IBM Security Trusteer Fraud Protection

Os Termos de Utilização ("ToU") são constituídos pelos presentes Termos de Utilização IBM – Termos de Oferta Específica do SaaS ("Termos de Oferta Específica do SaaS") e um documento intitulado Termos de Utilização IBM – Termos Gerais ("Termos Gerais"), que se encontra disponível no seguinte URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Em caso de conflito, os Termos de Oferta Específica do SaaS prevalecem sobre os Termos Gerais. Ao encomendar, aceder ou utilizar o IBM SaaS, o Cliente está a aceitar os presentes ToU.

Os ToU são regidos pelo Acordo IBM International Passport Advantage, o Acordo IBM International Passport Advantage Express ou o Acordo Internacional IBM para Ofertas Seleccionadas do IBM SaaS, conforme aplicável ("Acordo") e, em conjunto com os ToU, constituem o acordo integral.

1. IBM SaaS

As seguintes ofertas do IBM SaaS são abrangidas pelos presentes Termos da Oferta Específica do SaaS:

1.1 Ofertas Rapport do IBM SaaS

- 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 Pinpoint do IBM SaaS

- 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 Mobile do IBM SaaS

- 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 nos termos de uma das seguintes métricas de encargos, conforme especificado no Documento de Transacção:

a. **Participante Elegível** – corresponde a uma unidade de medida segundo a qual o IBM SaaS pode ser obtido. Cada indivíduo ou entidade elegível para participar em qualquer programa de prestação de serviços gerido ou controlado pelo IBM SaaS é um Participante Elegível. Têm de ser obtidas titularidades em número suficiente para cobrir todos os Participantes Elegíveis geridos ou controlados no IBM SaaS durante o período de medição especificado no Documento de Transacção do Cliente.

   Cada programa de prestação de serviços gerido pelo IBM SaaS é analisado separadamente e, em seguida, adicionado em conjunto. As pessoas singulares ou entidades elegíveis para vários programas de prestação de serviços requerem titularidades separadas.

   Para estas ofertas, um programa de prestação de serviços inclui uma única Aplicação Empresarial ou de Retalho do Cliente com uma página de início de sessão principal e páginas relacionadas para cada Aplicação Empresarial ou de Retalho. Um Participante Elegível consiste num utilizador final de um Cliente, que dispõe de credenciais de início de sessão na Aplicação Empresarial ou de Retalho.

b. **Dispositivo Cliente** – corresponde a uma unidade de medida segundo a qual o IBM SaaS pode ser obtido. Um Dispositivo Cliente consiste num dispositivo informático de utilizador único, sensor de finalidade especial ou dispositivo de telemetria que solicita a execução de, ou recebe para execução, um conjunto de comandos, procedimentos ou aplicações ou fornece dados a outro sistema informático que é geralmente designado por servidor ou, de outra forma, gerido pelo servidor. Vários Dispositivos Clientes podem partilhar o acesso a um servidor comum. Um Dispositivo Cliente poderá ter alguma capacidade de processamento ou poderá ser programável para permitir que um utilizador utilize o mesmo. O Cliente tem de obter titularidades para cada Dispositivo Cliente que executa, fornece dados a, utiliza serviços fornecidos por ou, de outra forma, acede ao IBM SaaS durante o período de medição especificado no Documento de Transacção do Cliente.

3. Encargos e Facturação

O montante a pagar pelo IBM SaaS é especificado num Documento de Transacção.

3.1 Encargos Mensais Parciais

Poderá ser avaliado um encargo mensal parcial, conforme especificado no Documento de Transacção, numa base proporcional ("rateado").

4. Conformidade e Auditoria

O acesso às ofertas IBM Security Trusteer Fraud Protection está sujeito a uma quantidade máxima de Participantes Elegíveis ou Dispositivos Clientes, conforme especificado no Documento de Transacção. O Cliente é responsável por assegurar que o respectivo número de Participantes Elegíveis ou Dispositivos Clientes não excede a quantidade máxima especificada no Documento de Transacção.

Pode ser realizada uma auditoria para verificar a conformidade com a quantidade máxima de Participantes Elegíveis ou Dispositivos Clientes.

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

O Documento de Transacção do Cliente especifica se o IBM SaaS será renovado no final do Período de Subscrição, designando uma das seguintes opções:

5.1 Renovação Automática

Caso o Documento de Transacção do Cliente especifique que a renovação do Cliente é automática, o Cliente pode denunciar o Período de Subscrição do IBM SaaS prestes a expirar, mediante pedido por escrito ao representante de vendas IBM ou Parceiro de Negócios IBM do Cliente com, pelo menos, noventa (90) dias de antecedência relativamente à data especificada no Documento de Transacção. Caso a IBM ou o seu Parceiro de Negócios IBM não receba o aviso de denúncia até à data de expiração, o Período de Subscrição prestes a expirar será automaticamente renovado por um período de um ano ou pela mesma duração do Período de Subscrição original, conforme especificado no Documento de Transacção.

5.2 Facturação Contínua

Se o Documento de Transacção indicar que a renovação do Cliente é contínua, o Cliente continuará a ter acesso ao IBM SaaS e ser-lhe-á cobrada a utilização do IBM SaaS numa base contínua. Para descontinuar a utilização do IBM SaaS e interromper o processo de facturação contínua, o Cliente terá de enviar uma notificação por escrito à IBM ou ao seu Parceiro de Negócios IBM, com antecedência de noventa (90) dias, a solicitar o cancelamento do respectivo IBM SaaS. Após o cancelamento do acesso do Cliente, serão cobrados ao Cliente quaisquer encargos de acesso pendentes durante o mês em que o cancelamento entrou em vigor.

5.3 Renovação Requisitada

Se o Documento de Transacção indicar que o tipo de renovação do Cliente é "resolução", o IBM SaaS será resolvido no final do Período de Subscrição e o acesso do Cliente ao IBM SaaS será removido. Para continuar a utilizar o IBM SaaS para lá da data de fim, o Cliente terá de efectuar um pedido junto do representante de vendas IBM ou do Parceiro de Negócios IBM do Cliente para adquirir um novo Período de Subscrição.

6. Suporte Técnico

Está disponível Suporte Técnico para o IBM SaaS, para assistência a um Cliente e respectivos Participantes Elegíveis na sua utilização do IBM SaaS.

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

Para cada oferta do IBM SaaS, está disponível uma subscrição de Suporte Premium por um encargo adicional, à excepção das ofertas IBM Security Trusteer Mobile SDK e ofertas IBM Security Trusteer Rapport Mandatory Service.

Suporte Padrão:

- Suporte das 8h00 às 17h00, no fuso horário local.
- Os Clientes e os respectivos Participantes Elegíveis podem submeter tickets de suporte electronicamente, conforme detalhado no Guia de Suporte de Software como um Serviço [SaaS].
- Os Clientes podem aceder ao Portal de Suporte ao Cliente para obter notificações, documentos, relatórios de casos e Perguntas Frequentes em: http://www-01.ibm.com/software/security/trusteer/support/.
- Para obter as opções de suporte e detalhes, aceda ao Guia de Suporte de Software como um Serviço [SaaS] da IBM: http://www-01.ibm.com/software/support/handbook.html.

Suporte Premium:

- Suporte 24 horas por dia, 7 dias por semana para todos os níveis de gravidade.
- Os Clientes podem contactar o suporte directamente por telefone.
- Os Clientes e os respectivos Participantes Elegíveis podem submeter tickets de suporte electronicamente, conforme detalhado no Guia de Suporte de Software como um Serviço [SaaS].
- Os Clientes podem aceder ao Portal de Suporte ao Cliente para obter notificações, documentos, relatórios de casos e Perguntas Frequentes em: http://www-01.ibm.com/software/security/trusteer/support/.
- Para obter as opções de suporte e detalhes, aceda ao Guia de Suporte de Software como um Serviço [SaaS] da IBM: http://www-01.ibm.com/software/support/handbook.html.

7. Termos Adicionais da Oferta do IBM SaaS

7.1 Conformidade com o Acordo Safe Harbor

A IBM cumpre o acordo U.S. – EU Safe Harbor Framework desenvolvido pelo Departamento de Comércio dos Estados Unidos em coordenação com a Comissão Europeia. Os produtos IBM Security Trusteer estão incluídos na certificação EU-U.S. Safe Harbor da IBM. Estão disponíveis mais informações sobre o acordo Safe Harbor e a lista de empresas Safe Harbor aqui: http://export.gov/safeharbor/.

7.2 Aumento do Encargo de Subscrição Anual 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, numa percentagem a determinar pela IBM e que não excederá 3%. O ajuste do encargo de subscrição entrará em vigor no aniversário da data do período de cobertura inicial. Este ajuste do encargo não altera a titularidade do Cliente relativamente ao IBM SaaS, nem a métrica de encargos através da qual o IBM SaaS foi obtido. Os Parceiros de Negócios IBM são independentes da IBM e determinam unilateralmente os seus preços e condições.

7.3 Suporte Premium

O Cliente tem direito a Suporte Premium apenas para as ofertas do IBM SaaS para as quais o Cliente subscreveu a oferta de Suporte Premium associada.

7.4 Utilização e Consentimento Legal

Autorização para Recolha e Tratamento de Dados

O IBM SaaS foi concebido para ajudar o Cliente a melhorar o seu ambiente de segurança e dados. O IBM SaaS irá recolher informações de Participantes Elegíveis e Dispositivos Clientes que interagem com as Aplicações Empresariais ou de Retalho para as quais o Cliente subscreveu a cobertura das ofertas do IBM SaaS. O IBM SaaS recolhe informações que, individualmente ou em combinação, podem ser considerados Dados Pessoais em algumas jurisdições. Dados Pessoais correspondem a quaisquer informações que possam ser utilizadas para identificar um indivíduo específico, como o nome, endereço de correio electrónico, endereço pessoal ou número de telefone, facultadas à IBM para guardar, processar ou transferir em nome do Cliente.

As práticas de recolha e tratamento de dados podem ser actualizadas para melhorar a funcionalidade do IBM SaaS. Um documento com uma descrição completa das práticas de recolha e tratamento de dados é actualizado conforme necessário e está disponível para o Cliente, a pedido. O Cliente autoriza a IBM a recolher estas informações e a processá-las em conformidade com a secção Transferências Transfronteiriças e a secção Privacidade de dados dos presentes ToU e a secção Privacidade de Dados e Segurança de Dados dos Termos Gerais dos ToU.

Para as ofertas IBM Security Trusteer Pinpoint:

Os dados recolhidos podem incluir o endereço IP, o ID de utilizador indexado de sentido único ou encriptado, cookies de domínio caso não sejam filtrados, visitas a Aplicações protegidas e sites de phishing, localização geográfica e credenciais introduzidas em sites de phishing.

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

Os dados recolhidos podem incluir o endereço IP do utilizador, o ID de utilizador indexado de sentido único ou encriptado, a localização geográfica e visitas a Aplicações protegidas, informações de cartões SIM, nome de dispositivos e afiliação ao Cliente.

Para as ofertas IBM Security Trusteer Rapport:

Os dados recolhidos podem incluir o endereço IP do utilizador, o ID de utilizador indexado de sentido único ou encriptado, eventos de segurança, o nome de utilizador e endereço de correio electrónico fornecido para efeitos de contacto com a IBM para suporte ao cliente, afiliação ao cliente, palavra-passe encriptada introduzida em sites protegidos, visitas a Aplicações protegidas e sites de phishing, número de cartão de pagamento encriptado e ficheiros e dados recolhidos remotamente por pessoal da IBM para inspeccionar software malicioso suspeito, actividade maliciosa ou funcionamento incorrecto.

Consentimento Informado dos Titulares dos Dados:

A utilização deste IBM SaaS poderá envolver a aplicação de várias leis ou regulamentos. O IBM SaaS só pode ser utilizado para fins legais e de uma forma compatível com a lei. O Cliente concorda em utilizar o IBM SaaS em conformidade com as leis, regulamento e políticas aplicáveis, e assume toda a responsabilidade pelo seu cumprimento.

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

O Cliente declara que obteve ou irá obter quaisquer consentimentos inteiramente informados, permissões ou licenças necessárias para permitir a utilização nos termos da lei do IBM SaaS e permitir a recolha e o tratamento das informações, por parte da IBM, através do IBM SaaS.

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

O Cliente autoriza a IBM a obter os consentimentos inteiramente informados necessários para permitir a utilização nos termos da lei do IBM SaaS e recolher e processar as informações descritas no Acordo de Licença de Utilizador Final, disponível em https://www.trusteer.com/support/end-user-license-agreement. Caso o Cliente determine que as comunicações de consentimento com os utilizadores finais serão tratadas por si (e não pela IBM), o Cliente declara que obteve ou irá obter quaisquer consentimentos inteiramente informados, permissões ou licenças necessárias para permitir a utilização nos termos da lei do IBM SaaS e permitir a recolha e o tratamento de dados das informações, por parte da IBM enquanto subcontratante para o tratamento de dados do Cliente, através do IBM SaaS.

7.5 Transferências Transfronteiriças

O Cliente aceita que a IBM possa processar o conteúdo, incluindo quaisquer Dados Pessoais, ao abrigo das leis e requisitos relevantes, além fronteiras, para subcontratantes e sub-subcontratantes para o tratamento nos seguintes países fora do Espaço Económico Europeu e países considerados pela Comissão Europeia com dispondo de níveis adequados de segurança: EUA.

7.6 Privacidade de Dados

Se o Cliente disponibilizar Dados Pessoais ao IBM SaaS nos Estados Membros da UE, na Islândia, Liechtenstein, Noruega ou Suíça, ou se o Cliente tiver Participantes Elegíveis ou Dispositivos Clientes nestes países, o Cliente, na qualidade de único responsável, nomeia a IBM como subcontratante para o tratamento (conforme definido na Directiva da UE 95/46/CE) de Dados Pessoais. A IBM só tratará os referidos Dados Pessoais na medida necessária para disponibilizar a oferta do IBM SaaS em conformidade com as descrições do IBM SaaS publicadas pela IBM e o Cliente aceita que o referido tratamento está de acordo com as suas instruções. A IBM irá avisar o Cliente com uma antecedência razoável caso a IBM efectue qualquer alteração substancial à localização de processamento ou à forma como protege os Dados Pessoais como parte do IBM SaaS. O Cliente pode pôr termo ao Período de Subscrição actual relativo ao IBM SaaS afectado, mediante notificação por escrito à IBM nos trinta (30) dias seguintes à notificação da IBM ao Cliente sobre a referida alteração. O Cliente aceita que a IBM possa processar conteúdo, incluindo quaisquer Dados Pessoais, além fronteiras, para os seguintes processadores e subprocessadores:

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

O Cliente aceita que a IBM possa, mediante aviso prévio, modificar esta lista de localizações de países, caso o determine razoavelmente necessário para o fornecimento do IBM SaaS.

O Cliente aceita que, no caso de serviços prestados através do centro de dados alemão, tal como determinado durante o processo de aprovisionamento, a IBM possa processar conteúdo, incluindo quaisquer Dados Pessoais, além fronteiras para os seguintes subcontratantes e sub-subcontratantes:

Nome do Subcontratante/Sub-subcontratante para o Tratamento	Função (Subcontratante ou Sub-subcontratante para o Tratamento de Dados)	Localização*
A entidade contratante IBM	Subcontratante para o Tratamento	Conforme indicado no Documento de Transacção
Amazon Web Services (Germany)	Sub-subcontratante para o Tratamento	Munique, Alemanha
IBM Israel Ltd.	Sub-subcontratante para o Tratamento	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

O Cliente aceita que, no caso de serviços prestados através do centro de dados do Japão, tal como determinado durante o processo de aprovisionamento, a IBM possa processar conteúdo, incluindo quaisquer Dados Pessoais, além fronteiras para os seguintes subcontratantes e sub-subcontratantes:

Nome do Subcontratante/Sub-subcontratante para o Tratamento	Função (Subcontratante ou Sub-subcontratante para o Tratamento de Dados)	Localização*
A entidade contratante IBM	Subcontratante para o Tratamento	Conforme indicado no Documento de Transacção
Amazon Web Services (Japan)	Sub-subcontratante para o Tratamento	Tóquio, Japão
IBM Israel Ltd.	Sub-subcontratante para o Tratamento	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* As localizações identificadas nas tabelas acima incluem os endereços dos escritórios corporativos do Subcontratante/Sub-subcontratante. Os centros de dados estão localizados no mesmo país identificado.

As partes ou as suas afiliadas relevantes poderão celebrar acordos de Cláusulas-Tipo padrão não modificados da UE no desempenho das suas funções, nos termos da Decisão 2010/87/UE da CE, com remoção das cláusulas opcionais. Quaisquer litígios ou responsabilidades resultantes de qualquer um destes acordos, mesmo se celebrado por afiliadas, serão tratados pelas partes como se o litígio ou responsabilidade tivesse ocorrido entre essas partes, ao abrigo do presente Acordo.

Apêndice A

1. Ofertas do IBM SaaS

A IBM disponibiliza estes serviços como serviços e ofertas autónomos ou como serviços e ofertas adicionais. As ofertas específicas do IBM SaaS encomendadas são especificadas na PoE do Cliente.

1.1 Definições de Empresarial e Retalho

Os produtos IBM Security Trusteer Fraud Protection são licenciados para utilização com tipos específicos de Aplicações. Uma Aplicação é definida como um dos seguintes tipos: Retalho ou Empresarial. Estão disponíveis ofertas separadas para Aplicações de Retalho e Aplicações Empresariais.

- Uma Aplicação de Retalho é definida como uma aplicação de banca online, aplicação móvel ou aplicação de comércio electrónico concebida para servir consumidores. A política do Cliente pode classificar determinadas pequenas empresas como elegíveis para acesso de retalho.
- Uma Aplicação Empresarial é definida como uma aplicação de banca online, aplicação móvel ou aplicação de comércio electrónico concebida para servir entidades corporativas, institucionais ou equivalentes, ou qualquer outra aplicação que não seja categorizada como Retalho.

1.2 Ofertas de Subscrição Base do IBM SaaS

Ofertas Empresariais:

- 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 Retalho:

- 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

À excepção das ofertas IBM Security Trusteer Mobile SDK, para cada oferta Empresarial ou de Retalho, existe um produto de Suporte Premium associado disponível mediante um encargo adicional.

1.3 Ofertas de Subscrição Adicionais do IBM SaaS 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 suplemento Empresarial ou de Retalho nas ofertas IBM Security Trusteer Rapport, excepto no caso dos suplementos do IBM Security Trusteer Rapport Mandatory Service, existe um produto de Suporte Premium associado disponível mediante um encargo adicional.

A subscrição do IBM Security Trusteer Rapport for Business ou do IBM Security Trusteer Rapport for Retail é um pré-requisito das ofertas de subscrição adicionais associadas do IBM SaaS indicadas na presente secção.

1.4 Ofertas de Subscrição Adicionais do IBM SaaS 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 o 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

Está disponível Suporte Premium, mediante um encargo adicional, para cada uma das ofertas adicionais do IBM SaaS indicadas nesta secção.

A subscrição de ofertas IBM Security Trusteer Pinpoint Malware Detection for Business ou de ofertas IBM Security Trusteer Pinpoint Malware Detection for Retail é um pré-requisito das ofertas de subscrição adicionais associadas do IBM SaaS indicadas nesta secção.

1.5 Outras Subscrições Adicionais do IBM SaaS

Qualquer Subscrição adicional do IBM SaaS para as subscrições base acima que não se encontre aqui especificada, quer esteja actualmente disponível ou em desenvolvimento, não é considerada uma actualização e deverá ser concedida em separado.

1.6 Definições

Titular de Conta – designa o utilizador final do Cliente que instalou o software de activação de cliente, aceitou o acordo de licença de utilizador final ("EULA") e efectuou a autenticação, pelo menos, uma vez na Aplicação Empresarial ou de Retalho do Cliente para a qual o Cliente subscreveu coberturas de ofertas do IBM SaaS.

Software Cliente do Titular de Conta – designa o software de activação de cliente do IBM Security Trusteer Rapport, o software de activação de cliente do IBM Security Trusteer Mobile Browser ou qualquer outro software de activação de cliente fornecido com algumas subscrições do IBM SaaS para instalação no dispositivo do utilizador final.

Trusteer Splash – refere-se ao ecrã inicial fornecido ao Cliente com base nos modelos de ecrã inicial disponíveis.

Página de Destino – refere-se à página alojada pela IBM que é fornecida ao Cliente com o ecrã inicial do Cliente e o Software Cliente do Titular de Conta.

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 faculta uma camada de protecção contra phishing e ataques de software malicioso MitB (Man-in-the-Browser). Utilizando uma rede de dezenas de milhar de terminais em todo o mundo, o IBM Security Trusteer Rapport recolhe informações sobre ataques de phishing e software malicioso activos contra organizações de todo o mundo. O IBM Security Trusteer Rapport aplica algoritmos comportamentais destinados a bloquear ataques de phishing e a impedir a instalação e o funcionamento de estirpes de software malicioso MitB.

Esta oferta do IBM SaaS apresenta uma métrica de encargos de Participante Elegível. A oferta Empresarial é vendida em pacotes de 10 Participantes Elegíveis. A oferta de Retalho é vendida em pacotes de 100 Participantes Elegíveis.

Esta oferta do IBM SaaS inclui:

a. Trusteer Management Application ("TMA"):

   A TMA é disponibilizada no ambiente alojado na cloud do IBM Security Trusteer, através do qual o Cliente (e um número ilimitado de pessoal autorizado) pode: (i) receber relatórios de dados de eventos e avaliações de risco, (ii) ver, configurar e definir políticas relacionadas com relatórios de dados de eventos, e (iii) ver a configuração do software de activação de cliente licenciado ao público nos termos de um acordo de licença de utilizador final ("EULA") sem quaisquer custos e disponibilizado para transferência para os computadores desktop ou dispositivos (PC/MACs), também designado por conjunto de software Trusteer Rapport ("Software Cliente do Titular de Conta"). O Cliente pode apenas comercializar o Software Cliente do Titular de Conta utilizando o Trusteer Splash ou a Rapport API, sendo que o Cliente não poderá utilizar o Software Cliente do Titular de Conta para as suas operações de negócio internas ou para utilização dos seus funcionários (para além da utilização pessoal por parte dos funcionários).

b. Script da Web:

   Para acesso a um website para efeitos de acesso ou utilização das ofertas do IBM SaaS.

c. Dados de eventos:

   O Cliente (e um número ilimitado de pessoal autorizado) pode utilizar a TMA para receber dados de eventos gerados no Software Cliente do Titular de Conta em resultado das interacções online dos Titulares de Contas com a respectiva Aplicação Empresarial ou de Retalho para a qual o Cliente subscreveu cobertura de ofertas do IBM SaaS. Os dados de eventos serão recebidos a partir do Software Cliente do Titular de Conta nos dispositivos dos Participantes Elegíveis que tenham aceitado o EULA e efectuado a autenticação na Aplicação Empresarial ou de Retalho do Cliente pelo menos uma vez, sendo que a configuração do Cliente tem de incluir a recolha de IDs de utilizador.

d. Trusteer Splash:

   A plataforma de marketing Trusteer Splash identifica e comercializa o Software Cliente do Titular de Conta aos Participantes Elegíveis que acedem às Aplicações Empresarial e/ou de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS. O Cliente pode seleccionar entre os Modelos de Ecrã Inicial disponíveis. Pode ser contratado um ecrã inicial personalizado num acordo ou definição de trabalho em separado.

O Cliente pode aceitar fornecer as respectivas marcas comerciais, logótipos ou ícones para utilização em ligação com a TMA e apenas para utilização com o Trusteer Splash e para apresentação no Software Cliente do Titular de Conta ou nas páginas de destino alojadas pela IBM no website do IBM Security Trusteer. Qualquer utilização das respectivas marcas comerciais, logótipos ou ícones fornecidos será efectuada em conformidade com as políticas razoáveis da IBM no que respeita a publicidade e utilização de marcas comerciais.

O Cliente terá de subscrever a oferta IBM Security Trusteer Rapport Mandatory Service SaaS, caso o Cliente pretenda utilizar qualquer tipo de implementação obrigatória do Software Cliente do Titular de Conta.

A implementação obrigatória do Software Cliente do Titular de Conta inclui, mas não se limita a, qualquer tipo de implementação obrigatória através de qualquer mecanismo ou meio que, directa ou indirectamente, obrigue um Participante Elegível a transferir o Software Cliente do Titular de Conta, ou qualquer outro método, ferramenta, procedimento, acordo ou mecanismo, não criado por ou aprovado pela IBM, criado com o objectivo de contornar os requisitos de licenciamento desta implementação obrigatória do Software Cliente do Titular de Conta.

2.2 Ofertas Adicionais Opcionais do IBM SaaS para 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 da subscrição de quaisquer das seguintes ofertas adicionais do IBM SaaS. Se o IBM SaaS for designado como "for Business", a oferta adicional do IBM SaaS adquirida tem igualmente de ser designada como "for Business". Se o IBM SaaS for designado como "for Retail", a oferta adicional do IBM SaaS adquirida tem igualmente de ser designada como "for Retail". O Cliente receberá dados de eventos de Participantes Elegíveis que executem o Software Cliente do Titular de Conta, tenham aceitado o EULA e efectuado a autenticação

na(s) Aplicação(ões) Empresarial e/ou de Retalho do Cliente, sendo que a configuração do Cliente tem de incluir a recolha de IDs de Utilizador.

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 pessoal autorizado) pode utilizar a TMA para receber dados de eventos relacionados com infecções por software malicioso e outras vulnerabilidades de terminais no computador desktop de um determinado Titular de 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 pessoal autorizado) pode utilizar a TMA para receber notificações de dados de eventos relacionados com a submissão de credenciais de início de sessão do Titular de Conta num site de phishing ou potencialmente fraudulento suspeito. As aplicações online legítimas (URLs) podem ser erroneamente identificadas como sites de phishing e o IBM SaaS pode alertar os Titulares de Contas que um site legítimo é um site de phishing. Nesse caso, o Cliente terá de notificar a IBM de tal erro e a IBM compromete-se a corrigir o erro. Este será o único recurso do Cliente relativamente a 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 poderá utilizar uma instância da plataforma de marketing Trusteer Splash para exigir a transferência do Software Cliente do Titular de Conta aos Participantes Elegíveis que acedam às Aplicações Empresariais e/ou de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS.

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

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

O Cliente poderá implementar a funcionalidade adicional do IBM Security Trusteer Rapport Mandatory Service apenas se tiver sido encomendada e configurada para utilização com a Aplicação de Retalho ou Empresarial do Cliente para a qual o Cliente subscreveu cobertura de ofertas do IBM SaaS.

3. Ofertas IBM Security Trusteer Pinpoint

O IBM Security Trusteer Pinpoint é um serviço baseado na cloud concebido para facultar uma camada adicional de protecção e que visa detectar e mitigar ataques de software malicioso, phishing e tomada de controlo de contas. O Trusteer Pinpoint pode ser integrado nas Aplicações Empresariais e/ou de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS e processos de prevenção de fraude.

Esta oferta do IBM SaaS inclui:

a. TMA:

   A TMA é disponibilizada no ambiente alojado na cloud do IBM Security Trusteer, através da qual o Cliente (e um número ilimitado de pessoal autorizado) pode: (i) receber relatórios de dados de eventos e avaliações de risco, e (ii) ver, configurar e definir políticas de segurança e políticas relacionadas com relatórios de dados de eventos.

b. Script da Web e/ou APIs:

   Para implementação num website, para efeitos de acesso ou utilização do IBM SaaS.

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

Em caso de detecção de software malicioso nas ofertas IBM Security Trusteer Pinpoint Malware Detection ou detecção de tomada de controlo de contas nas ofertas IBM Security Trusteer Pinpoint Criminal Detection, o Cliente deverá cumprir com o Manual de Melhores Práticas do Pinpoint. Não utilize as ofertas IBM Security Trusteer Pinpoint Malware Detection ou as ofertas IBM Security Trusteer Pinpoint Criminal Detection de qualquer modo que efecte a experiência dos Participantes Elegíveis imediatamente após uma detecção de software malicioso ou tomada de controlo de contas, de tal forma que permita a terceiros associar as acções do Cliente à utilização das ofertas IBM Security Trusteer

Pinpoint (por exemplo, notificações, mensagens, bloqueio de dispositivos ou bloqueio de acesso à Aplicação Empresarial e/ou de Retalho imediatamente após uma detecção de software malicioso ou tomada de controlo de contas).

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

Detecção sem cliente de uma actividade de tomada de controlo de conta suspeita por parte de navegadores que estabeleçam ligação a uma Aplicação Empresarial ou de Retalho, utilizando um ID de dispositivo, detecção de phishing e detecção de roubo de credenciais através de software malicioso. As ofertas IBM Security Trusteer Pinpoint Criminal Detection facultam uma camada adicional de protecção e visam detectar tentativas de tomada de controlo de contas e apresentar, directamente ao Cliente, pontuações de avaliação de risco de navegadores e dispositivos móveis (através do navegador nativo ou da aplicação móvel do Cliente) que acedam a uma Aplicação Empresarial ou de Retalho.

a. Dados de eventos:

   O Cliente (e um número ilimitado de pessoal autorizado) pode utilizar a TMA para receber dados de eventos gerados em resultado de interacções online de Participantes Elegíveis com Aplicação(ões) Empresarial(is) e/ou de Retalho para a(s) qual(is) o Cliente subscreveu cobertura de ofertas do IBM SaaS ou o Cliente pode receber os dados de eventos através de um modo de disponibilização de API 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 concebidas para facultar uma camada adicional de protecção e visam proteger contra tomada de controlo de contas e actividades fraudulentas, identificando o acesso criminoso a contas e proporcionando uma recomendação ao Cliente. Esta oferta do IBM SaaS recolhe informações com origem tanto na Aplicação Empresarial e/ou de Retalho do Cliente, utilizando a API PPCD Mobile, como nos dispositivos móveis de Participantes Elegíveis. As ofertas IBM Security Trusteer PPCD Mobile são concebidas para correlacionar informações complexas relacionadas com dispositivos móveis de Participantes Elegíveis com outras fontes de dados, tais como infecção por software malicioso em tempo real e incidentes de phishing integrados através de outras ofertas IBM SaaS do IBM Security Trusteer nos presentes ToU.

O Cliente pode aceder e utilizar as ofertas IBM Security Trusteer PPCD Mobile no ambiente alojado na cloud do IBM Security Trusteer e receber dados de avaliação de risco de dispositivos móveis de Participantes Elegíveis, gerados em resultado das interacções online destes dispositivos móveis com a Aplicação Empresarial ou de Retalho do Cliente para a qual o Cliente subscreveu a cobertura de ofertas do IBM SaaS. Para efeitos destas ofertas, "dispositivos móveis" incluem apenas telemóveis 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 sem cliente de navegadores financeiros infectados por software malicioso MitB (Man in the Browser) que estabeleçam ligação a uma Aplicação Empresarial e/ou de Retalho. As ofertas IBM Security Trusteer Pinpoint Malware Detection facultam uma camada adicional de protecção e visam permitir às organizações focarem-se em processos de prevenção de fraude com base em risco de software malicioso, facultando ao Cliente avaliações e alertas da presença de software malicioso financeiro MitB.

a. Dados de eventos:

   O Cliente (e um número ilimitado de pessoal autorizado) pode utilizar a TMA para receber dados de eventos gerados em resultado de interacções online de Participantes Elegíveis com Aplicação(ões) Empresarial(is) e/ou de Retalho do Cliente.

b. Edição Avançada:

   As Edições Avançadas para Empresas e/ou Retalho oferecem uma camada adicional de detecção e protecção que é ajustada e personalizada de acordo com a estrutura e fluxo das Aplicações Empresariais e/ou de Retalho do Cliente e podem ser personalizadas de acordo com o cenário de

ameaças específico que visa o Cliente. Pode ser incorporada em várias localizações nas Aplicações Empresariais e/ou de Retalho do Cliente.

A Edição Avançada é oferecida ao Cliente em quantidades mínimas de, pelo menos, 100.000 Participantes de Retalho Elegíveis ou 10.000 Participantes Empresariais Elegíveis, o que corresponde a 1000 pacotes de 100 Participantes Elegíveis para Retalho ou 1000 pacotes de Participantes Elegíveis para Empresas.

c. Edição Standard:

A Edição Standard para Empresas ou para Retalho é uma solução de rápida implementação que faculta as funcionalidades centrais desta oferta do IBM SaaS, tal como descrito no presente documento.

3.2 Ofertas Adicionais Opcionais do IBM SaaS para 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 do IBM Security Trusteer Rapport Remediation for Retail, existe 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 IBM Security Trusteer Pinpoint Carbon Copy for Retail, existe um pré-requisito do IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou do IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Para IBM Security Trusteer Pinpoint Carbon Copy for Business, existe um pré-requisito do IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition ou do 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

Ofertas IBM Security Trusteer Pinpoint Carbon Copy concebidas para fornecer uma camada adicional de protecção e um serviço de monitorização que pode ajudar a identificar se as credenciais de um Participante Elegível foram comprometidas por ataques de Phishing nas Aplicações de Retalho ou Empresariais do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

O IBM Security Trusteer Rapport Remediation for Retail visa investigar, reparar, bloquear e remover infecções por software malicioso MitB (man-in-the-browser) de dispositivos infectados (PC/MACs) de Participantes Elegíveis do Cliente que acedam à Aplicação de Retalho do Cliente numa base ad-hoc, sempre que tenham sido detectadas infecções por software malicioso MitB através de dados de eventos do IBM Security Trusteer Pinpoint Malware Detection. O Cliente tem de ter uma subscrição actual do IBM Security Trusteer Pinpoint Malware Detection em execução na Aplicação de Retalho do Cliente. O Cliente pode utilizar esta oferta do IBM SaaS apenas em relação com Participantes Elegíveis que acedam à Aplicação de Retalho do Cliente e exclusivamente como uma ferramenta que visa investigar e reparar um determinado dispositivo infectado (PC/MAC) numa base ad-hoc. O IBM Security Trusteer Rapport Remediation for Retail tem de ser efectivamente executado em tal dispositivo de Participante Elegível afectado (PC/MAC), tal Participante Elegível tem de aceitar o EULA, efectuar a autenticação na(s) Aplicação(ões) de Retalho do Cliente pelo menos uma vez e a configuração do Cliente tem de incluir a recolha de IDs de Utilizador. Para que não restem dúvidas, esta oferta do IBM SaaS não inclui o direito de utilizar o Trusteer Splash e/ou promover o Software Cliente do Titular de Conta de qualquer outra forma à população geral de Participantes Elegíveis 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 foi concebido para adicionar outra camada de protecção e visa facultar acesso online seguro por parte dos dispositivos móveis dos Participantes Elegíveis que acedam às Aplicações de Retalho ou Empresariais do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS, avaliação de risco de dispositivos móveis e protecção contra phishing. A detecção de Wi-Fi seguro só está disponível para plataformas Android. Para efeitos desta oferta do IBM SaaS, os dispositivos móveis incluem telemóveis ou tablets e não incluem PCs e Macs Portáteis.

Através da TMA, o Cliente (e um número ilimitado de pessoal autorizado) pode receber dados de eventos, análises informações estatísticas relacionadas com Dispositivos cujos Participantes Elegíveis tenham: (i) transferido o Software Cliente do Titular de Conta, uma aplicação licenciada ao público ao abrigo de um acordo de licença de utilizador final ("EULA") sem quaisquer custos e disponibilizada para transferência para os dispositivos móveis dos Participantes Elegíveis, e (ii) aceitado o EULA e efectuado a autenticação pelo menos uma vez nas Aplicações Empresariais e de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS. O Cliente só pode comercializar o Software Cliente do Titular de Conta utilizando o Trusteer Splash e não pode utilizar o Software Cliente do Titular de Conta para as suas operações de negócio internas.

a. Dados de eventos:

   O Cliente (e um número ilimitado de pessoal autorizado) pode utilizar a TMA para receber dados de eventos gerados em resultado das interacções online dos dispositivos móveis com as Aplicações de Retalho ou Empresariais do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS.

b. Trusteer Splash:

   A plataforma de marketing Trusteer Splash identifica e comercializa o Software Cliente do Titular de Conta aos Participantes Elegíveis que acedem às Aplicações Empresarial e/ou de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS. O Cliente pode seleccionar entre modelos de ecrã inicial disponíveis ("Modelo de Ecrã Inicial"). Pode ser contratado um ecrã inicial personalizado num acordo ou definição de trabalho em separado.

O Cliente pode aceitar fornecer as respectivas marcas comerciais, logótipos ou ícones para utilização em ligação com a TMA e apenas para utilização com o Trusteer Splash e para apresentação no Software Cliente do Titular de Conta e nas páginas de destino alojadas pela IBM no website do IBM Security Trusteer. Qualquer utilização das respectivas marcas comerciais, logótipos ou ícones fornecidos será efectuada em conformidade com as políticas razoáveis da IBM no que respeita a publicidade e utilização de marcas comerciais.

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 concebidas para adicionar outra camada de protecção, de modo a facultar acesso da Web seguro às Aplicações Empresariais e/ou de Retalho do Cliente para as quais o Cliente subscreveu cobertura de ofertas do IBM SaaS, avaliação de risco de dispositivos e protecção contra pharming. A detecção de Wi-Fi seguro só está disponível para plataformas Android.

As ofertas IBM Security Trusteer Mobile SDK incluem um kit de programador de software móvel proprietário ("SDK"), um pacote de software que contém documentação, bibliotecas de software proprietário de programação e outros ficheiros e itens relacionados, conhecido 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 aplicações móveis autónomas e protegidas para iOS ou Android do Cliente para as quais o Cliente subscrever cobertura de ofertas do IBM SaaS ("Aplicação Móvel Integrada do Cliente").

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

Através da TMA, o Cliente (e um número ilimitado de pessoal autorizado) pode receber relatórios de dados de eventos e avaliações de tendências de risco. Através da Aplicação Móvel Integrada do Cliente, o Cliente pode receber análises de risco e informações de dispositivos móveis relacionadas com dispositivos móveis dos Participantes Elegíveis que tenham transferido a Aplicação Móvel Integrada do Cliente, permitindo ao Cliente formular uma política de prevenção de fraude que aplique acções de mitigação face a estes riscos. Para efeitos desta oferta, "dispositivos móveis" incluem apenas telemóveis e tablets suportados e não incluem PCs ou MACs.

O Cliente pode:

a. utilizar internamente o IBM Security Trusteer Mobile SDK apenas para efeitos de desenvolvimento da Aplicação Móvel Integrada do Cliente;

b. incorporar o Redistribuível (apenas num formato de código objecto), como uma forma integral não separável na Aplicação Móvel Integrada do Cliente. Qualquer parte modificada ou intercalada do Redistribuível ao abrigo desta concessão de licença estará sujeita aos termos dos presentes ToU; e

c. comercializar e distribuir o Redistribuível para transferência para dispositivos móveis de Participantes Elegíveis ou para o titular do Dispositivo Cliente, desde que:

- Salvo na medida do expressamente permitido no presente Acordo, o Cliente (1) não poderá utilizar, copiar, modificar ou distribuir o SDK; (2) não poderá inverter a assemblagem, inverter a compilação ou de outra forma converter inverter a engenharia do SDK, salvo se expressamente permitido por lei sem possibilidade de renúncia contratual; (3) não poderá sublicenciar, alugar ou locar o SDK; (4) não poderá remover quaisquer direitos de autor ou ficheiros de aviso contidos no Redistribuível; (5) não poderá utilizar o mesmo nome de caminho que os ficheiros/módulos do Redistribuível original; e (6) não poderá utilizar os nomes ou marcas comerciais da IBM, seus licenciadores ou distribuidores em relação com a comercialização da Aplicação Móvel Integrada do Cliente sem o prévio consentimento por escrito da IBM ou desse licenciador ou distribuidor.
- O Redistribuível tem de permanecer integrada de uma forma não separável na Aplicação Móvel Integrada do Cliente. O Redistribuível tem de estar em formato de código objecto apenas e estar em conformidade com todas as orientações, instruções e especificações no SDK e respectiva documentação. O acordo de licença de utilizador final da Aplicação Móvel Integrada do Cliente terá de notificar o utilizador final de que o Redistribuível não pode ser i) utilizado para quaisquer fins que não o de activar a Aplicação Móvel Integrada do Cliente ii) copiado (excepto para efeitos de cópia de segurança), iii) posteriormente distribuído ou transferido iv) sujeito a inversão de assemblagem, inversão de compilação ou de outra forma convertido, salvo se especificamente permitido por lei sem possibilidade de renúncia contratual. O acordo de licença do Cliente tem de apresentar, no mínimo, um nível de protecção para a IBM igual ao dos termos do presente Acordo
- O SDK só pode ser implementado como parte do desenvolvimento interno do Cliente e testes unitários em dispositivos de teste móveis especificados do Cliente. O Cliente não está autorizado a utilizar o SDK para processamento de volumes de trabalho de produção, simulação de volumes de trabalho de produção ou teste de escalabilidade de qualquer código, aplicação ou sistema. O Cliente não está autorizado a utilizar qualquer parte do SDK para quaisquer outros fins.

O Cliente é responsável por toda a assistência técnica à Aplicação Móvel Integrada do Cliente e por quaisquer modificações aos Redistribuíveis efectuadas pelo Cliente, conforme permitido no presente documento.

O Cliente está autorizado a instalar e utilizar os Redistribuíveis e o IBM Security Mobile SDK apenas para suporte da utilização, por parte do Cliente, da oferta do IBM SaaS.

A IBM testou aplicações exemplo criadas com ferramentas móveis fornecidas no IBM Security Trusteer Mobile SDK ("Ferramentas Móveis") para determinar se seriam correctamente executadas em determinadas versões de plataformas de sistema operativo móvel da Apple (iOS), da Google (Android) e de terceiros (colectivamente, "Plataformas de SO Móvel"). No entanto, as Plataformas de SO Móvel são fornecidas por terceiros, não se encontram sob controlo da IBM e estão sujeitas a alterações sem aviso prévio à IBM. Deste modo, e não obstante qualquer disposição em contrário, a IBM não garante que quaisquer aplicações ou outro resultado criado através da utilização das Ferramentas Móveis sejam correctamente executados, interajam ou sejam compatíveis com quaisquer Plataformas de SO Móvel ou dispositivos móveis.

O Cliente concorda em criar, manter e facultar à IBM e aos seus auditores registos escritos exactos, "outputs" de ferramentas do sistema e outras informações do sistema suficientes para permitir a verificação passível de auditoria de que a utilização do IBM Security Trusteer Mobile SDK, por parte do Cliente, está em conformidade com os termos dos presentes ToU.

5. Implementação de Ofertas de Protecção Contra Fraude do IBM SaaS

A subscrição base do Cliente inclui actividades de configuração e implementação inicial necessárias, incluindo arranque único inicial, configuração, Modelo de Ecrã Inicial, teste e formação.

Podem ser contratados serviços adicionais mediante um encargo adicional, num acordo em separado.

Apêndice B

A IBM faculta o seguinte acordo de nível de serviço ("SLA") de disponibilidade para o IBM SaaS, sendo que este é aplicável se especificado no Documento de Transacção do Cliente:

Será aplicável a versão deste SLA vigente no início ou renovação do período de subscrição do Cliente. O Cliente compreende que o SLA não constitui uma garantia a favor do Cliente.

1. Definições

a. **Contacto Autorizado** – designa a pessoa indicada pelo Cliente à IBM que tem autorização para submeter Reclamações ao abrigo do presente SLA.

b. **Crédito de Disponibilidade** – designa a reparação que a IBM disponibilizará em consequência de uma Reclamação validada. O Crédito de Disponibilidade será aplicado sob a forma de um crédito ou desconto numa factura futura de encargos de subscrição relativas ao IBM SaaS.

c. **Reclamação** – designa uma reclamação submetida pelo Contacto Autorizado do Cliente à IBM, em conformidade com o presente SLA, por não ter sido atingido o Nível de Serviço durante um Mês Contratado.

d. **Mês Contratado** – designa o mês completo durante o período de vigência do IBM SaaS medido das 00h00 GMT no primeiro dia do mês até às 23h59 GMT no último dia do mês.

e. **Cliente** – designa uma entidade que subscreve o IBM SaaS directamente à IBM e que se encontra em situação de incumprimento de quaisquer obrigações materiais, incluindo obrigações de pagamento, ao abrigo do seu contrato com a IBM relativo ao IBM SaaS.

f. **Tempo de Inactividade** – designa um período de tempo durante o qual o processamento do sistema de produção do Serviço se encontra interrompido e todos os utilizadores do Cliente estão impedidos de utilizar todos os aspectos do Serviço para o qual dispõem de autorizações adequadas. O Tempo de Inactividade não inclui o período de tempo durante o qual o Serviço não está disponível em resultado de:

- Tempo de Inactividade Planeado do Sistema;
- Força Maior;
- Problemas com aplicações, equipamento ou dados do Cliente ou de terceiros;
- Actos ou omissões do Cliente ou de terceiros (incluindo qualquer pessoa que obtenha acesso ao IBM SaaS através das palavras-passe ou de equipamento do Cliente);
- Falha na adopção de configurações de sistemas requeridas e em plataformas suportadas para acesso ao IBM SaaS; ou
- Conformidade da IBM com quaisquer concepções, especificações ou instruções fornecidas pelo Cliente ou por terceiros em nome do Cliente.

g. **Evento** – designa uma circunstância ou um conjunto de circunstâncias concomitantes, que tenha como efeito o não cumprimento de um Nível de Serviço.

h. **Força Maior** – designa acasos, terrorismo, acções laborais, incêndios, inundações, terramotos, motins, guerra, actos governamentais, ordens ou restrições, vírus, ataques de recusa de serviço e outros comportamentos maliciosos, falhas de conectividade de utilitários e de rede ou qualquer outra causa de indisponibilidade do IBM SaaS alheia ao controlo razoável da IBM.

i. **Tempo de Inactividade Planeado do Sistema** – designa uma desactivação prevista do IBM SaaS para fins de manutenção.

j. **Nível de Serviço** – designa o padrão especificado abaixo, através do qual a IBM mede o nível de serviço que presta no presente SLA.

2. Créditos de Disponibilidade

a. De modo a ser elegível para submeter uma Reclamação, é necessário que o Cliente tenha registado um ticket de suporte para cada Evento junto do Help Desk de suporte ao Cliente da IBM para o IBM SaaS aplicável, em conformidade com o procedimento da IBM para comunicação de problemas de suporte de Gravidade 1. O Cliente tem de indicar todas as informações detalhadas

necessárias acerca do Evento e prestar assistência razoável à IBM no diagnóstico e resolução do Evento, na medida do necessário para tickets de suporte de Gravidade 1. O referido ticket tem de ser registado no prazo de vinte e quatro (24) horas após o Cliente ter tomado conhecimento de que o Evento afectou a respectiva utilização do IBM SaaS.

b. O Contacto Autorizado do Cliente terá de submeter a Reclamação do Cliente para obtenção de um Crédito de Disponibilidade num prazo não superior a três (3) dias úteis após o final do Mês Contratado ao qual a Reclamação se refere.

c. O Contacto Autorizado do Cliente terá de fornecer à IBM todos os detalhes razoáveis relativos à Reclamação, incluindo mas não se limitando a, descrições detalhadas de todos os Eventos relevantes e do Nível de Serviço ao qual se refere a reclamação de incumprimento.

d. A IBM irá avaliar internamente o Tempo de Inactividade total combinado durante cada Mês Contratado aplicável ao Nível de Serviço correspondente indicado na tabela abaixo. Os Créditos de Disponibilidade serão baseados na duração do Tempo de Inactividade medido desde a hora em que o Cliente indicou que foi afectado pela primeira vez pelo Tempo de Inactividade. Se o Cliente reportar a ocorrência simultânea de um Evento de Tempo de Inactividade da Aplicação e de um Evento de Tempo de Inactividade do Processamento de Dados, a IBM irá considerar os períodos de sobreposição do Tempo de Inactividade como um único período de Tempo de Inactividade e não como dois períodos separados de Tempo de Inactividade. Para cada Reclamação válida, a IBM irá aplicar o Crédito de Disponibilidade aplicável mais elevado com base no Nível de Serviço alcançado durante cada Mês Contratado, tal como indicado nas tabelas abaixo. A IBM não estará obrigada a vários Créditos de Disponibilidade correspondentes ao(s) mesmo(s) Evento(s) no mesmo Mês Contratado.

e. No caso do Serviço Agrupado (IBM SaaS individuais agrupados e vendidos em conjunto por um preço combinado único), o Crédito de Disponibilidade será calculado com base no preço combinado único correspondente ao Serviço Agrupado e não no encargo de subscrição mensal de cada IBM SaaS mensal. O Cliente pode apenas submeter Reclamações relacionadas com um IBM SaaS individual num conjunto em qualquer Mês Contratado, não sendo a IBM responsável por quaisquer Créditos de Disponibilidade respeitantes a mais do que um IBM SaaS num conjunto em qualquer Mês Contratado.

f. Se o Cliente adquiriu o IBM SaaS junto de um revendedor IBM válido numa transacção de recomercialização na qual a IBM conserve a principal responsabilidade pelo cumprimento do IBM SaaS e dos compromissos do SLA, o Crédito de Disponibilidade basear-se-á no RSVP (Relationship Suggested Value Price, Preço de Volume Sugerido de Relação) então actual correspondente ao IBM SaaS em vigor no Mês Contratado sujeito a Reclamação, com um desconto de 50%.

g. Os Créditos de Disponibilidade totais concedidos com respeito a qualquer Mês Contratado não deverão, em circunstância alguma, exceder dez por cento (10%) de um duodécimo (1/12) do encargo anual pago pelo Cliente à IBM pelo IBM SaaS.

h. A IBM utilizará bom senso razoável na validação de Reclamações com base em informações disponíveis nos registos da IBM, que prevalecerão no caso de um conflito com os dados nos registos do Cliente.

i. OS CRÉDITOS DE DISPONIBILIDADE FACULTADOS AO CLIENTE EM CONFORMIDADE COM O PRESENTE SLA CONSTITUEM O ÚNICO E EXCLUSIVO RECURSO DO CLIENTE NO QUE RESPEITA A QUALQUER RECLAMAÇÃO.

3. Níveis de Serviço

Disponibilidade do IBM SaaS durante um Mês Contratado

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

O "Nível de Serviço Alcançado", expresso em percentagem, é calculado como: (a) o número total de minutos num Mês Contratado menos (b) o número total de minutos de Tempo de Inactividade num Mês Contratado, dividido pelo (c) número total de minutos num Mês Contratado.

Exemplo: 250 minutos de Tempo de Inactividade total durante um Mês Contratado

Total de 43.200 minutos num Mês Contratado de 30 dias - 250 minutos de Tempo de Inactividade = 42.950 minutos _____ Total de 43.200 minutos	= 2% de Crédito de Disponibilidade para 99,4% de Nível de Serviço Alcançado durante o Mês Contratado

3.1 Exclusões

O presente SLA é disponibilizado apenas a Clientes IBM. Este SLA não se aplica às seguintes situações:

- Serviços Beta e de Teste.
- Ambientes de não produção, incluindo, mas não se limitando a teste, recuperação de desastre, garantia de qualidade ou desenvolvimento.
- Reclamações efectuadas por utilizadores, visitas, participantes e convidados autorizados de um Cliente do IBM SaaS.
- Em caso de incumprimento de quaisquer obrigações materiais por parte do Cliente ao abrigo dos presentes ToU, incluindo, sem limitação, violação de quaisquer obrigações de pagamento.