações regulares de segurança e manutenção do proprietário da plataforma ou do Fornecedor.

algoritmos criptográficos, incluindo, entre outros, criptografia conforme especificado na Seção 17.9 (Requisitos de Criptografia) deste documento.

3. Versões de sistemas operacionais em fase de pré-produção, incluindo, entre outras, versões beta, de acesso antecipado e de prévia de recursos, não são permitidas no ambiente de produção.
4. O Fornecedor deve ser capaz de fornecer uma lista dos componentes integrados de terceiros, incluindo, entre outros, bibliotecas de softwares livres e de código aberto que são agrupadas/alavancadas pela solução móvel.
5. O aplicativo móvel deve seguir os requisitos e as melhores práticas que permitem que aplicativos móveis sejam publicados por meio de lojas públicas de aplicativos, como a Apple App Store ou a Google Play Store. As lojas de aplicativos públicos listadas serão o método preferido e principal para distribuir/publicar o aplicativo móvel.
6. Os aplicativos móveis Android devem aproveitar o esquema de assinatura APK v2+. O esquema de assinatura APK versão 1 (também conhecido como assinatura JAR) não deve ser usado.
7. O tipo e o tamanho da chave de assinatura do aplicativo móvel devem estar em conformidade com a seção 17.9 – Requisitos de **Criptografia** deste documento.
8. Cada chave de assinatura de aplicativo e certificado X.509v3 associado deve ser gerenciada individualmente e dedicada a um único ID de Aplicativo/ID de pacote. A assinatura de chaves não deve ser compartilhada entre os aplicativos.
9. Se um aplicativo móvel exigir a retenção de dados no dispositivo móvel, ele deve manter apenas os dados mais recentes no dispositivo que são necessários para a(s) finalidade(s) do aplicativo/serviço, ou enquanto for necessário de acordo com requisitos legais ou regulatórios.
 - a. A coleta, processamento e/ou armazenamento de dados do usuário deve estar em conformidade com as leis locais, incluindo, entre outros, regulamentos de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR) e a Diretiva 2002/58/CE (ePrivacy) ou seus equivalentes regionais.
 - b. Componentes integrados de terceiros (por exemplo, bibliotecas) não devem coletar, processar e/ou armazenar dados de usuários.
10. Os aplicativos móveis não devem tornar quaisquer dados de aplicativos acessíveis em âmbito mundial.
 - a. Se o compartilhamento de dados com outros aplicativos for necessário, os aplicativos devem aproveitar técnicas, métodos e controles comercialmente razoáveis para os respectivos sistemas operacionais compartilharem apenas a quantidade necessária de dados com o número mínimo de outros aplicativos onde esse compartilhamento de dados é devidamente justificado e documentado.

11. Os aplicativos móveis devem depender apenas de instalações de comunicação seguras fornecidas pelos respectivos sistemas operacionais móveis. Por exemplo:
 - a. Os aplicativos Android devem declarar explicitamente que o tráfego de rede inseguro não é permitido para nenhum domínio de rede em seu manifesto de aplicativo e/ou arquivo de configuração de rede.
 - b. Os aplicativos iOS/iPadOS devem aproveitar a Segurança do Transporte de Aplicativos (Application Transport Security – ATS) sem qualquer exceção.
12. Os materiais criptográficos devem estar vinculados a um keystore seguro com suporte de hardware.
13. Os aplicativos móveis devem ser construídos no modo de release e não devem conter:
 - a. Qualquer característica ou método que possa ignorar os controles de segurança,
 - b. Informações de depuração, como nomes de arquivos do código-fonte, nomes de variáveis, nomes de símbolos, comentários etc., que têm o potencial de facilitar a engenharia reversa.
14. Os aplicativos móveis devem estar equipados com mecanismos eficazes anti-hooking ou antiviolação para evitar a injeção de código malicioso que possa alterar ou monitorar o comportamento do aplicativo no tempo de execução.
15. Os aplicativos móveis devem implementar técnicas abrangentes de antidepuração ou antiengenharia reversa/ofuscação para impedir ataques de engenharia reversa.
16. Os pacotes de aplicativos móveis devem estar equipados com um recurso que permita verificar a autenticidade e integridade de seu conteúdo (por exemplo, usando verificador criptográfico e/ou assinatura digital).
17. Se o aplicativo móvel exigir autenticação de usuário, as verificações de integridade do aplicativo e/ou dispositivo devem ser concluídas antes do início da autenticação de usuário.
18. Os aplicativos móveis que acessam/processam/armazenam informações de propriedade do Citi com uma classificação do Citi de Confidencial ou acima e/ou para as quais sua classificação de risco de IS é Média ou acima devem utilizar apenas modalidades biométricas fortes (por exemplo, atender ou superar a categoria Classe 3/Forte, conforme definido no [Android Compatibility Definition Document](#) correspondente).
19. Os aplicativos móveis devem implementar contramedidas para proteger contra ataques Man-in-the-middle (MitM).
20. Os aplicativos móveis devem ser capazes de detectar dispositivos comprometidos que incluem, entre outros, dispositivos móveis desbloqueados por “jailbreak” ou desbloqueados por “rooting” e reagir de acordo com a avaliação de risco da empresa e os requisitos regulatórios.

21. Os aplicativos móveis devem implementar uma vinculação forte ao dispositivo para evitar que o token de software (por exemplo, prova de posse) seja clonado.
22. Os aplicativos móveis devem usar aplicativos/soluções de teclado seguros (por exemplo, aqueles que são incorporados/pré-instalados pelos sistemas operacionais móveis).
23. Notificações push não devem conter informações sigilosas (por exemplo, informações do Citi classificadas como Confidenciais ou acima). No entanto, uma senha única (OTP) pode ser distribuída por meio de notificação push.
24. As soluções de aplicativos móveis devem estar equipadas com a capacidade de rejeitar/ignorar tentativas de comunicação com clientes móveis que usam versões de aplicativos com vulnerabilidades conhecidas/exploráveis.
25. Os aplicativos móveis devem seguir as melhores práticas do setor, incluindo, entre outros, técnicas de prevenção publicadas no [OWASP Mobile Top 10](#).
26. Os aplicativos móveis que utilizam técnicas de inteligência artificial e aprendizado de máquina (IA/ML) devem fazer isso de forma ética e de acordo com a Seção 19 – **Error! Reference source not found.** (incluindo IA Generativa/IA Agêntica).
27. O aplicativo móvel deve aproveitar as permissões mínimas do dispositivo necessárias para executar a(s) finalidade(s)/função(ões) que são utilizadas pelo Citi.
28. Os aplicativos móveis não devem armazenar informações não públicas sobre armazenamento externo/removível, como cartões SD.**Error! Reference source not found.**

17.65 Divulgação de Software

O Fornecedor deverá divulgar todos e quaisquer componentes de software, incluindo, sem limitação, software de código aberto, contidos em quaisquer produtos ou serviços fornecidos ao Citi (coletivamente, “Componentes de Software”). O Fornecedor não incorporará, por meio de uma atualização, upgrade ou de outra forma, quaisquer Componentes de Software em qualquer versão dos produtos ou serviços a serem instalados nos Sistemas do Citi sem divulgação prévia ao Citi em cada caso. Além disso, o Fornecedor deve garantir que seus produtos ou serviços não incluam Componentes de Software que sejam licenciados sob quaisquer termos que sujeitem o Citi ou suas Afiliadas a quaisquer obrigações não expressamente divulgadas e aceitas pelo Citi em um Contrato. O Fornecedor deve divulgar ao Citi quaisquer Componentes de Software mal-intencionados detectados dentro da organização, produtos ou serviços do Fornecedor dentro de 30 dias da descoberta. Especificamente, o Fornecedor deve divulgar seu uso de Componentes de Software em cada lançamento e versão dos produtos ou serviços por meio do fornecimento ao Citi de uma Lista de Materiais de Software (“SBOM”) no formato de arquivo OWASP CycloneDX ou no formato de arquivo de especificação ISO/IEC 5962:2021 Software Package Data Exchange (SPDX). Tal divulgação deve incluir a origem dos Componentes de Software (por exemplo: fornecedor comercial, banco de dados embarcado, gerenciador público de pacotes binários, compilação a partir de código-fonte, qualquer Software Embarcado ou provedor de Componentes de Software selecionados) e informar se o Fornecedor — ou qualquer

entidade de sua cadeia de suprimentos de software — obteve uma cópia dos Componentes de Software (o chamado “fork”) e, posteriormente, incorporou-a aos seus produtos ou serviços, seja como uma dependência de pacote ou como código-fonte integrado ao código-fonte do Fornecedor a partir do qual os produtos e serviços são compilados.

17.66 Modelagem de Ameaças

O fornecedor deve implementar um processo de modelagem de ameaças que aborde e/ou inclua, de forma abrangente, todos os itens a seguir:

1. Definição do Escopo: o Fornecedor deve definir claramente o escopo do modelo de ameaça, com foco em componentes de software e fluxos de dados que processam, armazenam ou transmitem informações Confidenciais e acima do Citi.
2. Identificação de Ameaças: o fornecedor deve identificar sistematicamente possíveis ameaças e vulnerabilidades relevantes para o projeto, arquitetura e uso pretendido do software, considerando vários vetores de ataque e agentes de ameaças no início do ciclo de vida do projeto.
3. Análise de Risco: o Fornecedor deve analisar as ameaças identificadas para avaliar seu possível impacto e probabilidade, permitindo a priorização dos riscos de segurança.
4. Integração de Controles: o Fornecedor deve definir e integrar controles de segurança e estratégias de mitigação apropriados no projeto e desenvolvimento do software para abordar esses riscos priorizados.
5. Documentação: o Fornecedor deve documentar o modelo de ameaça, incluindo ameaças identificadas, riscos associados e as medidas de mitigação correspondentes implementadas.
6. Revisão Periódica: o fornecedor deve revisar e atualizar regularmente os modelos de ameaças, especialmente quando houver alterações significativas no projeto, na funcionalidade ou no ambiente de implantação do software.

17.67 Inteligência Artificial

1. Os fornecedores devem implementar e adotar um Secure Software Development Lifecycle (SSDLC) robusto para todos os sistemas e componentes de IA/ML fornecidos ou integrados no Citi. Isso inclui projeto, desenvolvimento, teste, implantação e manutenção contínua seguros.
2. Os sistemas de IA fornecidos pelo fornecedor devem demonstrar integridade em suas operações e exibir resistência robusta a ataques adversários. Isso inclui a implementação de mecanismos para detecção de “prompt injection” e higienização de entradas, bem como a manutenção do isolamento de dados.
3. Os agentes e componentes de IA fornecidos pelos fornecedores devem interagir com os sistemas do Citi e outras ferramentas de forma segura. Isso exige um gerenciamento robusto de identidade e acesso, uma validação rigorosa dos argumentos de execução das ferramentas e o isolamento de operações de ferramentas de alto risco. Mecanismos de “Human-in-the-Loop” (HITL) devem ser incorporados para ações sigilosas ou de alto risco.

4. Os sistemas de IA dos fornecedores devem gerar registros abrangentes, imutáveis e auditáveis de todos os eventos significativos. Esses registros devem ser protegidos contra adulteração, agregados e mantidos de acordo com as políticas do Citi. Os recursos contínuos de monitoramento e detecção de anomalias são necessários para identificar e alertar sobre incidentes relevantes de segurança e atividades suspeitas.
5. Os sistemas de IA do fornecedor devem apoiar a supervisão humana baseada em risco, permitindo intervenção apropriada e ser projetados com uma responsabilidade clara para as realizações e ações de IA. Isso inclui classificar os resultados de IA por nível de risco e oferecer suporte a recursos de intervenção humana.
6. Todos os agentes, componentes e sistemas de IA fornecidos pelos fornecedores devem implementar controles robustos de gestão de identidade e acesso. Toda interação de IA deve ser atribuída a uma identidade identificável (humana ou não humana), com autenticação necessária para todo acesso. Os agentes de IA devem usar identidades gerenciadas e seguir os princípios de privilégio mínimo ao acessar os recursos do Citi.
 - a. Os Fornecedores devem provisionar e garantir que todos os agentes de IA recebam identidades de agentes da Citi Object Identity Network (COIN), federadas com os sistemas de Gestão de Identidade e Acesso (IAM) do Citi, para permitir a aplicação das políticas de segurança do Citi, gestão centralizada de identidade e possibilidade de auditoria.
 - b. Os Fornecedores devem integrar agentes terceirizados à COIN usando mecanismos de integração aprovados pelo Citi, incluindo a API de COIN disponibilizada por meio de gateways seguros (como SSG Gateway ou Apigee) e devem garantir que essa integração seja realizada de maneira segura de acordo com os requisitos de segurança aplicáveis do Citi.
 - c. Os Fornecedores, se hospedados internamente, devem gerar seus tokens que se alinham com a COIN; os Fornecedores hospedados externamente e autenticando em entrada com seu próprio token federado precisam ter um token de troca apoiado por tokens do Citi, por exemplo, troca de tokens MSFT para COIN. Qualquer novo tipo de token que não seja atualmente aceito pela exchange deve ser analisado para aprovação pela equipe de IAM do Citi.
7. Quando fornecedores utilizam ou disponibilizam servidores ou clientes do Model Context Protocol (MCP), eles devem implementar o MCP RFC 7591, incluindo todos os recursos opcionais.
8. Os sistemas de IA do fornecedor devem proteger as instruções do sistema e os trabalhos internos contra divulgação ou manipulação. A gestão de contexto deve impor limites rígidos para evitar vazamento de dados entre tenants, usuários ou ambientes.
9. Os Fornecedores devem ter procedimentos documentados para detectar, responder e relatar incidentes de segurança específicos de IA, incluindo ataques de disputa, manipulação de modelo, ações não autorizadas de IA ou violações de dados envolvendo sistemas de IA. O Citi deve ser notificado imediatamente sobre esses incidentes.

18 DIRETRIZES DE LOCAL DE TRABALHO SEGURO

Aplicável aos Fornecedores que acessam/processam/armazenam/gerenciam Informações do Citi E/OU hospedam aplicações que usam a Internet com marca do Citi E/OU têm conectividade aos recursos de rede do Citi E/OU exigem acesso sem acompanhamento às instalações do Citi.

Os Fornecedores devem proteger os ativos tangíveis e intangíveis do Citi e de seus clientes. Os ativos do Citi e dos Clientes podem ser usados apenas para fins aprovados e de maneiras aprovadas (por exemplo, de acordo com as licenças, termos e condições aplicáveis) e, então, apenas com respeito aos fins comerciais do Citi e dos Fornecedores do Citi. Os ativos incluem dinheiro, títulos mobiliários, propriedade física, serviços, planos de negócios, Informações do Citi, informações de Fornecedores, informações de distribuidores, propriedade intelectual (programas de computador, modelos e outros itens) e todas as outras informações pessoais, exclusivas e confidenciais. A apropriação indevida ou divulgação não autorizada de ativos do Citi é uma violação de sua obrigação com o Citi e pode constituir um ato de fraude contra o Citi. De modo semelhante, negligência, desperdício ou uso não autorizado com relação aos ativos do Citi também é uma violação de sua obrigação para com o Citi.

Item	Exigências
Informações do Citi (documentação eletrônica e impressa)	Trancar e proteger as Informações do Citi depois do horário normal do trabalho e sempre que o fornecedor estiver longe do espaço de trabalho designado.
Computadores Pessoais (PCs) e Notebooks	Computadores pessoais e notebooks usados para acessar ou visualizar informações do Citi devem ser protegidos por senhas de proteção de tela depois de um período de inatividade. Sempre que um fornecedor sair do espaço de trabalho designado, deve bloquear o computador e/ou notebook com CTRL + ALT + DEL e selecionar "Bloquear computador". Se um fornecedor estiver usando um notebook para visualizar informações do Citi, deverá garantir que tal notebook fique preso à unidade base por meio de cabo ou trava de segurança durante o horário de expediente e guardado com segurança no final do horário normal de trabalho.
Trancar	Armários de arquivo e gavetas que armazenam Informações do Citi devem ser trancados depois do horário normal do trabalho.
Áreas Abertas do Escritório	As áreas abertas do escritório não devem ser usadas como servidor de arquivos/minicentro de dados para armazenar Informações do Citi, a menos que tenham sido concebidas especificamente para esse uso e documentadas no Citi.
Bandejas de Impressoras, Fotocopiadoras e Fax	Todo o material relacionado ao Citi deve ser retirado de impressoras, fotocopiadoras e bandejas de fax.

Item	Exigências
Descarte	Descarte de Informações do Citi que não são mais necessárias (siga os cronogramas de retenção específicos). Os documentos devem ser picados ou colocados em uma lixeira de reciclagem segura/trancada. Mídias magnéticas devem ser descartadas de maneira segura depois dos procedimentos adequados de apagamento serem seguidos.

19 INTELIGÊNCIA ARTIFICIAL/APRENDIZADO DE MÁQUINA (INCLUINDO IA GENERATIVA/IA AGÊNTICA)

Aplicável a Fornecedores que utilizam Inteligência Artificial/Aprendizado de Máquina (IA/ML), incluindo IA Generativa IA/Agêntica, conforme definido pelo Citi nestas Exigências para Fornecedores, em qualquer parte do produto/serviço que estejam fornecendo.

19.1 O Fornecedor não deverá utilizar, e deverá garantir que quaisquer Subcontratados não utilizem, a IA/ML descrita abaixo, a menos que tal utilização tenha sido acordada entre as Partes no Anexo ou na Ordem de Serviço aplicável de acordo com o Contrato:

- a. Usada, contida ou de outra forma incorporada em qualquer produto ou serviço para o qual esteja sob Contrato para fornecer direta ou indiretamente ao Citi, ou em qualquer parte dele, incluindo qualquer produto ou serviço de terceiros contido ou incorporado nele; ou
2. Utilizada de qualquer maneira na execução de qualquer Contrato pelo Fornecedor, independentemente de tal IA/ML ser usada, contida ou incorporada de outra forma no produto ou serviço real que está sendo entregue ao Citi; ou
3. Utilizada pelo Fornecedor de qualquer maneira que possa expor as Informações do Citi a tal IA/ML, incluindo, entre outros, qualquer IA/ML utilizada pelo Fornecedor em suas operações de negócios não comerciais (por exemplo, manutenção de registros comerciais, melhorias de processos, pesquisa e desenvolvimento, conformidade e auditoria interna).

19.2 A falha do Fornecedor em cumprir essas obrigações será considerada uma violação relevante dos termos deste Contrato.

19.3 Se solicitado por um regulador, como parte de qualquer inspeção regulatória ou investigação forense sobre o uso de IA/ML em qualquer parte do produto/serviço, o Fornecedor deve ajudar o Citi a responder à solicitação do regulador, incluindo conduzir e/ou facilitar a realização de auditorias de algoritmos necessárias para descobrir as operações reais dos algoritmos compreendidos nos modelos de IA/ML.

19.4 Os seguintes princípios também devem ser observados:

Legalidade. A IA/ML do fornecedor cumprirá a Lei Aplicável.

Finalidade e Proporcionalidade. O Fornecedor não deve mesclar Conteúdo ou Informações do Citi com o Fornecedor ou quaisquer dados de terceiros. O Fornecedor não deve usar Conteúdo ou Informações do Citi para treinar IA/ML sem aprovação por escrito do Citi. A IA/ML do Fornecedor não usará Conteúdo ou Informações do Citi, exceto na medida necessária para a prestação dos Serviços.

20 RECLAMAÇÕES DO CLIENTE

20.1 Uma Reclamação é uma comunicação verbal ou escrita, que pode ser recebida verbalmente (pessoalmente ou por telefone) ou por escrito (por correio ou por meio de comunicações eletrônicas, como e-mail, chat ou mídia social etc.), que expressa insatisfação de um Cliente, não Cliente, Cliente potencial, cliente do Citi, Cliente potencial ou representante autorizado de um Cliente (em conjunto, “Cliente”) sobre uma Política do Citi, produto ou serviço oferecido pelo Citi ou por meio do Citi, um funcionário do Citi, contratado do Citi ou um prestador de serviços terceirizado agindo em nome do Citi ou qualquer combinação do acima exposto.

20.2 Os Fornecedores devem adotar a Política de Tratamento de Reclamações de Clientes do Citi, bem como quaisquer Normas e Procedimentos aplicáveis relacionados à Reclamação do Citi. O Fornecedor notificará seu principal contato comercial (ou representante) do Citi por escrito no prazo de vinte e quatro (24) horas após qualquer apresentação escrita ou oral de insatisfação ou preocupação (individualmente, “Reclamação”) recebida pelo Fornecedor de qualquer Cliente (ou não Cliente ou Cliente potencial, de acordo com a definição de Reclamação do Citi) ou de qualquer Regulador relacionada aos Serviços prestados pelo Fornecedor em nome do Citi, ou de outra forma relacionada ao Citi. A menos que o Citi disponibilize tal sistema ao Fornecedor, o Fornecedor também desenvolverá, implementará e manterá um sistema (“Sistema de Rastreamento”) razoavelmente satisfatório ao Citi para rastrear Reclamações e fornecer ao Citi, a seu critério, uma cópia dos relatórios ou acesso ao sistema. O Sistema de Rastreamento:

- a. categorizará as Reclamações por tipo, data de recebimento e data em que a notificação da Reclamação foi fornecida ao Citi,
- b. acompanhará o andamento do tratamento da Reclamação até a conclusão/resolução, e
- c. se encarregará de todos os outros assuntos que possam ser razoavelmente solicitados pelo Citi. O Sistema de Rastreamento deve ser projetado para permitir que o Fornecedor determine se recebe um número excessivo de Reclamações sobre um assunto específico para que o Fornecedor (em consulta com o Citi) possa determinar se há um problema sistêmico relacionado aos negócios do Fornecedor ou sua prestação de Serviços e prontamente corrigir os problemas.

21 POLÍTICA DE NEGOCIAÇÃO E INVESTIMENTO PESSOAL

A Política de Negociação e Investimento Pessoal (PTIP) do Citi define atividades de negociação e investimento permitidas e proibidas, requisitos de pré-autorização e requisitos relativos à manutenção, divulgação e monitoramento de contas de corretagem ou negociação de uma Pessoa Coberta. Estabelece padrões mínimos para promover compliance com as leis e regulamentos para evitar o uso inadequado da posição ou relacionamento de um indivíduo com o Citi, incluindo o conhecimento do indivíduo sobre (1) Informações Não Públicas Relevantes ou informações internas (em conjunto chamadas de “MNPI”) em relação ao Citi ou a um terceiro; ou (2) informações sobre posições, transações e estratégias de valores mobiliários, derivativos e commodities de clientes.

Todo o pessoal do Fornecedor que requer acesso regular a MNPI como parte de suas responsabilidades de trabalho no Citi e é designado como Pessoas Cobertas e/ou pessoas com Acesso do Citi deve cumprir os requisitos do PTIP. O pessoal do Fornecedor deve cumprir as solicitações da ICRM relacionadas à divulgação de contas pessoais, pré-autorização de atividades de negociação pessoal e restrições a negociações pessoais e envio de demonstrações periódicas.

22 NORMAS DE FATURAMENTO E COBRANÇA

Em conexão com os esforços do Citi para melhorar a pontualidade do serviço e aprimorar os controles, todos os Fornecedores devem apoiar os métodos preferidos de envio de faturas do Citi, bem como as opções de pagamento preferenciais de faturas, conforme detalhado abaixo:

- O Fornecedor criará arquivos eletrônicos a serem transmitidos ao Citi no formato comunicado pelo Citi ao Fornecedor e/ou utilizará a ferramenta iSupplier do Citi para inserir os dados de cobrança/faturamento necessários para a transmissão digital subsequente ao Citi.
- O Fornecedor fornecerá ao Citi todas as informações bancárias e documentação comprobatória necessárias para facilitar o pagamento eletrônico ao Fornecedor e/ou utilizar a oferta de pagamentos com Cartão Virtual do Citi (quando disponível).

Observação: os prazos de pagamento são calculados a partir da data em que a fatura enviada é recebida pelo Citi.

Para pagar em tempo hábil e cumprir os compromissos contratuais, o Citi exige que todos os Fornecedores incluam os seguintes dados da fatura e cumpram as diretrizes associadas ao faturar o Citi por bens ou serviços:

1. A entidade comercial correta do Citi, endereço para “Cobrança” e nome do contato de negócios associado do Citi.
2. Número da Fatura, Data da Fatura e Número do Pedido de Compra.

3. As faturas devem ser enviadas para o local ou endereço de e-mail do Citi detalhado no pedido de compra do Citi.
4. Bens ou serviços sendo faturados devem ter detalhes claros e descritivos na fatura.
5. Incluir apenas os encargos atuais para a fatura específica (não incluir outros saldos não pagos de faturas pendentes).
6. As faturas devem estar em inglês, incluindo documentação comprobatória.

23 POLÍTICA DE AUSÊNCIA OBRIGATÓRIA

A Política de ausência obrigatória do Citi exige que os indivíduos que desempenham atividades sigilosas ou de alto risco particularmente aquelas que afetam os registros contábeis e a documentação da empresa, se afastem periodicamente de tais funções. Esse afastamento compulsório visa fortalecer os controles internos, criando oportunidades para detectar possíveis fraudes, roubos ou outras condutas inadequadas que, de outra forma, poderiam permanecer ocultas. A política está em conformidade com as expectativas de supervisão estabelecidas pelo Federal Reserve Board dos EUA em relação às ausências obrigatórias para profissionais em cargos sigilosos.

Todos os profissionais de fornecedores que tenham acesso a dados sigilosos, como parte de suas responsabilidades no Citi, e que sejam designados como pessoas em funções “Sigilosas” devem cumprir os requisitos da MA Police. Pessoas nessas funções sigilosas são obrigadas a agendar e cumprir integralmente, a cada ano, um Período de Ausência Obrigatória, observando todas as regras e restrições da política. Durante esse período, não devem realizar, instruir, autorizar ou aprovar quaisquer atividades sigilosas, nem responder de forma substantiva a quaisquer comunicações – incluindo interações com clientes – exceto para redirecionar solicitações para o profissional responsável pela substituição. Caso o período de ausência precise ser interrompido após o seu início, os gestores ou contatos de negócios do Citi devem cancelá-lo nos sistemas de Compliance para que o acesso ao sistema seja restabelecido. Na sequência, o colaborador deverá agendar um novo período de ausência.

APÊNDICE – DEFINIÇÕES

Air – Gap é uma medida de segurança na qual um computador, sistema ou rede é fisicamente separado de outros computadores, sistemas ou redes. Uma arquitetura de backup de dados com air-gap limita a exposição a um ataque cibernético e permite a restauração de dados até um ponto no tempo antes do início do ataque.

Lei Aplicável inclui: (a) leis e regulamentos estaduais de execução e (b) as regras, diretrizes e outros comunicados emitidos por várias agências federais dos Estados Unidos, incluindo o Office of the Comptroller of the Currency, às vezes chamadas de Diretrizes e Regulamentos de Sinais de Alerta (Red. Flag Guidelines and Regulations), implementando a seção 114 da Lei de Transações de Crédito Justas e Precisas de 2003

Zona de Disponibilidade é onde o Provedor de Serviço de Nuvem tem um grupo de data centers lógicos. Uma Zona de Disponibilidade é um ou mais data centers discretos com energia, rede e telecomunicações redundantes em uma Região de Nuvem.

Inteligência Artificial (IA) refere-se a um método quantitativo, sistema ou abordagem (“técnicas”) que emula a inteligência humana por meio de programas de computador para fazer estimativas, previsões, recomendações ou decisões de maneiras que vão além das abordagens estatísticas, matemáticas, econométricas ou financeiras clássicas. Isso inclui todas as categorias de IA estabelecidas abaixo, bem como variações de IA – por exemplo: Modelos de IA Generativa, IA Agêntica, Grandes Modelos de Linguagem, IA de Propósito Geral (GPAI) etc.

As categorias de IA incluem:

- **IA Estática:** Técnicas de IA treinadas manualmente off-line ou cujos parâmetros são explicitamente programados e usados para fazer estimativas, previsões, recomendações ou decisões.
- **IA Dinâmica:** Técnicas que, ao contrário da “IA Estática”, podem retreinar automaticamente os parâmetros periodicamente, em produção.
- **IA Automática:** Técnicas de “IA Dinâmica” que adicionalmente são capazes de alterar automaticamente sua estrutura básica (por exemplo, hiperparâmetros, variáveis de entrada).
- **IA Cognitiva:** Técnicas que podem tomar decisões de forma autônoma e agir em conformidade, mesmo em assuntos para os quais não foram treinadas especificamente.

Aprendizado de Máquina (ML) é o subconjunto de IA que deriva representações ou inferências de dados sem programar explicitamente cada representação de parâmetro ou etapa de computador; por exemplo, Random Forests, abordagens baseadas em rede neural. Em contraste, as técnicas de IA que não são membros do subconjunto de ML incluem técnicas como lógica difusa, técnicas de análise de dependência complexa para processamento de linguagem natural.

Business Activity Owner (BAO) é um funcionário do Citi responsável por executar e gerenciar ativamente determinadas atividades associadas a relacionamentos com Fornecedores.

Facilitador de Negócios é um Fornecedor contratado pelo Citi para agir em nome do Citi para identificar novas oportunidades de negócios ou gerenciar relacionamentos com clientes existentes.

Presente de Negócios é qualquer item de valor (exceto entretenimento de negócios) dado ou recebido por um funcionário do Citi em conexão com negócios do Citi ou negócios da parte externa, geralmente incluindo itens no valor de US\$ 25 ou menos.

Informações do Citi são informações que o Citi possui ou é obrigado a proteger durante o armazenamento, processamento, transmissão ou descarte em formatos digitais e não digitais.

Classificações de Informações do Citi Incluem:

Confidenciais são Informações sobre negócios e/ou partes relacionadas do Citi que não fazem referência a indivíduos e exigem um alto nível de proteção. O comprometimento da confidencialidade, integridade ou disponibilidade dessas informações pode ter um impacto sério nas operações, situação financeira, franquia ou clientes corporativos do Citi.

Informações de Identificação Pessoal Confidenciais são Informações Pessoais sobre um indivíduo que têm o potencial de facilitar atividades ilegais, como roubo de identidade, fraude de crédito ou outra fraude financeira contra o referido indivíduo. O comprometimento da confidencialidade, integridade ou disponibilidade dessas informações pode ter um impacto significativo sobre o(s) indivíduo(s), incluindo, entre outros, perda financeira ou fraude.

- Elementos de dados pessoais que, quando combinados com outros dados pessoais, constituem PII Confidenciais incluem nome ou informações de contato individuais (endereço, telefone ou endereço de e-mail) em combinação com:
 - Elementos de dados de transações que podem resultar em movimentação de fundos ou podem ser usados para cometer roubo de identidade ou fraude, como:
 - Número de cartão de crédito/débito
 - Valor de Verificação do Cartão (CVV) ou PIN
 - Dados de relatório de crédito (pontuação de crédito)
 - Data de nascimento completa
 - Desempenho do trabalhador (avaliação/feedback) ou informações de remuneração
 - Gravações de vídeo, incluindo gravações de CCTV e ATM
- Certos elementos de dados pessoais isoladamente devem constituir PII Confidenciais:
 - Um número de Seguro Social dos EUA, número de identificação emitido pelo Governo (que seja equivalente ao número de Seguro Social dos EUA em termos de uso e/ou proteção legal), número de passaporte, número de carteira de habilitação ou número de contribuinte de um indivíduo

Interna é Informação que não é sobre um indivíduo, destinada a fins comerciais e requer um nível moderado de proteção. O comprometimento da confidencialidade, integridade ou disponibilidade dessas informações pode ter um **impacto limitado** em uma equipe ou grupo de trabalho.

- **Informações de Identificação Pessoal (PII)** Informação pessoal é qualquer informação que:

- Identifique ou possa ser usada para identificar um indivíduo ou família (como nome, assinatura, endereço, identificador nacional único, como número de seguro social ou número de registro de residente, data de nascimento, número da carteira de habilitação).
- Esteja relacionada, descreva, possa ser associada a, ou poderia ser razoavelmente vinculada (direta ou indiretamente) a um indivíduo ou família;
- Possa ser usada para autenticar um indivíduo ou fornecer acesso a uma conta (como nome de usuário, endereço de e-mail, senha, número de identificação pessoal (PIN), resposta a perguntas de segurança); ou se relaciona com um indivíduo e que pode ser sigilosa (como informações médicas ou de saúde pessoais, número da conta, valor da conta).
- As Informações Pessoais também incluem Informações Protegidas de Saúde (conforme definido pela Lei de Responsabilidade e Portabilidade de Seguros de Saúde dos Estados Unidos), Informações Pessoais Sigilosas e Informações de Crédito (conforme definido em várias leis de proteção/privacidade de dados e confidencialidade bancária).

Públicas são informações livremente disponibilizadas fora do Citi ou que se destinam a serem utilizadas pelo público, como comunicados à imprensa do Citi ou artigos que aparecem nas notícias sobre o Citi.

Restritas são Informações cujo uso é limitado a pessoas ou grupos específicos que são mais sigilosos para o Citi ou suas afiliadas e exigem o mais alto nível de proteção. O comprometimento da confidencialidade, integridade ou disponibilidade dessas informações pode ter um **impacto grave (em toda a empresa, várias regiões, vários setores)** nas operações, situação financeira, franquia ou clientes corporativos do Citi.

- **PII Sigilosas** Informações Pessoais que, nos termos de leis específicas, exigem proteção adicional, que podem ser potencialmente usadas para discriminar ilegalmente ou causar injustiça ou danos a um indivíduo. O comprometimento da confidencialidade, integridade ou disponibilidade dessas informações pode ter um impacto significativo sobre o(s) indivíduo(s), incluindo, entre outros, perda financeira, fraude ou impacto discriminatório.
- Dados especificamente relacionados com: informações sobre raça, religião ou crença religiosa, etnia, filiação ou opiniões políticas, associação a sindicatos, antecedentes criminais ou crimes, dados genéticos, dados biométricos ou dados relativos à orientação ou atividade sexual de um indivíduo.
 - Informações sobre a Saúde Pessoal (PHI), que incluem informações sobre o histórico médico ou condição mental ou física do indivíduo.

Cliente significa qualquer cliente do Citi e pode incluir indivíduos (ou seja, pessoas naturais), bem como empresas, instituições, organizações e pessoas jurídicas.

Região de Nuvem é um local físico onde o Provedor de Serviços de Nuvem agrupa o(s) data center(s).

Equipamentos, Sistemas e Serviços de Comunicação são qualquer hardware, software ou aplicativo usado na transmissão de comunicações eletrônicas escritas, de voz ou de vídeo. Entre os Canais de eComm estão: computadores, laptops, tablets, dispositivos móveis ou telefones celulares, incluindo “Bring Your Own Device” (BYOD), BlackBerry, telefone, facsimile (serviços de fax), acesso à intranet e à internet, serviços Wi-Fi, serviços de e-mail, mensagens instantâneas serviços como mensagens do Microsoft Lync, Skype e Bloomberg, sites e aplicativos com recursos de comunicação incorporados, plataformas de videoconferência ou colaboração, como Zoom ou Microsoft Teams, e serviços de mídia social, serviços interativos de

compartilhamento de informações, salas de bate-papo de terceiros, quadros de avisos eletrônicos e blogs.

Conteúdo significa as Informações Confidenciais do Citi e quaisquer outros dados, relatórios, estatísticas ou informações de qualquer tipo (a) fornecidos ou disponibilizados direta ou indiretamente ao Fornecedor por ou em nome do Citi ou de suas Afiliadas ou por ou em nome de seus clientes ou prestadores de serviços, (b) criados, produzidos por meio dos Serviços ou (c) derivados de qualquer um dos anteriores.

Contrato é um documento legal por escrito, assinado por duas ou mais partes, que inclui oferta, aceitação, contraprestação, obrigações das partes e legalidade do objetivo. Exemplos de Contratos podem incluir Acordos Gerais para produtos e serviços, especificações de trabalho/ordens de serviço, alterações e adendos, cronograma, pedidos, ou qualquer outro documento escrito e assinado por uma entidade do Citi e um Fornecedor. Um Acordo de Confidencialidade (NDA) também é considerado um Contrato para os fins desta política

Teste de Denial of Access (DOA) valida a equipe e o suporte do Fornecedor para os processos de negócios do Citi que podem ser recuperados no prazo de RTO definido.

Teste de Denial of Service (DOS) valida que o aplicativo do Fornecedor e os componentes subjacentes da infraestrutura que dão suporte aos negócios do Citi podem ser recuperados dentro do RTO definido.

“Materiais de Depósito” significa as seguintes subseções (i)-(vi), coletivamente, com relação, conforme aplicável, ao software licenciado para o Citi para operação no ambiente do Citi ou aos materiais usados pelo Fornecedor para Serviços Hospedados fornecidos ao Citi:

- (i) Uma versão exata e duplicada do Código-Fonte para o software usado para o desenvolvimento, operação, manutenção e suporte do software licenciado ou Serviços Hospedados estabelecido no contrato aplicável com o Citi (e todas as versões subsequentes de tal software ou Serviços Hospedados) e toda a Documentação para esse software (independentemente de o Citi já poder ter uma cópia de partes desse Código-Fonte) (“**Depósito do Código-Fonte**”);
- (ii) O Código-Fonte para qualquer software de terceiros ao qual o Fornecedor tenha direitos com relação ao desenvolvimento, operação e manutenção e suporte do software licenciado ou Serviços Hospedados;
- (iii) Uma cópia licenciada de todas as ferramentas de software, como depuradores, montadores e compiladores necessários para converter o Código-Fonte incluído nos Materiais de Depósito em formulário executável, conforme necessário para operar, manter e apoiar o software ou os Serviços Hospedados;
- (iv) Na medida que ainda não foi fornecida acima, qualquer Documentação que forneça o seguinte: (A) descrições gerais e operações dos Materiais de Depósito; (B) arquitetura e funções básicas do programa; (C) informações de fluxo de dados; (D) mapa e lista de memória detalhada; (E) mapas de porta de entrada/saída; e (F) outros detalhes que permitiriam que um programador com habilidade comum nas linguagens de programação aplicáveis usasse e modificasse o Código-Fonte incluído nos Materiais de Depósito;
- (v) Todas as outras informações técnicas relacionadas ao software ou Serviços Hospedados, conforme razoavelmente necessário para permitir que o Citi, ou um terceiro competente em nome do Citi, use, opere, modifique e aprimore o software ou Serviços Hospedados; e

- (vi) Uma lista de todos os softwares e tecnologia de terceiros usados em conexão com o software ou Serviços Hospedados, incluindo detalhes razoáveis sobre seu uso no software e informações de contato para o provedor de tal software ou tecnologia. O Citi reconhece e concorda que os Materiais de Depósito não contêm qualquer código-fonte de terceiros além do estabelecido na subseção (ii); e
- (vii) com relação aos Serviços Hospedados:
 - a. uma réplica reduzida do ambiente de produção hospedado na nuvem ou materiais relacionados à nuvem específicos do ambiente e outras informações que são necessárias para replicar o ambiente de produção do Citi, incluindo (entre outros): infraestrutura como código, scripts de terraform, recurso de nuvem, modelos de formação de nuvem, arquivos de configuração, inquilinos de nuvem, assinaturas de nuvem, imagens de máquinas, imagens docker e infraestrutura como código-fonte do software; e
 - b. uma cópia dos dados do Citi mantidos dentro do software.

Comunicações Eletrônicas são mensagens ou informações enviadas, recebidas ou usadas pelo Pessoal por meios eletrônicos, transmitidas por fio ou por sinais sem fio. As comunicações eletrônicas incluem, entre outros, mensagens de texto, e-mail, mensagens instantâneas ponto a ponto, postagens em blogs, postagens em mídias sociais, mensagens enviadas por meio de aplicativos de mensagens como WhatsApp, WeChat, Line, Signal ou Viber, e incluem anexos, capturas de tela, arquivos gravados ou ao vivo de vídeo ou voz e arquivos criados, recebidos, baixados, armazenados, transmitidos, excluídos ou usados por meio de Equipamentos, Sistemas e Serviços de Comunicação Eletrônica.

IDs Funcionais são IDs genéricas, como ADMIN ou ROOT, que são usadas por uma pessoa ou processo para acessar um sistema de segurança. Uma importante iniciativa na operação de Gestão de Identidade e Acesso (IAM) é garantir que o Citi tenha controles específicos e definidos implementados para proteger contra os riscos que cercam o uso de IDs Funcionais.

Processos Críticos para a Franquia/Aplicativos Críticos para a Franquia (FA) são aqueles processos/aplicativos que foram identificados pelo Citi como essenciais para a execução bem-sucedida de suas funções comerciais críticas para a franquia.

Fraude é um ato intencional, declaração falsa ou omissão com o objetivo de enganar outras pessoas, resultando em perdas para a vítima ou na obtenção de ganho pelo perpetrador.

Serviços Hospedados incluem quaisquer Aplicativos Instalados e quaisquer instalações e ambientes gerenciados ou utilizados pelo Fornecedor para fornecer os Serviços Hospedados, todos os aplicativos e outros softwares, bancos de dados, sites, servidores, hardware, redes, telecomunicações e outros equipamentos e outras tecnologias instaladas ou usadas dentro do ambiente de Serviços Hospedados e, em cada caso, todas as Atualizações e Serviços de Suporte, mas excluindo todo o Conteúdo e Sistemas do Citi.

Dados de Verificação de Identidade (IVD) são definidos como perguntas de segurança (SQ) ou perguntas de autenticação baseada em conhecimento (KBA). As Perguntas de Segurança são normalmente definidas pelo aplicativo e respondidas pelo usuário final. Exemplos são o nome de solteira da mãe, local de nascimento, sorvete favorito etc. Ambos os tipos de perguntas devem ser tratados como Dados de Autenticação.

Segurança da Informação ou “IS” significa o estado em que um computador ou sistema de computador é protegido contra acesso não autorizado ou ataque e, graças a esse estado, (a) o computador ou sistema de computador continua disponível e operacional; (b) a integridade do computador ou sistema de computador é mantida e (c) a integridade e confidencialidade das

informações armazenadas, processadas ou transmitidas por meio do computador ou sistema de computador são mantidas.

Ameaça à IS significa um ato ou atividade (conhecido ou suspeito) realizado em um computador ou sistema de computador ou por meio dele que possa prejudicar ou afetar adversamente a segurança da informação desse computador ou de um outro computador ou sistema de computador.

Vulnerabilidade da IS significa qualquer vulnerabilidade em um computador ou sistema de computador que possa ser explorada por uma ou mais ameaças à IS.

Sem Geração de Receita/Cliente é definida como atividades cruciais de negócios não associadas a atividades de geração de receitas, incluindo atividades jurídicas, de supervisão, regulatórias e de Continuidade das atividades dos Negócios.

Acordo de Confidencialidade (NDA) é um acordo entre o Citi e um fornecedor em que a troca, utilização e divulgação de informações são regidas pelos termos do acordo.

Software de código aberto significa código-fonte ou um programa de computador compilado no qual o código-fonte está disponível para o público em geral para uso ou modificação de seu projeto original.

Pessoal significa, seja declarado diretamente ou derivado do contexto, o Fornecedor e suas afiliadas, diretores, executivos, funcionários, agentes, auditores, consultores, prestadores de serviços e contratados (excluindo o pessoal do Citi). O pessoal do Fornecedor também inclui diretores, executivos, funcionários, agentes, auditores, consultores ou outros representantes de qualquer Subcontratado.

Inventário de Registros é uma listagem detalhada que inclui os tipos de registro, localização, datas etc., de registros do Citi e é necessário para uma empresa gerenciar adequadamente seus registros ao longo do ciclo de vida das informações.

Retenção de Informações é um requisito colocado nos Registros e Informações que suspende a modificação ou descarte até que seja retirado pela autoridade que emitiu a retenção.

Capacidade de Recuperação é o volume, quantidade ou velocidade de entrega dos produtos e serviços do Fornecedor, expressos como porcentagem da entrega normal de produtos e serviços.

Duração da Recuperação é a duração máxima, em dias corridos, que o Fornecedor é capaz de sustentar operações enquanto está no modo de recuperação.

Objetivo do Ponto de Recuperação é o ponto no tempo no passado, mencionado em horas, em que os dados devem ser recuperados depois de uma interrupção de negócios. É o período específico máximo no qual os dados podem ser perdidos de um serviço de TI devido a um incidente importante. O ponto de recuperação (Recovery Point Objective, RPO) é apenas uma medida do período de tempo máximo no qual os dados podem ser perdidos se houver um incidente grave que afete um serviço de TI. Não é uma medida direta de quantos dados podem ter sido perdidos, por exemplo, ao final do processamento do dia anterior.

Objetivo de Tempo de Recuperação é a duração em horas entre o momento de uma interrupção de serviço e a restauração dos produtos e serviços.

“Evento de Liberação” significa qualquer um ou mais dos seguintes itens:

- (i) O Fornecedor (A) torna-se insolvente ou admite sua incapacidade de pagar suas dívidas em geral à medida que se tornam devidas; (B) torna-se sujeito, voluntária ou

involuntariamente, a qualquer processo de acordo com qualquer lei de falência ou insolvência nacional ou estrangeira que não seja totalmente suspenso dentro de sete (7) dias úteis ou não seja extinto ou cancelado dentro de quarenta e cinco (45) dias após a propositura; (C) faz uma atribuição geral para o benefício de credores; ou (D) tem um depositário judicial, administrador, custodiante ou agente semelhante nomeado por ordem de qualquer tribunal de jurisdição competente para assumir ou vender qualquer parte relevante de sua propriedade ou negócio.

Organização de Gestão de Recursos (RMO) é a responsável pela gestão global de recursos de ponta a ponta do Citi, incluindo Recursos Estratégicos, Operações da Compra ao Pagamento, Departamento de Recursos Humanos e Estrutura de Gestão de Fornecedores.

Gestor de Recursos de RMO é uma pessoa na Organização de Gestão de Recursos (RMO) que é responsável pela negociação dos termos de negócios, requisitos e fixação de preços do Contrato, incluindo RFPs e outras atividades de seleção de Fornecedores, administração dos termos e condições do Contrato e requisitos de reconhecimento de avaliação financeira.

Um efeito adverso Grave ou Catastrófico para um indivíduo significa que seria razoável esperar que o impacto possa resultar em efeitos adversos para o indivíduo, incluindo perda financeira, perda de emprego ou perda ou dificuldade para encontrar emprego, perda de direitos humanos, humilhação pessoal ou pública ou prisão indevida.

Subcontratado: um subcontratado é uma quarta parte (pessoa ou entidade), que foi contratado por um terceiro para executar alguns ou todos os serviços ou atividades que o Citi contratou com o terceiro.

Orientação:

Q1: Todos os subcontratados do Terceiro precisam ser reportados?

A1: Somente subcontratados relacionados ao serviço que está sendo executado precisam ser reportados. Exemplos de serviços ou atividades realizadas por um subcontratado incluem, entre outros:

*Um subcontratado que presta serviços de tecnologia ou software que direta ou indiretamente apoiam o serviço/atividades que o Citi contratou para o Terceiro; ou

*Um subcontratado cujos serviços incluem acesso a informações Confidenciais ou acima do Citi; ou

*Um subcontratado que tenha interação direta ou indireta com qualquer Cliente existente/potencial do Citi; ou

*Um subcontratado que não é acompanhado e realiza serviços de trituração ou arquivamento de documentos do Citi dentro ou fora de qualquer instalação do Citi; ou

*Um subcontratado que dá suporte às principais funções ou serviços bancários, como pagamentos, cobrança, empréstimos etc.

Fornecedor: para os fins deste documento de “Exigências do Citi para Fornecedores”, um “Fornecedor” refere-se exclusivamente a um Terceiro Externo que celebrou um acordo comercial para fornecer produtos ou serviços diretamente a uma Entidade do Citi ou para apoiar uma Entidade do Citi no cumprimento de seus objetivos de negócios. Um Terceiro Externo é definido como uma entidade que não é do Citi. Os Fornecedores também podem ser clientes de uma Entidade do Citi ou podem apoiar interações com clientes do Citi; no entanto, os acordos baseados exclusivamente em sua qualidade de cliente do Citi não são considerados relacionamentos com fornecedores no escopo deste documento.

Informações Transitórias: um Registro é a versão final e mais completa das informações que o Citi é obrigado a manter por motivos comerciais legais, regulatórios ou aprovados. Todas as outras informações são classificadas como “Informações Transitórias”.