IBM MobileFirst Protect (SaaS)

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 intitulado Termos de Uso da IBM – Termos Gerais ("Termos Gerais") disponível na seguinte URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Em caso de 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 os ToU.

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

1. IBM SaaS

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

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser (SaaS) Step up for existing Customers
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Management Suite (SaaS)
- IBM MobileFirst Protect – Management Suite (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Secure Mail (SaaS)

- IBM MobileFirst Protect – Secure Mail (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up for existing Customers
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

2. Métricas de Encargos

O IBM SaaS é vendido sob uma das métricas de encargos a seguir, conforme especificado no Documento de Transação:

a. **Usuário Autorizado** – é uma unidade de medida pela qual o IBM SaaS pode ser obtido. O Cliente deve obter autorizações separadas e vinculadas a cada Usuário Autorizado distinto com acesso ao IBM SaaS de qualquer forma, direta ou indiretamente (por exemplo, por meio de um programa multiplex, dispositivo ou servidor de aplicativos), através de quaisquer meios. Devem ser obtidas autorizações suficientes para cobrir o número de Usuários Autorizados que receberam acesso ao IBM SaaS durante o período de medição especificado no Certificado de Titularidade (PoE) ou no Documento de Transação do Cliente.

b. **Gigabyte** – é uma unidade de medida pela qual o IBM SaaS pode ser obtido. Um Gigabyte é definido como 2 elevado à 30ª potência de bytes de dados (1.073.741.824 bytes). Devem ser obtidas autorizações suficientes para cobrir o número total de Gigabytes processados pelo IBM SaaS durante o período de medição especificado no Certificado de Titularidade (PoE) ou no Documento de Transação do Cliente.

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

d. **Dispositivo do Cliente** – é uma unidade de medida pela qual o IBM SaaS pode ser obtido. Um Dispositivo do Cliente é um dispositivo de computação de um único usuário ou um sensor com propósito especial ou um dispositivo de telemetria que solicita a execução de, ou recebe para execução, um conjunto de comandos, procedimentos ou solicitações, ou fornece dados para outro sistema de computador que geralmente é referido como um servidor, ou é, de qualquer outra forma, gerenciado pelo servidor. Diversos Dispositivos de Cliente podem compartilhar acesso a um servidor comum. Um Dispositivo de 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 é executado, fornece dados, usa serviços fornecidos pelo ou acessa de alguma outra forma o IBM SaaS durante o período de medição especificado no Certificado de Titularidade (PoE) ou no Documento de Transação do Cliente.

3. Encargos e Faturamento

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

3.1 Encargos Mensais Parciais

Um encargo mensal parcial conforme especificado no Documento de Transação pode ser calculado de maneira proporcional.

3.2 Encargos de Excedentes

Se o uso real do IBM SaaS pelo Cliente durante o período de medição exceder a autorização declarada no PoE, o Cliente será cobrado pelo excedente, conforme estabelecido no Documento de Transação.

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

O Certificado de Titularidade (PoE) do Cliente estabelecerá se o IBM SaaS será renovado no final do Período de Subscrição, designando um dos seguintes:

4.1 Renovação Automática

Se o PoE do Cliente declarar que a renovação do Cliente é automática, o Cliente poderá rescindir o Período de Subscrição do IBM SaaS a expirar através de uma solicitação por escrito para o representante de vendas IBM ou Parceiro Comercial IBM, pelo menos 90 (noventa) dias antes da data de expiração estabelecida no PoE. Se a IBM ou o Parceiro Comercial 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 pela mesma duração do Período de Subscrição original, conforme estabelecido no PoE.

A QUANTIDADE DE AUTORIZAÇÕES NA RENOVAÇÃO SERÁ IGUAL À MAIOR DAS QUANTIDADES DO PEDIDO ORIGINAL OU AO USO MENSAL RELATADO PARA O MÊS ANTERIOR À GERAÇÃO DA FATURA DE RENOVAÇÃO, A NÃO SER QUE A IBM RECEBA UMA NOTIFICAÇÃO ESPECIFICANDO UMA QUANTIDADE DE AUTORIZAÇÃO DIFERENTE.

A QUANTIDADE DE AUTORIZAÇÕES NA RENOVAÇÃO DA OFERTA STEP UP SERÁ IGUAL À QUANTIDADE DO PEDIDO ORIGINAL.

4.2 Faturamento Contínuo

Quando o PoE 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 um sistema de faturamento contínuo. Para descontinuar o uso do IBM SaaS e parar o processo de faturamento contínuo, o Cliente precisará fornecer à IBM ou a seu Parceiro Comercial IBM um aviso, por escrito, com noventa (90) dias de antecedência, solicitando o cancelamento do IBM SaaS do Cliente. Após o cancelamento do acesso do Cliente, o Cliente será cobrado por quaisquer encargos de acesso pendentes até durante o mês em que o cancelamento entrou em vigor.

4.3 Renovação Obrigatória

Quando o PoE declarar que o tipo de renovação do Cliente é "rescindir", o IBM SaaS terminará no final 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 fazer um pedido ao representante de vendas IBM ou Parceiro Comercial IBM do Cliente para adquirir um novo Período de Subscrição.

5. Suporte Técnico

O suporte técnico do IBM SaaS é um suporte estruturado de segundo nível para uma equipe de Operação do Cliente, não um suporte ao Usuário Final, e está disponível durante o período de subscrição.

O suporte é fornecido por meio de vários canais, 24 horas por dia, 7 dias da semana. Informações relacionadas à solução IBM SaaS podem ser localizadas no portal do produto.

Objetivos de Responsividade Esperados:

Gravidade	Definição de Gravidade	Inicial Objetivos de Tempo de Resposta	Cobertura do Tempo de Resposta
1	**Impacto crítico nos negócios/inatividade do serviço:** Funcionalidades essenciais para os negócios estão inoperáveis ou uma interface essencial falhou. Geralmente, se aplica a um ambiente de produção e indica uma incapacidade de acessar serviços que resulta em um impacto crítico nas operações. Essa condição requer uma solução imediata.	30 minutos	24 horas por dia, 7 dias por semana
2	**Impacto significativo nos negócios:** O uso de um recurso de negócios de serviço ou de uma função do serviço está gravemente restrito ou o Cliente corre o risco de perder prazos finais de negócios.	1 hora em horário comercial	24 horas por dia, 7 dias por semana
3	**Impacto menor nos negócios:** Indica que o serviço ou a funcionalidade está utilizável e não há um impacto crítico nas operações.	2 horas em horário comercial	24 horas por dia, 7 dias por semana
4	**Impacto mínimo nos negócios:** Uma solicitação ou consulta não técnica	3 horas em horário comercial	24 horas por dia, 7 dias por semana

6. Termos Adicionais da Oferta IBM SaaS

6.1 Limitação para Ofertas Step up

Para ofertas IBM SaaS designadas como "Step up for existing Customers" ("Step up SaaS"), o Cliente deve ter adquirido, prévia ou simultaneamente, as autorizações de licença apropriadas para o programa da IBM associado, conforme identificado no nome da oferta Step up SaaS. Por exemplo, o Cliente que compra o "IBM MobileFirst Protect – Devices (SaaS) Step up for existing Customers" deve ter autorizações licenciadas para o programa da IBM associado do IBM MobileFirst Protect. As autorizações do Cliente para o Step up SaaS não podem exceder as autorizações do programa da IBM associado.

Ao adquirir o Step up SaaS, o Cliente não poderá usar as mesmas autorizações de licença do programa da IBM associado dentro de seu ambiente instalado no local, bem como com as autorizações do Step up SaaS. Por exemplo, se o Cliente tiver 250 autorizações de Dispositivo do Cliente Gerenciado para o programa da IBM associado e optar por comprar 100 autorizações de Dispositivo do Cliente Gerenciado do Step up SaaS, o Cliente poderá gerenciar 100 Dispositivos do Cliente Gerenciados do Step up SaaS a partir do ambiente do IBM SaaS e 150 Dispositivos do Cliente Gerenciados a partir do software instalado no local.

O Cliente declara que adquiriu as (1) autorizações de licença e (2) Subscrição e Suporte aplicáveis para o(s) programa(s) da IBM associado(s). Durante o Período de Subscrição do Step up SaaS, o Cliente deve manter atualizados Subscrição e Suporte para as autorizações do programa da IBM usadas em conjunto com as autorizações do Step up SaaS. Caso a licença do Cliente para usar os programas da IBM associados ou Subscrição e Suporte do Cliente para os programas da IBM associados sejam finalizados, o direito do Cliente de usar o Step Up SaaS será finalizado.

6.2 Cookies

O Cliente concorda que a IBM pode usar cookies e tecnologias de rastreamento para coletar informações de identificação pessoal a fim de reunir estatísticas de uso e informações projetadas para ajudar a melhorar a experiência do usuário e/ou para customizar interações com usuários de acordo com http://www-01.ibm.com/software/info/product-privacy/index.html.

6.3 Transferências Além das Fronteiras

Se o Cliente disponibilizar Informações Pessoais para ofertas do IBM SaaS nos Estados Membros da União Europeia, Islândia, Liechtenstein, Noruega ou Suíça, Turquia e qualquer outro país da Europa que tenha decretado legislação de proteção ou de privacidade de dados locais, o Cliente concorda que a IBM pode processar o Conteúdo, incluindo quaisquer Informações Pessoais protegidas por leis e os requisitos relevantes, além das fronteiras de um país para processadores e subprocessadores nos países a seguir fora da Área Econômica Europeia e nos países considerados pela Comissão Europeia como tendo níveis adequados de segurança:

Nome do Processador/Subprocessador	Função (Processador ou subprocessador de dados)	Local
IBM Corporation	Subprocessador	1 New Orchard Rd. Armonk, NY 10504, EUA I
IBM India Private Limited	Subprocessador	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Índia

O Cliente concorda que a IBM pode, mediante aviso prévio, alterar esta lista de locais de país quando determinar razoavelmente que isso é necessário para a provisão do IBM SaaS.

6.4 Privacidade de Dados da União Européia

Se o Cliente disponibilizar dados pessoais para ofertas do IBM SaaS nos Estados Membros da União Europeia, Islândia, Liechtenstein, Noruega ou Suíça, Turquia e qualquer outro país da Europa que tenha decretado legislação de proteção ou de privacidade de dados locais, ou se o Cliente tiver usuários ou dispositivos autorizados nestes países, então o Cliente, como único controlador destes dados, nomeia a IBM como processador para processar Informações Pessoais (da forma que estes termos são definidos na Diretiva 95/46/EC da União Européia). A IBM só processará tais Informações Pessoais na medida necessária para tornar a oferta IBM SaaS disponível de acordo com as descrições publicadas do IBM SaaS, e o Cliente concordar que tal processamento está de acordo com as instruções do Cliente.

6.5 Conformidade como o Safe Harbor

As ofertas IBM SaaS estão incluídas na certificação US-EU Safe Harbor da Fiberlink Communications Corporation (Subsidiária da IBM). A IBM e a Fiberlink estão em conformidade com o U.S.–EU Safe Harbor Framework, conforme a definição do Departamento de Comércio dos Estados Unidos com relação à coleta, ao uso e à retenção de informações coletadas a partir da União Europeia. Para obter mais informações sobre o Safe Harbor ou para acessar a declaração de certificação da Fiberlink, acesse http://www.export.gov/safeharbor/.

Quando o US-EU Safe Harbor Framework da IBM não se aplicar a uma transferência de Informações Pessoais do Espaço Econômico Europeu (EEE), as partes ou suas afiliadas relevantes poderão firmar contratos distintos, não modificados, padrão EU Model Clause em suas funções correspondentes, em conformidade com a Decisão da Comunidade Européia 2010/87/EU com as cláusulas opcionais removidas. Todos os litígios ou responsabilidades oriundas desses contratos, mesmo se firmados pelas afiliadas, serão tratados pelas partes como se a disputa ou responsabilidade tivesse surgido entre elas sob os termos deste Contrato.

6.6 Locais de Benefício Derivado

Onde aplicável, os tributos são baseados no(s) local(is) que o Cliente identificar como recebedor(es) dos benefícios do IBM SaaS. A IBM aplicará tributos com base no endereço comercial listado no pedido do IBM SaaS como o local de benefício primário, a menos que o Cliente forneça informações adicionais à IBM. O Cliente é responsável por manter tais informações atualizadas e por fornecer quaisquer mudanças à IBM.

6.7 Dados Normativos

Não obstante qualquer disposição em contrário, apenas para propósitos de pesquisa normativa, análise, demonstração e relatórios normativos, a IBM pode reter e usar, em formato agregado e anônimo (ou seja, de modo que o Cliente ou seus usuários autorizados não possam ser identificados como a origem dos dados, e de modo que informações de identificação pessoal que permitem a identificação do Cliente ou dos usuários autorizados do Cliente sejam removidas), dados que refletem experiências individuais do usuário autorizado do Cliente com o IBM SaaS.

6.8 Uso Lícito e Consentimento

6.8.1 Autorização para Coletar e Processar Dados

O IBM SaaS é projetado para fornecer, gerenciar, proteger, monitorar e controlar dispositivos móveis. O IBM SaaS coletará informações dos usuários e dispositivos autorizados pelo Cliente para interagir com o IBM SaaS para o qual o Cliente está subscrito. O IBM SaaS coleta informações que, sozinhas ou em conjunto, podem ser consideradas Informações Pessoais em algumas jurisdições. Os dados coletados poderão incluir o nome do usuário autorizado, o número do telefone, o endereço de email registrado e o local do dispositivo, o ID do usuário e o histórico de navegação segura, informações sobre o hardware, o software e as configurações do dispositivo do usuário final e as informações geradas pelo dispositivo. O Cliente autoriza a IBM a coletar, processar e usar essas informações de acordo com os termos destes Termos de Uso.

6.8.2 Consentimento Informado dos Assuntos de Dados

O uso deste IBM SaaS pode envolver várias leis e vários regulamentos. O IBM SaaS só pode ser usado para propósitos lícitos e de uma forma lícita. O Cliente concorda em usar o IBM SaaS em conformidade com as leis, os regulamentos e as políticas aplicáveis e assume toda a responsabilidade pelo cumprimento dos mesmos.

O Cliente concorda que obteve ou que obterá quaisquer consentimentos inteiramente informados, permissões ou licenças necessários para permitir o uso lícito do IBM SaaS e para permitir a coleta e o processamento das informações pela IBM como processador de dados do Cliente por meio do IBM SaaS. O Cliente, por meio destes ToU, autoriza a IBM a obter os consentimentos inteiramente informados necessários para permitir o uso lícito do IBM SaaS e para coletar e processar as informações conforme descrito no contrato de licença do usuário final disponível em http://www.ibm.com/software/sla/sladb.nsf/.

6.9 Retenção de Dados

A IBM excluirá quaisquer informações coletadas que possam incluir Informações Pessoais, após o término destes Termos de Uso, exceto por aquelas que devem ficar obrigatoriamente retidas para os propósitos estabelecidos acima, ou pela lei, norma ou regulamento aplicáveis. Nesse caso, a IBM reterá as informações coletadas pelo período requerido por tal propósito, lei, norma ou regulamento aplicáveis.

Apêndice A

O MobileFirst Protect é uma plataforma em nuvem de fácil utilização com toda a funcionalidade essencial para o gerenciamento de ponta a ponta dos dispositivos móveis atuais, incluindo iPhones, iPads, Androids, dispositivos Kindle Fire, Windows Phones e smartphones BlackBerry. A seguir há uma breve descrição das ofertas IBM SaaS:

1. IBM MobileFirst Protect – Devices (SaaS)

Os principais recursos de gerenciamento de dispositivos móveis (MDM) incluem registro de dispositivo, configuração, gerenciamento de política de segurança e ações do dispositivo, tais como enviar mensagem, localizar, bloquear e limpar. Os recursos de MDM Avançado incluem regras de conformidade automatizadas, configurações de privacidade para dispositivos de uso pessoal (BYOD) e painéis e relatórios do Mobility Intelligence.

2. IBM MobileFirst Protect – Applications (SaaS)

O MobileFirst Protect Applications fornece a capacidade de incluir aplicativos e distribuí-los para os dispositivos suportados gerenciados pelo MobileFirst Protect. Isto inclui o MobileFirst Protect App Catalog, um aplicativo móvel para os usuários visualizarem, instalarem e serem alertados sobre atualizações para os aplicativos gerenciados.

3. IBM MobileFirst Protect – Application Security (SaaS)

O MobileFirst Protect Application Security fornece proteção de dados adicional para aplicativos corporativos que usam WorkPlace SDK durante o desenvolvimento ou para que aplicativos iOS façam upload de aplicativos (.ipa), o provisionamento de perfis e para que certificados de autenticação sejam integrados automaticamente. O Mobile Application Security integra o aplicativo ao Secure Productivity Suite. Esta integração permite o início de sessão unificado (SSO), o acesso à Intranet por meio do Mobile Enterprise Gateway e a imposição das configurações de segurança de dados.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

O MobileFirst Protect Gateway for Apps fornece a usuários fora da rede da empresa acesso direto e seguro a aplicativos internos sem a necessidade de uma conexão VPN completa com o dispositivo.

5. IBM MobileFirst Protect – Content (SaaS)

O MobileFirst Protect Content permite que o administrador inclua e distribua documentos para os dispositivos suportados que são gerenciados pelo IBM MobileFirst Protect. Inclui o IBM MobileFirst Protect Doc Catalog, um recipiente protegido por senha no dispositivo que fornece aos usuários uma maneira segura e simples de acessar, visualizar e compartilhar documentos. Inclui o acesso transparente a conteúdos e repositórios distribuídos como SharePoint, Box e Google Drive. O acesso a compartilhamentos privados de arquivos no SharePoint e Windows estão disponíveis com o MobileFirst Protect Mobile Enterprise Gateway. Os documentos gerenciados por meio do MobileFirst Protect podem ser controlados por versão, auditados e protegidos por meio das opções de política de Prevenção contra Perda de Dados (DLP), como, por exemplo, exigência de autenticação, restrição da funcionalidade de copiar-colar e bloqueio de abertura ou o compartilhamento em outros aplicativos.

6. IBM MobileFirst Protect – Document Sync (SaaS)

O MobileFirst Protect Document Sync fornece aos usuários a capacidade de sincronizar, de maneira fácil e segura, o conteúdo do usuário nos dispositivos móveis gerenciados. Os administradores podem assegurar-se de que políticas tais como restrição de recortar, copiar e colar e bloqueio de abertura e compartilhamento de conteúdo em outros aplicativos estejam em vigor para o conteúdo do usuário em todos os dispositivos. O conteúdo é armazenado de maneira segura, tanto na nuvem quanto no dispositivo, e acessado somente por meio do MobileFirst Protect Doc Catalog.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor é um poderoso conjunto de aplicativos para escritório que permite que os usuários trabalhem com documentos de negócios enquanto estiverem em trânsito. O MobileFirst Protect Secure Editor permite:

- Criar e editar arquivos .DOC, .PPT e .XLS.
- Usar o modo de apresentação de slides
- Trabalhar facilmente com anexos de e-mail e outros arquivos do MobileFirst Protect for iOS.

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

Com o MobileFirst Protect Gateway for Documents, as organizações podem usar o MobileFirst Protect Content para também oferecer aos dispositivos fora da rede da empresa acesso direto e seguro aos sites internos do Connections, sites do SharePoint, Windows File Shares e outros armazenamentos de arquivos, sem a necessidade de uma conexão VPN completa com o dispositivo. O uso do MobileFirst Protect Gateway for Documents exige a compra do MobileFirst Protect Content também. Suporta iOS 5.0 e Android 4.0 ou mais recente.

9. IBM MobileFirst Protect – Email Management (SaaS)

O MobileFirst Protect Email Management inclui os principais recursos para o suporte do Microsoft Exchange ActiveSync and Lotus Traveler.

- Exchange ActiveSync: Fornece suporte para dispositivos móveis que se conectam ao Microsoft Exchange usando o protocolo ActiveSync. Os recursos incluem as principais funções de gerenciamento de dispositivo móvel, tais como a capacidade de configurar dispositivos, criar e impor políticas ActiveSync (usar senha, bloquear ou permitir acesso a e-mail) e executar ações no dispositivo, tais como bloquear e limpar, bem como gerar relatórios detalhados sobre os atributos do dispositivo.
- Lotus Traveler: Fornece suporte para dispositivos móveis que se conectam ao IBM Lotus Notes® usando o protocolo Lotus Traveler. Os recursos incluem a capacidade de configurar dispositivos, bloquear ou permitir dispositivos, impor políticas de senha, limpar dispositivos e desenvolver relatórios detalhados sobre os atributos do dispositivo.

10. IBM MobileFirst Protect – Browser (SaaS)

O MobileFirst Protect Browser é um navegador da web com todos os recursos que permite acesso seguro a sites da intranet corporativa e que impõe o cumprimento das políticas de conteúdo, através da definição de políticas de segurança e de filtros de websites para garantir que os usuários acessem somente conteúdo da web aprovado, ou seja, baseado em determinadas categorias de conteúdo, tais como sites de rede social, explícitos ou malware. Inclui a capacidade de desativar navegadores da web nativos e de terceiros, tanto por meio de política de aplicativo quanto por inserção em lista de negra, quando combinado com o MobileFirst Protect Devices. Permite criar lista de exceções para websites e cookies restringidos, recursos de copiar, colar e imprimir e ativação do modo Quiosque.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

O MobileFirst Protect Gateway for Browser permite que dispositivos suportados acessem websites internos aprovados sem a necessidade de uma conexão VPN completa com o dispositivo.

12. IBM MobileFirst Protect for Blackberry (SaaS)

Fornece suporte para dispositivos móveis conectados ao BlackBerry Enterprise Server (BES) usando APIs BlackBerry. Os recursos incluem ações remotas como envio de mensagem, reconfiguração de senha, designação de políticas BES e limpeza, além de relatório detalhado sobre os atributos do dispositivo. A instalação do MobileFirst Protect Cloud Extender é obrigatória. Disponível somente para dispositivos visualizados ou gerenciados com MobileFirst Protect por meio do BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

O MobileFirst Protect Expenses permite que o administrador crie políticas de uso de dados e as designe para os dispositivos suportados que são gerenciados pelo MobileFirst Protect; permite ainda a atribuição dessas políticas para um dispositivo, um grupo ou de forma global, e a configuração de limites para envio de alertas e mensagens sobre a utilização de dados, tanto em rede de telefonia local quanto em roaming.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Conjunto/Pacote de produtos incluindo MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content e MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Conjunto/Pacote de produtos incluindo MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content e MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

O MobileFirst Protect Secure Mail fornece um aplicativo de produtividade de escritório seguro e separado para os usuários acessarem e gerenciarem e-mail, calendário e contatos, com a capacidade de controlar e-mails e anexos para evitar vazamento de dados, através da restrição da capacidade de encaminhar ou mover conteúdo para outros aplicativos, da obrigatoriedade de autenticação, da restrição das ações cortar-copiar-colar e do bloqueio de anexos de e-mail, autorizando apenas a sua visualização.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

O MobileFirst Protect Gateway Suite permite que apps suportados em iOS e Android se comuniquem de forma direta e segura com os recursos na rede interna da empresa.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Conjunto/Pacote de produtos incluindo MobileFirst Protect Content, MobileFirst Protect Document Editor e MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

O MobileFirst Protect Threat Management fornece segurança de dispositivo móvel aprimorada com detecção de malware de dispositivo móvel e detecção avançada de jailbreak/root. Com o MobileFirst Protect Threat Management, o Cliente poderá configurar e gerenciar políticas de conformidade relacionadas com malware detectado e outras vulnerabilidades de segurança.

20. IBM MobileFirst Protect – Content Service (SaaS)

O MobileFirst Protect Content Service (SaaS) fornece aos usuários a capacidade de fazer o upload de pacotes de aplicativos e documentos para o sistema MobileFirst Protect Content Distribution.

Clientes com o MobileFirst Protect Content Service também precisarão adquirir uma ou ambas autorizações do MobileFirst Protect Content Service Storage (SaaS) e do MobileFirst Protect Content Service Bandwidth (SaaS).

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

O MobileFirst Protect Content Service Storage (SaaS) fornece aos usuários a capacidade de adquirir a quantidade total de armazenamento de dados disponível para uso com o MobileFirst Protect Content Service (SaaS)

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

O MobileFirst Protect Content Service Bandwidth (SaaS) fornece aos usuários a capacidade de adquirir a quantidade total de largura de banda disponível para uso com o MobileFirst Protect Content Service (SaaS)

23. IBM MobileFirst Protect – Professional (SaaS)

Fornece aos negócios de pequeno e médio porte uma maneira de configurar remotamente smartphones e tablets, impor políticas de segurança, enviar aplicativos e documentos por push e proteger dados em dispositivos corporativos e pessoais. Possibilita o acesso aos recursos certos de gerenciamento de mobilidade para os negócios do Cliente de maneira rápida, fácil e financeiramente acessível.

24. IBM MobileFirst Protect – Laptop (SaaS)

Fornece ao Cliente a capacidade de se inscrever para, configurar, gerenciar, proteger e relatar dispositivos baseados em OS X e Windows PC com smartphones e tablets. As organizações podem manter perfis e políticas de segurança consistentes tanto em dispositivos de propriedade do funcionário e da empresa dentro do mesmo console de gerenciamento do MobileFirst Protect.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) for Windows-based PCs fornece inscrição over-the-air (OTA) e relatório de gerenciamento de inventário sobre informações de hardware, sistema operacional e software. O módulo de relatório de segurança do terminal fornece relatório e análise de dados interativos para os aplicativos fornecidos pelo Cliente, tais como antivírus, backup/recuperação, criptografia de dados e firewall pessoal, bem como correções do sistema operacional perdidas. O módulo de proteção de dados fornece relatório e análise interativos para serviços de segurança, incluindo criptografia de dados, prevenção de vazamento de dados e backup/recuperação, além de outros aplicativos integrados. Suporta Windows XP SP3, Windows Vista, Windows 7, Windows 8+ e Windows 8+ Pro (incluindo 32 bits e 64 bits onde aplicável).

As ações do dispositivo incluem:

- Enviar mensagem para o dispositivo
- Bloquear o dispositivo
- Localizar o dispositivo (Requer o MobileFirst Protect Laptop Location)
- Parar/iniciar/reiniciar serviços
- Desligar/Reinicializar
- Limpar o disco rígido
- Configurar definições para patches (remendo)
- Distribuir software

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) for Mac OS X fornece inscrição over e relatório de gerenciamento de inventário sobre informações de hardware, sistema operacional e software. O módulo de relatório de segurança do terminal fornece relatório e análise de dados interativos para os aplicativos fornecidos pelo Cliente, tais como antivírus, backup/recuperação, criptografia de dados e firewall pessoal, bem como correções do sistema operacional perdidas. O módulo de proteção de dados fornece relatório e análise interativos para serviços de segurança de dados, incluindo criptografia de dados. O módulo de gerenciamento de configuração fornece gerenciamento remoto de inúmeras configurações de dispositivo e usuário, incluindo: senha, e-mail, VPN e Wi-Fi. Suporta Mac OS X versão 10.7.3 ou superior.

As ações do dispositivo incluem:

- Bloquear o dispositivo
- Limpar o disco rígido
- Alterar a política de dispositivo

25. IBM MobileFirst Protect – Laptop Location (SaaS)

O MobileFirst Protect Laptop Location (SaaS) ativa a capacidade de localizar laptops e tablets suportados. O MobileFirst Protect informa as coordenadas do endereço IP ou do Wi-Fi e converte esses dados em um endereço facilmente reconhecível. Quando um dispositivo está on-line, sua localização atual pode ser recuperada. O MobileFirst Protect armazena os locais relatados ao longo do tempo, portanto, o histórico de locais fica disponível para revisão. Requer IBM MobileFirst Protect Laptop (SaaS) for Windows. Suporta Windows XP SP3, Windows Vista, Windows 7, Windows 8+ e Windows 8+ Pro (incluindo 32 bits e 64 bits onde aplicável).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Fornece os recursos da oferta MobileFirst Protect – Laptop (SaaS) e inclui os recursos a seguir:

- Permite fazer o upload de pacotes na plataforma do MobileFirst Protect Content Service (SaaS) e planejar a distribuição de carga útil para os dispositivos, que são gerenciados pelo serviço MobileFirst Protect Laptop (SaaS) para Microsoft Windows. O Cliente controla todos os aspectos da distribuição, incluindo instruções de instalação e direcionamento em nível de dispositivo, grupo ou global. O Cliente é responsável por toda a criação do arquivo de instalação e empacotamento. A IBM não fornece suporte à criação de pacotes de instalação.

27. IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)

Fornece às organizações a capacidade de manter políticas e perfis de segurança consistentes tanto em dispositivos corporativos, quanto em dispositivos de propriedade do funcionário, dentro do mesmo console de gerenciamento.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

Os principais recursos de gerenciamento de dispositivos móveis (MDM) incluem registro de dispositivo, configuração, gerenciamento de política de segurança e ações do dispositivo, tais como enviar mensagem, localizar, bloquear e limpar. Os recursos de MDM Avançado incluem regras de conformidade automatizadas, configurações de privacidade para dispositivos de uso pessoal (BYOD) e painéis e relatórios do Mobility Intelligence.

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Fornece a habilidade de acessar e-mails de forma segura, armazenar, distribuir e gerenciar aplicativos e fornecer acesso ao site de intranet usando o Secure Browser.

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Fornece a habilidade de gerenciar e configurar smartphones e tablets remotamente, impor políticas de segurança, distribuir dados, fazer relatórios sobre o uso do Wi-fi, que podem ser usados para rastrear uso de dados e despesas, bem como o armazenamento de conteúdo e a distribuição para aplicativos e documentos.

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Fornece aos negócios de pequeno e médio porte uma maneira de configurar remotamente smartphones e tablets, impor políticas de segurança, enviar aplicativos e documentos por push e proteger dados em dispositivos corporativos e pessoais.

32. IBM MaaS360 Educational Bundle Prime (SaaS)

Fornece às organizações educacionais a habilidade de gerenciar e configurar remotamente smartphones e tablets, impor políticas de segurança, distribuir dados, bem como armazenamento de conteúdo e distribuição para aplicativos e gerenciamento de aplicativos.

33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Fornece às organizações a capacidade de gerenciar, atualizar, localizar e distribuir software para laptops, fornecendo políticas de segurança consistentes entre todos os laptops/áreas de trabalho relatados no console de gerenciamento do MaaS360.

Apêndice B

A IBM fornece o acordo de nível de serviço ("SLA") de disponibilidade a seguir para o IBM SaaS, que será aplicável se especificado no Certificado de Titularidade (PoE) ou Documento de Transação do Cliente.

Aplicar-se-á a versão deste SLA que estiver em vigor no início ou no momento da renovação do período de subscrição do Cliente. O Cliente entende que o SLA não constitui uma garantia.

1. Definições

a. **Contato Autorizado** – significa o indivíduo designado pelo Cliente para a IBM com autorização para enviar 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 enviada pelo Contato Autorizado do Cliente à IBM, conforme este SLA, de que o Nível de Serviço não foi atingido durante um Mês Contratado.

d. **Mês Contratado** – significa cada mês completo durante a vigência do IBM SaaS medido de 0h00 (GMT) no primeiro dia do mês até 23h59 (GMT) no último dia do mês.

e. **Cliente** – significa uma entidade que subscreve o IBM SaaS diretamente a partir da IBM e que não está inadimplente com nenhuma obrigação material, incluindo obrigações de pagamento, no âmbido de seu contrato com a IBM para o IBM SaaS.

f. **Tempo de Inatividade** – significa o Tempo de Inatividade e/ou Tempo de Inatividade de Processamento de Entrada do Aplicativo aplicável ao Nível de Serviço correspondente na tabela abaixo. O Tempo de Inatividade não inclui o período de tempo durante o qual o IBM SaaS fica indisponível 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 um indivíduo obter acesso ao IBM SaaS por meio de senhas ou equipamentos do Cliente);
- Falha em aderir às configurações do sistema necessárias e às plataformas suportadas para o acesso ao IBM SaaS; ou
- A conformidade da IBM com qualquer design, especificação ou instrução fornecida pelo Cliente ou por um terceiro em nome do Cliente.

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

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

2. Créditos de Disponibilidade

a. Para ser elegível ao envio de uma Reivindicação, o Cliente deverá ter registrado um chamado de suporte para cada Evento no help desk de suporte ao Cliente IBM para o IBM SaaS aplicável, de acordo com o procedimento da IBM para relatar problemas de suporte de Gravidade 1. O Cliente deve fornecer todas as informações necessárias detalhadas sobre o Evento e ajudar de forma razoável a IBM com o diagnóstico e a resolução do Evento na medida necessária para os

chamados de suporte de Gravidade 1. Esse chamado deverá ser registrado dentro de vinte e quatro (24) horas após o Cliente ficar primeiramente ciente de que o Evento causou impacto no uso do IBM SaaS pelo Cliente.

b. O Contato Autorizado do Cliente deve enviar a Reivindicação para um Crédito de Disponibilidade não mais do que três (3) dias úteis após o término do Mês Contratado que é o objeto da Reivindicação.

c. O Contato Autorizado deve fornecer à IBM todos os detalhes razoáveis com relação à Reivindicação, incluindo, mas não se limitando a, descrições detalhadas de todos os Eventos relevantes e do Nível de Serviço reclamado por não ter sido atingido.

d. A IBM medirá internamente o Tempo de Inatividade total combinado 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 em que o Cliente relatou ter sido primeiramente 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 sobrepostos de Tempo de Inatividade como um único período de Tempo de Inatividade, e não como dois períodos distintos. Para cada Reivindicação válida, a IBM aplicará o mais alto Crédito de Disponibilidade aplicável 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 mesmo Evento no mesmo Mês Contratado.

e. Para Serviço Incluídos em Pacote Configurável (IBM SaaS individuais agrupados e vendidos juntos por um único preço conjunto), o Crédito de Disponibilidade será calculado com base no preço mensal único conjunto para o Serviço Incluído em Pacote Configurável, e não no encargo de subscrição mensal para cada IBM SaaS individual. O Cliente somente poderá submeter Reivindicações relacionadas a um Produto IBM SaaS individual incluído em um pacote, em qualquer Mês contratado e a IBM não será responsabilizada pelos Créditos de disponibilidade relacionados a mais de um Produto IBM SaaS incluído em um pacote, em qualquer Mês Contratado.

f. Caso o Cliente tenha adquirido o IBM SaaS a partir de um revendedor válido da IBM em uma transação de revenda na qual a IBM mantenha a responsabilidade primária de cumprir os compromissos do IBM SaaS e do SLA, o Crédito de disponibilidade será baseado no Preço Sugerido de Relacionamento por Volume (RSVP) então vigente para o IBM SaaS que esteja em vigor no Mês Contratado que é objeto de uma Reivindicação, descontado a uma razão de 50%.

g. O total em Créditos de Disponibilidade concedidos com relação a qualquer Mês Contratado não deve, sob nenhuma circunstância, exceder dez por cento (10%) de um doze avos (1/12) do encargo anual pago pelo Cliente para a IBM pelo IBM SaaS.

h. A IBM se utilizará de razoabilidade 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 AS ÚNICAS E EXCLUSIVAS REPARAÇÕES PARA O CLIENTE COM RELAÇÃO A QUALQUER REIVINDICAÇÃO.

3. Níveis de Serviço

Disponibilidade do IBM SaaS durante o Mês Contratado

Nível de Serviço Atingido (durante um Mês Contratado)	**Crédito de Disponibilidade (% do Encargo de Subscrição Mensal para o Mês Contratado que é objeto de uma Reivindicação)**
Menos de 99,8%	2%
Menos de 98,8%	5%
Menos de 95,0%	10%

O Nível de Serviço Atingido, 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: 50 minutos de Tempo de Inatividade total durante o Mês Contratado

Total de 43,200 minutos em um Mês Contratado de 30 dias - 50 minutos de Tempo de Inatividade = 43.150 minutos _____ 43.200 minutos totais	= 2% de Crédito de Disponibilidade para 99,8% do Nível de Serviço Atingido durante o Mês Contratado

4. Exclusões

Este Acordo de Nível de Serviço (SLA) está disponível apenas aos Clientes da IBMEste SLA não se aplica ao seguinte:

- Serviço beta e de teste.
- Ambientes de não produção, incluindo, dentre outros, de teste, recuperação de desastre, controle de qualidade ou desenvolvimento.
- Reivindicações feitas pelos usuários, guests, participantes e convidados autorizados do Cliente IBM do IBM SaaS.
- Software de Ativação