IBM Security Trusteer Fraud Protection

Os Termos de Uso ("ToU") são compostos por estes Termos de Uso da IBM – Termos da Oferta Específica do SaaS ("Termos da Oferta Específica do SaaS") e um documento denominado Termos de Uso da IBM - Termos Gerais ("Termos Gerais") disponível na URL a seguir: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Em caso de um conflito, os Termos da Oferta Específica do SaaS prevalecem sobre os Termos Gerais. Ao solicitar, acessar ou usar o IBM SaaS, o Cliente concorda com estes ToU.

Os ToU são regidos pelo Contrato Internacional do IBM Passport Advantage, o Contrato Internacional do IBM Passport Advantage Express ou o Contrato Internacional IBM para Ofertas do IBM SaaS Selecionadas, conforme aplicável ("Acordo") e junto com os ToU formam o acordo completo.

1. IBM SaaS

As seguintes ofertas do IBM SaaS são cobertas por estes Termos da Oferta Específica do SaaS:

1.1 Ofertas IBM SaaS Rapport

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Ofertas IBM SaaS Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Ofertas IBM SaaS Mobile

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Métricas de Encargos

O IBM SaaS é vendido sob uma da(s) métrica(s) de encargos a seguir, conforme especificado no Documento de Transação:

a. **Participante Elegível** – é uma unidade de medida pela qual o IBM SaaS pode ser obtido. Cada indivíduo ou entidade elegível a participar em qualquer programa de entrega de serviço gerenciado ou controlado pelo IBM SaaS é um Participante Elegível. Autorizações suficientes devem ser obtidas para cobrir todos os Participantes Elegíveis gerenciados ou monitorados dentro do IBM SaaS durante o período de medição especificado no Documento de Transação do Cliente.

   Cada programa de entrega de serviço gerenciado pelo IBM SaaS é analisado separadamente e, então, incluído aos outros. Os indivíduos ou as entidades elegíveis para diversos programas de entrega de serviço requerem autorizações separadas.

   Para estas ofertas, um programa de entrega de serviços inclui um único Aplicativo de Negócios ou Varejo do Cliente com uma página de login principal e páginas relacionadas para cada Aplicativo de Negócios ou Varejo. Um Participante Elegível é um usuário final de um Cliente que possui credenciais de login no Aplicativo de Negócios ou Varejo.

b. **Dispositivo do Cliente** – é uma unidade de medida pela qual o IBM SaaS pode ser obtido. Um Dispositivo do Cliente é um único dispositivo de computação do usuário ou um sensor com propósito especial ou dispositivo de telemetria que solicita a execução ou recebe para execução um conjunto de comandos, procedimentos ou aplicativos ou fornece dados para outro sistema de computador que geralmente é referido como um servidor ou de qualquer outra forma gerenciado pelo servidor. Diversos Dispositivos do Cliente podem compartilhar acesso a um servidor comum. Um Dispositivo Cliente pode ter alguma capacidade de processamento ou ser programável para permitir que um usuário trabalhe. O Cliente deve obter autorizações para cada Dispositivo do Cliente que executa, fornece dados, usa serviços fornecidos ou, de qualquer outra forma, acessa o IBM SaaS durante o período de medição especificado no Documento de Transação do Cliente.

3. Encargos e Faturamento

A quantia a pagar pelo IBM SaaS estará especificada em um Documento de Transação.

3.1 Encargos Mensais Parciais

Um encargo mensal parcial conforme especificado no Documento de Transação pode ser acessado em uma base rateada.

4. Conformidade e Auditoria

O acesso às ofertas IBM Security Trusteer Fraud Protection está sujeito a uma quantidade máxima de Participantes Elegíveis ou Dispositivos do Cliente, conforme especificado no Documento de Transação. O Cliente é responsável por garantir que seu número de Participantes Elegíveis ou de Dispositivos do Cliente não exceda a quantidade máxima, conforme especificado no Documento de Transação.

Uma auditoria pode ser realizada para verificar a conformidade com a quantidade máxima de Participantes Elegíveis ou Dispositivos do Cliente.

5. Opções de Renovação do Período de Subscrição do IBM SaaS

O Documento de Transação do Cliente irá definir se o IBM SaaS será renovado no término do Período de Subscrição ao designar um dos seguintes:

5.1 Renovação Automática

Se o Documento de Transação do Cliente declarar que a renovação do Cliente é automática, o Cliente poderá rescindir o Período de Subscrição do IBM SaaS a expirar mediante uma solicitação por escrito para seu representante de vendas IBM ou Parceiro de Negócios IBM, com pelo menos 90 (noventa) dias de antecedência da data de expiração, conforme definido no Documento de Transação. Se a IBM ou seu Parceiro de Negócios IBM não receber tal aviso de rescisão até a data de expiração, o Período de Subscrição a expirar será automaticamente renovado por um ano ou a mesma duração que o Período de Subscrição original, conforme estabelecido no Documento de Transação.

5.2 Faturamento Contínuo

Quando o Documento de Transação declarar que a renovação do Cliente é contínua, o Cliente continuará a ter acesso ao IBM SaaS e será faturado pelo uso do IBM SaaS em uma base contínua. Para descontinuar o uso do IBM SaaS e parar o processo de faturamento contínuo, o Cliente precisará fornecer à IBM ou a seu Parceiro de Negócios IBM um aviso, por escrito, com noventa (90) dias de antecedência, solicitando o cancelamento do IBM SaaS do Cliente. Mediante o cancelamento do acesso do Cliente, ele será faturado por quaisquer encargos de acesso pendentes durante o mês em que o cancelamento entrou em vigor.

5.3 Renovação Obrigatória

Quando o Documento de Transação declarar que o tipo de renovação do Cliente é "rescindir", o IBM SaaS finalizará no término do Período de Subscrição e o acesso do Cliente ao IBM SaaS será removido. Para continuar a usar o IBM SaaS além da data de encerramento, o Cliente precisará colocar uma ordem com o representante de vendas IBM ou Parceiros de Negócios IBM do Cliente para adquirir um novo Período de Subscrição.

6. Suporte Técnico

O Suporte Técnico para o IBM SaaS está disponível para um Cliente e seus Participantes Elegíveis para ajudar em seu uso do IBM SaaS.

O Suporte Padrão está incluído na subscrição de todas as ofertas. O Trusteer Rapport Mandatory Service, que é um complemento ao Trusteer Rapport, tem um pré-requisito do Premium Support para a subscrição de base do Trusteer Rapport base.

Para cada oferta IBM SaaS, uma subscrição de Premium Support está disponível mediante um encargo adicional, com a exceção das ofertas IBM Security Trusteer Mobile SDK e das ofertas IBM Security Trusteer Rapport Mandatory Service.

Suporte Padrão:

- Suporte no horário local - 8h às 17h.
- Os Clientes e seus Participantes Elegíveis podem submeter chamados de suporte eletronicamente, conforme detalhado na publicação Software as a Service [SaaS] Support Handbook.
- Clientes podem acessar o Portal de Suporte a Clientes para obter notificações, documentos, relatórios de caso e Perguntas Frequentes em: http://www-01.ibm.com/software/security/trusteer/support/.
- Para opções e detalhes de suporte, acesse a publicação IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

Premium Support:

- Suporte 24x7 para todas as gravidades.
- Os Clientes podem obter suporte diretamente via telefone.
- Os Clientes e seus Participantes Elegíveis podem submeter chamados de suporte eletronicamente, conforme detalhado na publicação Software as a Service [SaaS] Support Handbook.

- Clientes podem acessar o Portal de Suporte a Clientes para obter notificações, documentos, relatórios de caso e Perguntas Frequentes em: http://www-01.ibm.com/software/security/trusteer/support/.
- Para opções e detalhes de suporte, acesse a publicação IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

7. Termos Adicionais da Oferta IBM SaaS

7.1 Conformidade com o Safe Harbor

A IBM adere ao U.S. – EU Safe Harbor Framework desenvolvido pelo U.S. Department of Commerce em coordenação com a Comissão Europeia. Os produtos IBM Security Trusteer são incluídos na certificação EU-U.S. Safe Harbor da IBM. Mais informações sobre o Safe Harbor e a lista de empresas do Safe Harbor podem ser localizadas aqui: http://export.gov/safeharbor/.

7.2 Aumento do Encargo Anual de Subscrição do Cliente

A IBM reserva-se o direito de ajustar o encargo de subscrição do IBM SaaS não mais do que uma vez a cada doze (12) meses em uma porcentagem a ser determinada pela IBM, não excedendo 3%. O ajuste do encargo de subscrição será efetivo no aniversário da data do período de cobertura inicial. Esta taxa de ajuste não altera a autorização do Cliente ao IBM SaaS ou a métrica de encargo pela qual o IBM SaaS é obtido. Os Parceiros de Negócios IBM são independentes da IBM e determinam unilateralmente os seus preços e prazos.

7.3 Suporte Premium

O Cliente está autorizado ao Suporte Premium apenas para as ofertas IBM SaaS para as quais o Cliente tenha subscrito a oferta de Suporte Premium associada.

7.4 Uso Legal e Consentimento

Autorização para Coletar e Processar Dados

O IBM SaaS é projetado para ajudar o Cliente a melhorar seu ambiente e dados de segurança. O IBM SaaS irá coletar informações dos Participantes Elegíveis e dos Dispositivos do Cliente que interagem com os Aplicativos de Negócios ou Varejo para os quais o Cliente assinou para obter a cobertura das ofertas IBM SaaS. O IBM SaaS coleta informações que sozinhas ou em combinação podem ser consideradas Dados Pessoais em algumas jurisdições. Dados Pessoais são quaisquer informações que podem ser usadas para identificar um indivíduo específico, tal como um nome, endereço de e-mail, endereço residencial ou número de telefone que é fornecido para a IBM armazenar, processar ou transferir em nome do Cliente.

Práticas de coleta e processamento de dados podem ser atualizadas para melhorar a funcionalidade do IBM SaaS. Um documento com uma descrição completa das práticas de coleta e processamento de dados é atualizado conforme necessário e está disponível para o Cliente mediante solicitação. O Cliente autoriza a IBM a coletar estas informações e processá-las de acordo com a seção Transferências entre Fronteiras e a seção Privacidade de Dados destes ToU e a seção Privacidade de Dados e Segurança de Dados dos Termos Gerais dos ToU.

Para as ofertas IBM Security Trusteer Pinpoint:

Os dados coletados podem incluir endereço IP do usuário, ID do usuário criptografado ou em hash unidirecional, cookies de domínio se não filtrados, visitas a Aplicativos protegidos e sites de phishing, localização geográfica e credenciais inseridas nos sites de phishing.

Para ofertas IBM Security Trusteer Mobile SDK e ofertas IBM Security Trusteer Mobile Browser:

Os dados coletados podem incluir endereço IP do usuário, ID do usuário criptografado ou em hash unidirecional, localização geográfica e visitas a Aplicativos protegidos, informações de cartão SIM, nome de dispositivo e afiliação do cliente.

Para as ofertas IBM Security Trusteer Rapport:

Dados coletados podem incluir endereço IP, ID do usuário criptografado ou em hash unidirecional, eventos de segurança, nome de usuário e endereço de e-mail fornecidos com o propósito de entrar em contato com a IBM para suporte ao Cliente, afiliação do cliente, senha criptografada inserida em sites protegidos, visitas a Aplicativos protegidos e sites de phishing, número de cartão de débito criptografado e arquivos e dados coletados remotamente pela equipe IBM para inspecionar malware suspeito, atividade maliciosa ou mau funcionamento.

Consentimento Informado dos Sujeitos de Dados:

O uso deste IBM SaaS pode envolver diversas leis ou regulamentos. O IBM SaaS só pode ser usado para propósitos legais e de uma forma legal. O Cliente concorda em usar o IBM SaaS em conformidade e assume toda a responsabilidade pelo cumprimento com as leis, os regulamentos e as políticas aplicáveis.

Para ofertas IBM Security Trusteer Pinpoint e para ofertas IBM Security Trusteer Mobile SDK:

O Cliente concorda que obteve ou irá obter quaisquer consentimentos totalmente informados, permissões ou licenças necessários para permitir o uso legal do IBM SaaS e para permitir a coleta e o processamento das informações pela IBM através do IBM SaaS.

Para ofertas IBM Security Trusteer Rapport e para ofertas e IBM Security Trusteer Mobile Browser:

O Cliente autoriza a IBM a obter os consentimentos totalmente informados necessários para permitir o uso legal do IBM SaaS e para coletar e processar as informações, conforme descrito no Contrato de Licença do Usuário Final disponível em https://www.trusteer.com/support/end-user-license-agreement. No caso do Cliente determinar que ele (e não a IBM) irá lidar com as comunicações de consentimento com usuários finais, o Cliente concorda que obteve ou obterá quaisquer consentimentos totalmente informados, permissões ou licenças necessários para permitir o uso legal do IBM SaaS e para permitir a coleta e o processamento das informações pela IBM como processador de dados do Cliente através do IBM SaaS.

7.5 Transferências entre Fronteiras

O Cliente concorda que a IBM pode processar o Conteúdo, incluindo quaisquer Dados Pessoais, sob leis e requisitos relevantes através das fronteiras de países para processadores e subprocessadores nos países a seguir fora da Área Econômica Europeia e países considerados pela Comissão Europeia como tendo níveis adequados de segurança: os EUA.

7.6 Privacidade de Dados

Caso o Cliente disponibilize Dados Pessoais para o IBM SaaS nos Estados Membros da União Europeia, Islândia, Liechtenstein, Noruega, Suíça ou se o Cliente tiver Participantes Elegíveis ou Dispositivos Clientes nesses países, então o Cliente como o único controlador nomeia a IBM como um processador para processar Dados Pessoais (conforme tais termos são definidos na EU Directive 95/46/EC). A IBM irá processar tais Dados Pessoais apenas na medida necessária para tornar a oferta IBM SaaS disponível de acordo com as descrições publicadas da IBM do IBM SaaS e o Cliente concorda que tal processamento está em conformidade com as instruções do Cliente. A IBM fornecerá um aviso prévio razoável se fizer uma mudança material no local de processamento ou na maneira como ela protege os Dados Pessoais como parte do IBM SaaS. O Cliente pode finalizar o Período de Subscrição atual para o IBM SaaS afetado, mediante notificação por escrito à IBM dentro de trinta (30) dias a contar da notificação da IBM da mudança para o Cliente. O Cliente concorda que a IBM pode processar conteúdo incluindo quaisquer Dados Pessoais através das fronteiras do país para os seguintes processadores e subprocessadores:

Nome do Processador/Subprocessador	Função (Processador ou Subprocessador de Dados)	Local*
A entidade contratante da IBM	Processador	Conforme indicado no Documento de Transação
Amazon Web Services LLC	Subprocessador	410 Terry Ave. N Seattle, WA 98109 Estados Unidos
Connectria Corp.	Subprocessador	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Estados Unidos
IBM Israel Ltd.	Subprocessador	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Subprocessador	1 New Orchard Rd. Armonk, NY 10504 Estados Unidos

O Cliente concorda que a IBM pode, no aviso, variar essa lista de locais de país quando determinar razoavelmente que isso é necessário para a provisão do IBM SaaS.

O Cliente concorda que o serviço fornecido através do datacenter da Alemanha, conforme determinado durante o processo de fornecimento ("provisioning"), a IBM pode processar conteúdo, incluindo quaisquer Dados Pessoais através das uma fronteiras do país para seguintes processadores e subprocessadores:

Nome do Processador/Subprocessador	Função (Processador ou Subprocessador de Dados)	Local*
A entidade contratante da IBM	Processador	Conforme indicado no Documento de Transação
Amazon Web Services (Alemanha)	Subprocessador	Munique, Alemanha
IBM Israel Ltd.	Subprocessador	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

O Cliente concorda que o serviço fornecido através do datacenter do Japão, conforme determinado durante o processo de fornecimento ("provisioning"), a IBM pode processar conteúdo, incluindo quaisquer Dados Pessoais através das fronteiras do país para seguintes processadores e subprocessadores:

Nome do Processador/Subprocessador	Função (Processador ou Subprocessador de Dados)	Local*
A entidade contratante da IBM	Processador	Conforme indicado no Documento de Transação
Amazon Web Services (Japão)	Subprocessador	Tóquio, Japão
IBM Israel Ltd.	Subprocessador	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* Os locais identificados nas tabelas acima incluem os endereços dos escritórios corporativos do Processador/Subprocessador. Os datacenters estão localizados no mesmo país identificado.

As partes ou suas filiais relevantes podem firmar contratos separados de Cláusula de Modelo da União Europeia padrão não modificados em suas funções correspondentes em conformidade com o EC Decision 2010/87/EU com cláusulas opcionais removidas. Todos os litígios ou responsabilidades oriundas desses contratos, mesmo se realizados pelas afiliadas, serão tratados pelas partes como se a disputa ou responsabilidade tivesse surgido entre elas sob os termos deste Contrato.

Apêndice A

1. Ofertas IBM SaaS

A IBM oferece estes serviços como serviços e ofertas independentes, ou como serviços e ofertas adicionais. As ofertas IBM SaaS específicas solicitadas são especificadas na PoE do Cliente.

1.1 Definições de Negócios e Varejo

Os produtos de fraude IBM Security Trusteer são licenciados para uso com tipos específicos de Aplicativos. Um Aplicativo é definido como um dos tipos a seguir: Varejo ou Negócios. Ofertas separadas estão disponíveis para Aplicativos de Varejo e Aplicativos de Negócios.

- Um Aplicativo de Varejo é definido como um aplicativo bancário online, aplicativo móvel ou aplicativo de e-commerce projetado para atender consumidores. A política do Cliente pode classificar determinadas pequenas empresas como elegíveis para acesso de varejo.
- Um Aplicativo de Negócios é definido como um aplicativo bancário online, aplicativo móvel ou aplicativo de e-commerce projetado para atender entidades corporativas, institucionais ou equivalentes, ou qualquer aplicativo que não seja categorizado como de Varejo.

1.2 Ofertas de Subscrição Base IBM SaaS

Ofertas de Negócios:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Ofertas de Varejo:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Para cada uma das ofertas de Negócios e Varejo, há um produto de Premium Support associado disponível mediante o pagamento de um encargo adicional, com a exceção das ofertas IBM Security Trusteer Mobile SDK.

1.3 Ofertas de Subscrição IBM SaaS Adicionais para Ofertas IBM Security Trusteer Rapport

Ofertas adicionais disponíveis para o IBM Security Trusteer Rapport for Business:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Ofertas adicionais disponíveis para o IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

Para cada um dos complementos de Negócios e Varejo para as ofertas IBM Security Trusteer Rapport, exceto para os complementos do IBM Security Trusteer Rapport Mandatory Service, há um produto de Premium Support associado disponível mediante o pagamento de um encargo adicional.

A subscrição do IBM Security Trusteer Rapport for Business ou IBM Security Trusteer Rapport for Retail é pré-requisito para as ofertas de subscrição IBM SaaS adicionais associadas listadas nesta seção.

1.4 Ofertas de Subscrição IBM SaaS Adicionais para Ofertas IBM Security Trusteer Pinpoint Malware Detection

Ofertas adicionais disponíveis para o IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Ofertas adicionais disponíveis para o IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

A subscrição de Premium Support está disponível mediante o pagamento de um encargo adicional para cada uma das ofertas IBM SaaS adicionais listadas nesta seção.

A subscrição das ofertas IBM Security Trusteer Pinpoint Malware Detection for Business ou das ofertas IBM Security Trusteer Pinpoint Malware Detection for Retail é um pré-requisito para as ofertas de subscrição IBM SaaS adicionais associadas listadas nesta seção.

1.5 Outras Subscrições Adicionais do IBM SaaS

Qualquer Subscrição IBM SaaS adicional para as subscrições base acima que não estiver listada aqui, seja atualmente disponível ou em desenvolvimento, não será considerada uma atualização e deverá ser concedida separadamente.

1.6 Definições

Titular da Conta – significa o usuário final do Cliente, que instalou o software de habilitação do cliente, aceitou o contrato de licença do usuário final ("EULA") e se autenticou pelo menos uma vez com o Aplicativo de Varejo ou de Negócios do Cliente para o qual o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS.

Software Cliente do Titular da Conta – significa o software de habilitação do cliente IBM Security Trusteer Rapport ou o software de habilitação do cliente IBM Security Trusteer Mobile Browser ou qualquer outro software de habilitação do cliente que é fornecido com algumas subscrições do IBM SaaS para instalação no dispositivo do usuário final.

Trusteer Splash – refere-se ao splash que é fornecido para Cliente com base em modelos splash disponíveis.

Página de Entrada – refere-se à página hospedada pela IBM que é fornecida para o Cliente com o splash do Cliente e o Software Cliente do Titular da Conta transferido por download.

2. Ofertas IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail e/ou IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

O Trusteer Rapport fornece uma camada de proteção contra phishing e ataques de malware Man-in-the-Browser (MitB). Usando uma rede de dezenas de milhões de terminais em todo o mundo, o IBM Security Trusteer Rapport coleta inteligência sobre ataques ativos de phishing e malware contra organizações no mundo inteiro. O IBM Security Trusteer Rapport aplica algoritmos comportamentais destinados a bloquear ataques de phishing e evitar a instalação e a operação de variantes de malware MitB.

Esta oferta IBM SaaS possui uma métrica de encargo de Participante Elegível. A oferta de Negócios é vendida em pacotes de 10 Participantes Elegíveis. A oferta de Varejo é vendida em pacotes de 100 Participantes Elegíveis.

Este oferta IBM SaaS inclui:

a. Trusteer Management Application ("TMA"):

   O TMA é disponibilizado no ambiente hospedado em nuvem do IBM Security Trusteer, através do qual o Cliente (e um número ilimitado de membros de sua equipe autorizada) pode: (i) receber relatórios de dados de eventos e avaliações de risco, (ii) visualizar, configurar e definir políticas relacionadas ao relatório de dados de eventos e (iii) visualizar a configuração do software de habilitação do cliente licenciado para o público sob um contrato de licença do usuário final ("EULA"), sem encargos e disponibilizado para download em desktops ou dispositivos do Participante Elegível (PC/MACs), também conhecido como suíte de software Trusteer Rapport ("Software Cliente do Titular da Conta"). O Cliente pode comercializar o Software Cliente do Titular da Conta apenas usando o Trusteer Splash ou Rapport API e o Cliente não pode usar o Software Cliente do Titular da Conta para suas operações internas de negócios ou para uso de seus funcionários (exceto para uso pessoal dos funcionários).

b. Script da Web:

   Para acesso em um website para os propósitos de acesso ou uso das ofertas IBM SaaS.

c. Dados de eventos:

   O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados a partir de Software Cliente do Titular da Conta como resultado das interações online dos Titulares da Conta com seu Aplicativo de Negócios ou Varejo para o qual o Cliente assinou para obter a cobertura das ofertas IBM SaaS. Dados de eventos serão recebidos a partir do Software Cliente do Titular da Conta dos Participantes Elegíveis que está em execução em seus dispositivos, que aceitaram o EULA, se autenticaram com o Aplicativo de Negócios ou Varejo do Cliente pelo menos uma vez, e a configuração do Cliente deve incluir a coleta de IDs do usuário.

d. Trusteer Splash:

   A plataforma de marketing Trusteer Splash identifica e comercializa o Software Cliente Titular da Conta para os Participantes Elegíveis que acessam Aplicativos de Negócios e/ou Varejo do Cliente para os quais o Cliente assinou para obter a cobertura das ofertas do IBM SaaS. O Cliente pode selecionar entre Modelos Splash disponíveis. Splashs customizados podem ser contratados sob um contrato ou descrição do trabalho separado.

O Cliente pode concordar em fornecer suas marcas comerciais, logotipos ou ícones para uso em conexão com o TMA e apenas para utilização com o Trusteer Splash e para exibição no Software Cliente do Titular da Conta ou nas páginas de entrada hospedadas pela IBM e no website do IBM Security Trusteer. Qualquer uso de suas marcas comerciais, logotipos ou ícones fornecidos estará de acordo com as políticas razoáveis da IBM com relação à publicidade e ao uso da marca comercial.

O Cliente deve assinar a oferta SaaS IBM Security Trusteer Rapport Mandatory Service se desejar empregar qualquer tipo de implementação obrigatória no Software Cliente do Titular da Conta.

A implementação obrigatória do Software Cliente do Titular da Conta inclui, mas não está limitada a qualquer tipo de implementação obrigatória por qualquer mecanismo ou meio que obrigue, direta ou indiretamente, um Participante Elegível a fazer download do Software Cliente do Titular da Conta, ou qualquer outro método, ferramenta, procedimento, acordo ou mecanismo, não criado por ou aprovado pela IBM, criado para efetuar bypass dos requisitos de licenciamento desta implementação obrigatória do Software Cliente do Titular da Conta.

2.2 Ofertas IBM SaaS Adicionais Opcionais para o IBM Security Trusteer Rapport for Business e/ou IBM Security Trusteer Rapport for Retail

A subscrição de ofertas IBM Security Trusteer Rapport é um pré-requisito para a subscrição de qualquer uma das ofertas IBM SaaS adicionais a seguir. Se o IBM SaaS for designado como "for Business", então, a oferta IBM SaaS adicional adquirida também deve ser designada como "for Business". Se o IBM SaaS for designado como "for Retail", então, a oferta IBM SaaS adicional adquirida também deve ser designada como "for Retail". O Cliente receberá dados de eventos dos Participantes Elegíveis executando o Software Cliente do Titular da Conta que aceitaram o EULA, se autenticaram com o(s) Aplicativo(s) de Negócios e/ou Varejo do Cliente pelo menos uma vez, e a configuração do Cliente deve incluir a coleta de IDs do usuário.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business e/ou IBM Security Trusteer Rapport Fraud Feeds for Retail

O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos relacionados a infecções de malware e outras vulnerabilidades de terminal em um desktop particular do Titular da Conta.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business e/ou IBM Security Trusteer Rapport Phishing Protection for Retail

O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber notificações de dados de eventos relacionados ao envio das credenciais de login do Titular da Conta para um site de phishing suspeito ou potencialmente fraudulento. Aplicativos online legítimos (URLs) podem ser erroneamente sinalizados como sites de phishing e o IBM SaaS pode alertar os Titulares de Conta que um site legítimo é um site de phishing. Nesse caso, o Cliente deverá notificar a IBM sobre tal erro, e a IBM deve corrigir o erro. Esta deverá ser a reparação exclusiva do Cliente para tal erro.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business e/ou IBM Security Trusteer Rapport Mandatory Service for Retail

O Cliente pode usar uma instância da plataforma de marketing Trusteer Splash para impor o download do Software Cliente do Titular da Conta aos Participantes Elegíveis acessando Aplicativos de Negócios e/ou Varejo do Cliente para o qual o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS.

O IBM Security Trusteer Rapport Premium Support for Business é um pré-requisito para o IBM Security Rapport Mandatory Service for Business.

O IBM Security Trusteer Rapport Premium Support for Retail é um pré-requisito para o IBM Security Rapport Mandatory Service for Retail.

O Cliente pode implementar a funcionalidade adicional do IBM Security Trusteer Rapport Mandatory Service somente se ela foi solicitada e configurada para uso com o Aplicativo de Varejo ou Negócios do Cliente para o qual o Cliente assinou para obter a cobertura das ofertas IBM SaaS.

3. Ofertas IBM Security Trusteer Pinpoint

O IBM Security Trusteer Pinpoint é um serviço baseado em nuvem que é projetado para fornecer outra camada de proteção e é destinado a detectar e mitigar ataques de malware, phishing e controle de conta. O Trusteer Pinpoint pode ser integrado nos Aplicativos de Negócios e/ou Varejo do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS e processos de prevenção de fraudes.

Este oferta IBM SaaS inclui:

a. TMA:

   O TMA é disponibilizado no ambiente hospedado em nuvem do IBM Security Trusteer, através do qual o Cliente (e um número ilimitado de membros de sua equipe autorizada) pode: (i) receber relatórios de dados de eventos e avaliações de risco e (ii) visualizar, configurar e definir políticas de segurança relacionadas ao relatório de dados de eventos.

b. Script da Web e/ou APIs:

   Para implementação em um website para os propósitos de acesso ou uso do IBM SaaS.

3.1 IBM Security Trusteer Pinpoint Malware Detection e IBM Security Trusteer Pinpoint Criminal Detection

No caso de detecção de malware em ofertas IBM Security Trusteer Pinpoint Malware ou detecção de controle de conta em ofertas IBM Security Trusteer Pinpoint Criminal Detection, o Cliente deve seguir o Guia de Melhores Práticas do Pinpoint. O Cliente não deve usar ofertas IBM Security Trusteer Pinpoint Malware Detection ou ofertas IBM Security Trusteer Pinpoint Criminal Detection de qualquer maneira que irá afetar a experiência do Participante Elegível imediatamente após uma detecção de malware ou controle de conta, de tal forma que ela permitiria que outros vinculassem as ações do Cliente com o uso de ofertas IBM Security Trusteer Pinpoint (por exemplo, notificações, mensagens, bloqueio de dispositivos ou bloqueio do acesso ao Aplicativo de Negócios e/ou Varejo imediatamente após uma detecção de malware ou controle de conta).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business e/ou IBM Security Trusteer Pinpoint Criminal Detection for Retail

Detecção independente de Cliente de uma atividade de controle de conta suspeita de navegadores se conectando a um Aplicativo de Negócios ou Varejo, usando o ID do dispositivo, detecção de phishing e detecção de roubo de credenciais orientada por malware. As ofertas IBM Security Trusteer Pinpoint Criminal Detection fornecem outra camada de proteção e têm como objetivo detectar tentativas de controle de conta e entregar pontuações de avaliação de risco de navegadores ou dispositivos móveis (através do navegador nativo ou do aplicativo móvel do Cliente) acessando um Aplicativo de Negócios ou Varejo diretamente para o Cliente.

a. Dados de eventos:

   O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados como um resultado das interações online dos Participantes Elegíveis com o(s) Aplicativo(s) de Negócios e/ou Varejo do Cliente para o(s) qual(quais) o Cliente assinou para obter a cobertura das ofertas IBM SaaS ou o Cliente pode receber os dados dos eventos através de um modo de entrega de API de backend.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile e/ou IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

As ofertas IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) são projetadas para fornecer outra camada de proteção e têm como objetivo proteger contra atividades fraudulentas e de controle de conta ao identificar acesso criminoso à conta e ao fornecer uma recomendação para o Cliente. Esta oferta IBM SaaS coleta informações provenientes do Aplicativo de Negócios e/ou Varejo do Cliente usando a API PPCD Mobile e dos dispositivos móveis dos Participantes Elegíveis. As ofertas IBM Security Trusteer PPCD Mobile são projetadas para correlacionar informações complexas correlacionadas com dispositivos móveis de Participantes Elegíveis com outras origens de dados, tais como infecção por malware em tempo real e incidentes de phishing que são integrados através de outras ofertas IBM SaaS do IBM Security Trusteer especificadas nestes ToU.

O Cliente pode acessar e usar as ofertas IBM Security Trusteer PPCD Mobile no ambiente hospedado na nuvem do IBM Security Trusteer e receber dados de avaliações de risco de dispositivos móveis de Participantes Elegíveis, gerados como resultado das interações online destes dispositivos móveis com o Aplicativo de Negócios ou Varejo para o qual Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS. Para o propósito destas ofertas, "dispositivos móveis" incluem apenas telefones celulares e tablets suportados e não incluem PCs ou MACs.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Detecção independente de Cliente nos navegadores infectados por malware financeiro Man in the Browser (MitB) se conectado a um Aplicativo de Negócios e/ou Varejo. As ofertas IBM Security Trusteer Pinpoint Malware Detection fornecem outra camada de proteção e têm como objetivo permitir que as organizações foquem em processos de prevenção da fraude com base no risco do malware ao fornecer ao Cliente avaliações e alertas de uma presença de malware financeiro MITB.

a. Dados de eventos:

   O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados como um resultado das interações online dos Participantes Elegíveis com o(s) Aplicativo(s) de Negócios e/ou Varejo do Cliente.

b. Advanced Edition:

   As ofertas Advanced Editions para Negócios e/ou Varejo oferecem uma camada adicional de detecção e proteção que é ajustada e customizada para a estrutura e o fluxo dos Aplicativos de Negócios e/ou Varejo do Cliente, e pode ser customizada para cenário de ameaça específico visando o Cliente. Ela pode ser incorporada em diversos locais nos Aplicativos de Negócios e/ou Varejo do Cliente.

   A Advanced Edition é oferecida ao Cliente em quantidades mínimas de pelo menos 100 mil Participantes Elegíveis de Varejo ou 10 mil Participantes Elegíveis de Negócios, que são 1000

pacotes de 100 Participantes Elegíveis para Varejo ou 1000 pacotes de 10 Participantes Elegíveis para Negócios.

c. Standard Edition:

A Standard Edition for Business ou for Retail é uma solução de rápida implementação que fornece a funcionalidade principal desta oferta IBM SaaS, conforme descrito aqui.

3.2 Ofertas IBM SaaS Adicionais Opcionais para o IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition e/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Para as ofertas IBM Security Trusteer Rapport Remediation for Retail, há um pré-requisito do IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

Para o IBM Security Trusteer Pinpoint Carbon Copy for Retail, há um pré-requisito do IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Para o IBM Security Trusteer Pinpoint Carbon Copy for Business, há um pré-requisito do IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business e/ou IBM Security Trusteer Pinpoint Carbon Copy for Retail

As ofertas IBM Security Trusteer Pinpoint Carbon Copy são projetadas para fornecer outra camada de proteção e um serviço de monitoramento que podem ajudar a identificar quando as credenciais de um Participante Elegível foram comprometidas por ataques de Phishing em Aplicativos de Varejo ou Negócios do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

O IBM Security Trusteer Rapport Remediation for Retail tem como objetivo investigar, corrigir, bloquear e remover infecções de malware man-in-the-browser (MitB) de dispositivos infectados (PC/MACs) dos Participantes Elegíveis do Cliente que acessam o Aplicativo de Varejo do Cliente em uma base ad-hoc, onde as infecções de malware MitB foram detectadas por dados de eventos do IBM Security Trusteer Pinpoint Malware Detection. O Cliente deve ter uma subscrição atual para o IBM Security Trusteer Pinpoint Malware Detection realmente em execução no Aplicativo de Varejo do Cliente. O Cliente pode usar esta oferta IBM SaaS apenas em conexão com os Participantes Elegíveis que acessam o Aplicativo de Varejo do Cliente e exclusivamente como uma ferramenta que tem como objetivo investigar e corrigir um dispositivo particular infectado (PC/MAC) em uma base ad-hoc. O IBM Security Trusteer Rapport Remediation for Retail deve estar em real execução em um dispositivo do Participante Elegível afetado (PC/MAC) e tal Participante Elegível afetado tem que aceitar o EULA, autenticar com Aplicativo(s) de Varejo do Cliente, pelo menos uma vez, e a configuração do Cliente deve incluir a coleta de IDs de Usuário. Para evitar dúvidas, esta oferta IBM SaaS não inclui o direito de usar o Trusteer Splash e/ou promover o Software Cliente do Titular da Conta de qualquer outra forma na população de Participantes Elegíveis gerais do Cliente.

4. Ofertas IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business e/ou IBM Security Trusteer Mobile Browser for Retail

O IBM Security Trusteer Mobile Browser é projetado para incluir outra camada de proteção e tem como objetivo fornecer acesso online seguro dos dispositivos móveis dos Participantes Elegíveis que acessam Aplicativos de Varejo ou Negócios do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS, avaliação de risco de dispositivos móveis e proteção contra phishing. A detecção de Wi-Fi seguro está disponível apenas para plataformas Android. Para os propósitos desta oferta IBM SaaS, incluem dispositivos móveis, incluem telefones celulares ou tablets, e não incluem laptops PCs e Macs.

Através do TMA, o Cliente (e um número ilimitado de membros de sua equipe autorizada) pode receber dados de eventos, análise e informações de estatísticas relativas aos Dispositivos cujos Participantes Elegíveis: (i) transferiram por download o Software Cliente do Titular da Conta, um aplicativo licenciado

ao público sob um contrato de licença do usuário final ("EULA") sem encargos e disponibilizado para download nos dispositivos móveis dos Participantes Elegíveis e (ii) aceitaram o EULA e autenticaram pelo menos uma vez com os Aplicativos de Negócios ou varejo do Cliente para os quais o Cliente assinou para obter as coberturas das ofertas IBM. O Cliente só poderá comercializar o Software Cliente do Titular da Conta usando o Trusteer Splash e não poderá usar o Software Cliente do Titular da Conta para suas operações de negócios internas.

a. Dados de eventos:

   O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados como resultado das interações online dos dispositivos móveis com Aplicativos de Varejo ou Negócios do Cliente para os quais o Cliente assinou para obter a cobertura das ofertas IBM SaaS.

b. Trusteer Splash:

   A plataforma de marketing Trusteer Splash identifica e comercializa o Software Cliente Titular da Conta para os Participantes Elegíveis que acessam Aplicativos de Negócios e/ou de Varejo do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas do IBM SaaS. O Cliente pode selecionar entre modelos de splash disponíveis ("Modelo Splash"). Splashs customizados podem ser contratados sob um contrato ou descrição do trabalho separado.

O Cliente pode concordar em fornecer suas marcas comerciais, logotipos ou ícones para uso em conexão com o TMA e apenas para utilização com o Trusteer Splash e para exibição no Software Cliente do Titular da Conta ou nas páginas de entrada hospedadas pela IBM ou no website do IBM Security Trusteer. Qualquer uso de suas marcas comerciais, logotipos ou ícones fornecidos estará de acordo com políticas razoáveis da IBM com relação à publicidade e ao uso da marca comercial.

4.2 IBM Security Trusteer Mobile SDK for Business e/ou IBM Security Trusteer Mobile SDK for Retail

As ofertas IBM Security Trusteer Mobile SDK são projetadas para incluir outra camada de proteção para fornecer acesso à web seguro em Aplicativos de Negócios e/ou Varejo do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS, avaliação de risco dos dispositivos e proteção contra pharming. A detecção de Wi-Fi segura está disponível apenas para plataformas Android.

As ofertas IBM Security Trusteer Mobile SDK incluem um kit do desenvolvedor de software ("SDK") móvel proprietário, um pacote de software contendo documentação, bibliotecas de software proprietárias de programação e outros arquivos e itens relacionados, conhecidos como biblioteca móvel do IBM Security Trusteer, bem como o "Componente de Tempo de Execução" ou "Redistribuível", um código proprietário gerado pelo IBM Security Trusteer Mobile SDK que pode ser incorporado e integrado em aplicativos móveis iOS ou Android independentes protegidos do Cliente para os quais o Cliente tenha subscrito para obter a cobertura das ofertas IBM SaaS ("App Móvel Integrado do Cliente").

O IBM Security Trusteer Mobile SDK for Retail está disponível em pacotes de 100 Participantes Elegíveis ou pacotes de 100 Dispositivos do Cliente, e o IBM Security Trusteer Mobile SDK for Business está disponível em pacotes de 10 Participantes Elegíveis ou pacotes de 10 Dispositivos do Cliente.

Através do TMA, o Cliente (e número ilimitado de membros da sua equipe autorizada) pode receber relatórios de dados do evento e avaliações de tendências de risco. Através do App Móvel Integrado do Cliente, o Cliente pode receber informações sobre análise de risco e dispositivos móveis com relação aos dispositivos móveis dos Participantes Elegíveis que fizeram download do App Móvel Integrado do Cliente, permitindo que o Cliente formule uma política de prevenção de fraude ao tornar mandatórias ações de mitigação em relação a estes riscos. Para o propósito desta oferta, "dispositivos móveis" incluem apenas telefones celulares e tablets suportados e não incluem PCs ou MACs.

O Cliente pode:

a. usar internamente o IBM Security Trusteer Mobile SDK com o propósito exclusivo de desenvolver o App Móvel Integrado do Cliente;

b. integrar o Redistribuível (somente no formato de código objeto) de modo integral não separável no App Móvel Integrado do Cliente. Qualquer parte modificada ou integrada do Redistribuível conforme esta concessão de licença estará sujeita aos termos destes ToU; e

c. comercializar e distribuir o Redistribuível para download para dispositivos móveis dos Participantes Elegíveis ou no portador do Dispositivo do Cliente, desde que:

- Exceto conforme expressamente permitido neste Acordo, o Cliente (1) não pode usar, copiar, modificar ou distribuir o SDK; (2) não pode reverter a montagem, reverter a compilação ou de qualquer outra forma, converter ou reverter a engenharia do SDK, exceto conforme expressamente permitido por lei, sem a possibilidade de renúncia contratual; (3) não pode sublicenciar, alugar ou arrendar o SDK; (4) não pode remover quaisquer arquivos de copyright ou aviso contidos no Redistribuível; (5) não pode usar o mesmo nome de caminho que os arquivos/módulos do Redistribuível originais; e (6) não pode usar nomes ou marcas comerciais da IBM, de seus licenciadores ou distribuidores em conexão com a comercialização do App Móvel Integrado do Cliente sem o consentimento prévio e por escrito da IBM, do licenciador ou do distribuidor.
- O Redistribuível deve permanecer integrado de uma forma não separável dentro do App Móvel Integrado do Cliente. O Redistribuível deve estar apenas no formato de código de objeto e deve estar em conformidade com todas as orientações, instruções e especificações no SDK e na sua documentação. O contrato de licença do usuário final para o App Móvel Integrado do Cliente deve notificar o usuário final que o Redistribuível pode não ser i) usado para qualquer outro propósito além de ativar o App Móvel Integrado do Cliente, ii) copiado (exceto para propósitos de backup), iii) adicionalmente distribuído ou transferido, iv) ter sua montagem revertida, compilação revertida ou de qualquer outra forma, convertido, exceto conforme especificamente permitido por lei e sem a possibilidade de uma renúncia contratual. O contrato de licença do cliente deve ser pelo menos tão protetor da IBM quanto os termos deste Acordo
- O SDK pode ser implantado apenas como parte do desenvolvimento e testes de unidade internos do Cliente em dispositivos de teste móveis especificados do Cliente. O Cliente não está autorizado a usar o SDK para o processamento de cargas de trabalho de produção, simulação de cargas de trabalho de produção ou escalabilidade de testes de qualquer código, aplicativo ou sistema. O Cliente não está autorizado a usar qualquer parte do SDK para quaisquer outros propósitos.

O Cliente é responsável por toda a assistência técnica para o App Móvel Integrado do Cliente e por quaisquer modificações nos Redistribuíveis feitas pelo Cliente, conforme permitido neste documento.

O Cliente está autorizado a instalar e usar os Redistribuíveis e o IBM Security Mobile SDK apenas para suportar o uso da oferta IBM SaaS pelo Cliente.

A IBM testou aplicativos de amostra criados com as ferramentas móveis fornecidas no IBM Security Trusteer Mobile SDK ("Ferramentas Móveis") para determinar se eles serão executados corretamente em algumas versões das plataformas de sistemas operacionais móveis da Apple (iOS), Google (Android) e outras (coletivamente "Plataformas de SO Móveis"), no entanto, as Plataformas de SO Móveis são fornecidas por terceiros, não estão sob controle da IBM e estão sujeitas a alteração sem aviso para a IBM. Desta forma, e não obstante qualquer disposição em contrário, a IBM não garante que quaisquer aplicativos ou outros resultados criados usando as Ferramentas Móveis serão executadas apropriadamente em, interoperarão com ou serão compatíveis com quaisquer Plataformas de SO Móveis ou dispositivos móveis.

O Cliente concorda em criar, manter e fornecer à IBM e seus auditores registros precisos por escrito, saídas de ferramenta do sistema e outras informações do sistema suficientes para fornecer uma verificação auditável de que o uso do Cliente do IBM Security Trusteer Mobile SDK está em conformidade com os termos destes ToU.

5. Implementação das Ofertas de Proteção de Fraudes IBM SaaS

A subscrição base do Cliente inclui atividades de configuração obrigatória e implementação inicial, incluindo inicialização única, configuração, Modelo Splash, testes e treinamento.

Os serviços adicionais podem ser contratados por um encargo adicional sob um contrato separado.

Apêndice B

A IBM fornece o acordo de nível de serviço ("SLA") de disponibilidade a seguir para o IBM SaaS e é aplicável se especificado no Documento de Transação do Cliente:

A versão desse SLA que é atual no início ou renovação do termo de subscrição do Cliente se aplicará. O Cliente entende que o SLA não constitui uma garantia ao Cliente.

1. Definições

a. **Contato autorizado** – significa o indivíduo especificado pelo Cliente para a IBM com autorização para submeter Reivindicações sob este SLA.

b. **Crédito de Disponibilidade** – significa a solução que a IBM fornecerá para uma Reivindicação validada. O Crédito de Disponibilidade será aplicado na forma de um crédito ou desconto com relação a uma fatura futura de encargos de subscrição do IBM SaaS.

c. **Reivindicação** – significa uma reivindicação submetida pelo Contato autorizado do Cliente à IBM, conforme este SLA, de que um Nível de serviço não foi cumprido durante o Mês Contratado.

d. **Mês Contratado** – significa cada mês integral durante o termo do IBM SaaS medido de 12h00 (GMT) no primeiro dia do mês até 23h59 (GMT) no último dia do mês.

e. **Cliente** – significa uma entidade que está assinando o IBM SaaS diretamente da IBM e que não está em inadimplente em relação a quaisquer obrigações materiais, incluindo obrigações de pagamento, sob seu contrato com a IBM para o IBM SaaS.

f. **Tempo de Inatividade** – significa um período de tempo durante o qual o processamento do sistema de produção para o Serviço é interrompido e todos os usuários ficam incapazes de usar todos os aspectos do Serviço para o qual possuem as permissões apropriadas. O Tempo de Inatividade não inclui o período de tempo no qual o Serviço não fica disponível como resultado de:

- Tempo de Inatividade do Sistema Planejado;
- Força Maior;
- Problemas com aplicativos, equipamento ou dados do Cliente ou de terceiros;
- Atos ou omissões do Cliente ou de terceiros (incluindo qualquer pessoa obtendo acesso ao IBM SaaS por meio de senhas ou equipamentos do Cliente);
- Falha ao aderir às configurações do sistema necessárias e plataformas suportadas para o acesso ao IBM SaaS; ou
- A conformidade da IBM com qualquer design, especificação ou instrução fornecida pelo Cliente ou um terceiro em nome do Cliente.

g. **Evento** – significa uma circunstância ou um conjunto de circunstâncias reunidas, que resultam em uma falha ao atender um Nível de Serviço.

h. **Força Maior** – significa caso fortuito, força maior , terrorismo, questões trabalhistas, incêndio, enchente, terremoto, motim, guerra, atos governamentais, ordens ou restrições, vírus, ataques de recusa de serviço e outras condutas maliciosas, falhas de conectividade de rede e utilitário ou qualquer outra causa de indisponibilidade do IBM SaaS que esteja fora do controle plausível da IBM.

i. **Tempo de Inatividade Planejado do Sistema** – significa uma indisponibilidade planejada do IBM SaaS com o propósito de fazer manutenção.

j. **Nível de Serviço** – significa o padrão apresentado abaixo pelo qual a IBM mede o nível de serviço que fornece neste LA.

2. Créditos de Disponibilidade

a. Para ser elegível para submeter uma Reivindicação, o Cliente deve ter registrado um chamado de suporte para cada Evento com o help desk de suporte do cliente IBM para o IBM SaaS aplicável, em conformidade com o procedimento IBM para relatar problemas de suporte de Gravidade 1. O Cliente deve fornecer todas as informações detalhadas necessárias sobre o Evento e razoavelmente ajudar a IBM com o diagnóstico e a resolução do Evento na medida do necessário

para chamados de suporte de Gravidade 1. Tal chamado deve ser registrado no prazo de vinte e quatro (24) horas do Cliente primeiro tomar ciência de que o Evento impactou uso do IBM SaaS pelo Cliente.

b. O Contato Autorizado do Cliente deve submeter uma Reivindicação do Cliente por um Crédito de Disponibilidade não mais do que três (3) dias úteis após o término do Mês contratado que é o assunto da Reivindicação.

c. O Contato autorizado do Cliente deve fornecer à IBM todos os detalhes razoáveis com relação à Reivindicação, incluindo, mas sem se limitar a, descrições detalhadas de todos os Eventos relevantes e o Nível de serviço reclamado como não cumprido.

d. A IBM medirá internamente o Tempo de Inatividade combinado total durante cada Mês Contratado aplicável ao Nível de Serviço correspondente mostrado na tabela abaixo. Os Créditos de Disponibilidade serão baseados na duração do Tempo de Inatividade medido a partir do momento que o Cliente relata que foi primeiro impactado pelo Tempo de Inatividade. Se o Cliente relatar um Evento de Tempo de Inatividade do Aplicativo e um Evento de Tempo de Inatividade de Processamento de Dados de Entrada ocorrendo simultaneamente, a IBM tratará os períodos de sobreposição de Tempo de Inatividade como um único período de Tempo de Inatividade, e não como dois períodos separados. Para cada Reivindicação válida, a IBM aplicará o Crédito de Disponibilidade aplicável mais alto com base no Nível de Serviço atingido durante cada Mês Contratado, como mostrado nas tabelas abaixo. A IBM não será responsabilizada por diversos Créditos de Disponibilidade para o(s) mesmo(s) Evento(s) no mesmo Mês Contratado.

e. Para Serviço em Pacote Configurável (IBM SaaS individuais empacotados e vendidos juntos por um único preço combinado), o Crédito de Disponibilidade será calculado com base no preço mensal único combinado para o Serviço em Pacote Configurável, e não no encargo de subscrição mensal para cada IBM SaaS individual. O Cliente pode submeter somente Reivindicações relacionadas a um IBM SaaS individual em um pacote configurável em qualquer Mês Contratado e a IBM não será responsável pelos Créditos de Disponibilidade com respeito a mais de um IBM SaaS em um pacote configurável em qualquer Mês contratado.

f. Se o Cliente comprou o IBM SaaS de um revendedor IBM válido em uma transação de recomercialização em que a IBM mantém a responsabilidade primária para cumprir os compromissos do IBM SaaS e do SLA, então, o Crédito de Disponibilidade será baseado no Relationship Suggested Value Price (RSVP) então atual para o IBM SaaS em vigor para o Mês Contratado que é assunto de uma Reivindicação, descontado a uma taxa de 50%.

g. O total em Créditos de disponibilidade premiados com respeito a qualquer Mês contratado não deve, sob nenhuma circunstância, exceder dez por cento (10%) de um duodécimo (1/12º) dos encargos anuais pagos pelo Cliente à IBM para o IBM SaaS.

h. A IBM fará uso de seu julgamento razoável para validar as Reivindicações com base nas informações disponíveis nos registros da IBM, que prevalecerão no caso de um conflito com os dados nos registros do Cliente.

i. OS CRÉDITOS DE DISPONIBILIDADE FORNECIDOS AO CLIENTE DE ACORDO COM ESTE SLA SÃO A REPARAÇÃO ÚNICA E EXCLUSIVA DO CLIENTE COM RELAÇÃO A QUALQUER REIVINDICAÇÃO.

3. Níveis de Serviço

Disponibilidade do IBM SaaS durante o Mês Contratado

Nível de Serviço Realizado (durante um Mês Contratado)	**Crédito de Disponibilidade (% do Encargo de Subscrição Mensal para o Mês Contratado que é objeto de uma Reivindicação)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

O "Nível de Serviço Realizado", expresso como uma porcentagem é calculado como: (a) o número total de minutos em um Mês Contratado, menos (b) o número total de minutos de Tempo de Inatividade em um Mês Contratado, dividido por (c) o número total de minutos em um Mês Contratado.

Exemplo: 250 minutes de Tempo de Inatividade total durante o Mês Contratado

Total de 43.200 minutos em um Mês Contratado de 30 dias - 250 minutos de Tempo de Inatividade = 42.950 minutos _____ 43.200 minutos totais	= 2% de Crédito de Disponibilidade para 99,4% de Nível de Serviço Realizado durante o Mês Contratado

3.1 Exclusões

Este acordo de nível de serviço é disponibilizado apenas aos Clientes da IBM. Este SLA não se aplica ao seguinte:

- Serviços Beta e de teste.
- Ambientes de não produção, incluindo, mas não a eles limitados, teste, recuperação de desastre, controle de qualidade ou desenvolvimento.
- Reivindicações feitas pelos usuários, guests, participantes e convidados permitidos do Cliente do IBM SaaS.
- Se o Cliente violou qualquer obrigação material sob esses ToU, incluindo, sem limitação, violação de quaisquer obrigações de pagamento.