

Termos de Utilização da IBM – Termos de Oferta Específica do SaaS

IBM Application Security on Cloud

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 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:

- IBM Application Security Analyzer

2. Métricas de Encargos

O IBM SaaS é vendido nos termos das seguintes métricas, conforme especificado no Documento de Transação:

- Instância de Aplicação** – corresponde a uma unidade de medida segundo a qual o IBM SaaS pode ser obtido. Uma titularidade de Instância de Aplicação tem de ser obtida para cada instância de uma Aplicação ligada ao IBM SaaS. Se uma Aplicação tiver múltiplos componentes, sendo que cada um deles serve um propósito distinto e/ou uma base de utilizadores, e cada um deles pode ser ligado ao ou gerido pelo IBM SaaS, cada referido componente é considerado uma Aplicação independente. Além disso, os ambientes de teste, desenvolvimento, simulação e produção para uma Aplicação são considerados instâncias independentes da Aplicação e cada um deles tem de possuir uma titularidade. Múltiplas instâncias de Aplicação num único ambiente são consideradas instâncias independentes da Aplicação e cada uma delas tem de possuir uma titularidade. Têm de ser obtidas Titularidades suficientes para cobrir o número de Instâncias de Aplicação ligadas ao IBM SaaS durante o período de medição especificado na Prova de Titularidade (PoE) do Cliente ou no Documento de Transação.
- Acesso** – corresponde a uma unidade de medida segundo a qual o IBM SaaS pode ser obtido. Um Acesso consiste nos direitos de utilização do IBM SaaS. O Cliente tem de obter uma única titularidade de Acesso, de forma a utilizar o IBM SaaS durante o período de medição especificado na Prova de Titularidade (PoE) do Cliente ou num Documento de Transação.

3. Encargos e Faturação

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

3.1 Pagamento por Utilização

As opções de Pagamento por Utilização serão faturadas no mês seguinte àquele em que o serviço for utilizado, à taxa especificada no Documento de Transação.

3.2 Encargo Mensal Parcial

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

4. Suporte Técnico

Durante o Período de Subscrição e após a IBM notificar o Cliente de que o acesso ao IBM SaaS está disponível, é fornecido suporte técnico através de fóruns online e como suporte standard durante o período de tempo em que o Cliente incorrer em encargos de Pagamento por Utilização. A partir do IBM SaaS, os Clientes podem submeter um ticket de suporte ou abrir uma sessão de conversação para obter

assistência. A IBM disponibilizará o IBM Software as a Service Support Handbook que fornece informações de contacto de suporte técnico, bem como outras informações e processos.

Gravidade	Definição de Gravidade	Tempo de Resposta Iniciais	Cobertura de Tempo de Resposta
1	Impacto crítico no negócio/inatividade do serviço: Uma funcionalidade crítica do negócio está inoperável ou ocorreu uma falha numa interface crítica. Esta situação aplica-se normalmente a um ambiente de produção e indica uma incapacidade de acesso a serviços, resultando num impacto crítico nas operações. Esta condição requer uma solução imediata.	No prazo de 1 hora	24x7
2	Impacto significativo no negócio: Um serviço ou função do negócio encontra-se gravemente restringido na sua utilização ou o Cliente está em risco de falhar prazos de negócios.	No prazo de 2 horas de expediente	Horário de Expediente Seg. a Sex.
3	Impacto menor no negócio: Indica que o serviço ou funcionalidade pode ser utilizado e não tem impacto crítico nas operações.	No prazo de 4 horas de expediente	Horário de Expediente Seg. a Sex.
4	Impacto mínimo no negócio: Uma dúvida ou pedido não técnico	No prazo de 1 dia útil	Horário de Expediente Seg. a Sex.

4.1 Acesso aos Dados do Cliente

A IBM poderá aceder aos dados do Cliente com a finalidade de diagnosticar problemas relacionados com o serviço e facilitar verificações da aplicação do Cliente por parte do serviço. A IBM irá aceder aos dados apenas com a finalidade de corrigir defeitos ou de fornecer suporte para produtos ou serviços IBM.

5. Termos Adicionais da Oferta do IBM SaaS

As Verificações de Segurança podem não identificar todos os riscos de segurança numa aplicação.

O IBM SaaS pode ser utilizado para ajudar o Cliente a assegurar a conformidade com determinadas obrigações, quer estas se baseiem em leis, regulamentos, normas ou práticas. Quaisquer indicações, utilização sugerida ou orientação fornecida pelo Serviço não constitui qualquer parecer jurídico, contabilístico ou outro e recomenda-se que o Cliente obtenha os seus próprios pareceres jurídicos ou outros junto de especialistas. O Cliente é o único responsável por garantir que o Cliente e as suas atividades, aplicações e sistemas estão em conformidade com todas as leis, regulamentos, normas e práticas aplicáveis. A utilização deste Serviço não garante a conformidade com qualquer lei, regulamento, norma ou prática.

O IBM SaaS realiza testes invasivos e não invasivos no website e na aplicação móvel ou da Web que o Cliente opte por verificar, cujo teste implica certos riscos, incluindo, sem limitação, os seguintes:

- enquanto executam aplicações que se encontram sob teste, os sistemas informáticos do Cliente poderão parar ou avariar, resultando na indisponibilidade temporária do sistema ou em perda de dados;
- o desempenho e a produtividade dos sistemas do Cliente, bem como o desempenho e a produtividade de routers e firewalls associados, poderão diminuir temporariamente durante o teste;
- poderão ser criadas quantidades excessivas de mensagens de registo, resultando no consumo excessivo de espaço em disco pelo ficheiro de registo;
- os dados poderão ser alterados ou eliminados em consequência da investigação de vulnerabilidades;

- e. poderão ser ativados alarmes pelos sistemas de deteção de intrusão;
- f. poderão ser ativadas mensagens de correio eletrónico pela função de correio eletrónico da aplicação da Web que está a ser testada;
- e
- g. o serviço de cloud poderá intercetar o tráfego da rede monitorizada para efeitos de procura de eventos.

No caso de o Cliente introduzir credenciais de início de sessão autenticado para a aplicação sob teste no Serviço, o Cliente apenas deverá introduzir tais credenciais para contas de teste e não para utilizadores de produção. A utilização de credenciais de utilizador de produção poderá resultar na transmissão de dados pessoais através do Serviço.

O IBM SaaS poderá ser configurado para verificar aplicações da Web de produção. Quando o Cliente define o tipo de verificação como "produção", o serviço foi concebido para executar verificações de uma forma que reduza os riscos indicados acima; no entanto, em determinadas situações, o Serviço de Cloud poderá levar à degradação ou instabilidade do desempenho na infraestrutura e nos sites de produção testados. A IBM não presta quaisquer garantias ou declarações relativamente à adequação de utilização do Serviço de Cloud para verificar sites de produção.

É DA RESPONSABILIDADE DO CLIENTE DETERMINAR SE O SERVIÇO É APROPRIADO OU SEGURO PARA O WEBSITE, APLICAÇÃO DA WEB, APLICAÇÃO MÓVEL OU AMBIENTE TÉCNICO DO CLIENTE.

O IBM SaaS foi concebido para identificar uma variedade de potenciais problemas de segurança e conformidade em aplicações móveis e da Web e em serviços da Web. Não testa todas as vulnerabilidades ou riscos de conformidade, nem atua como barreira contra ataques de segurança. As ameaças, regulamentos e normas de segurança estão em constante mudança e o Serviço poderá não refletir todas estas alterações. A segurança e conformidade da aplicação da Web, dos sistemas e dos funcionários do Cliente, bem como quaisquer ações de reparação, são da exclusiva responsabilidade do Cliente. É do critério exclusivo do Cliente a utilização ou não utilização de quaisquer das informações fornecidas pelo Serviço.

Algumas leis proíbem qualquer tentativa não autorizada de intrusão ou acesso a sistemas informáticos. O CLIENTE É RESPONSÁVEL POR ASSEGURAR QUE NÃO UTILIZA O SERVIÇO PARA VERIFICAR WEBSITES E/OU APLICAÇÕES QUE NÃO OS WEBSITES E/OU APLICAÇÕES DE PROPRIEDADE DO CLIENTE OU AQUELES QUE O CLIENTE TENHA O DIREITO E AUTORIDADE PARA VERIFICAR.

5.2 Cookies

O Cliente tem conhecimento e concorda que a IBM pode, como parte do funcionamento e suporte normal do IBM SaaS, recolher informações pessoais do Cliente (dos seus funcionários e subcontratados) relacionadas com a utilização do IBM SaaS, através de tecnologias de rastreio e outras. A IBM recolhe estas informações com o objetivo de recolher estatísticas de utilização e informações sobre a eficácia do IBM SaaS, para efeitos de melhoria da experiência do utilizador e/ou personalização das interações com o Cliente. O Cliente confirma que irá obter ou obteve consentimento para permitir à IBM o processamento das informações pessoais recolhidas para as finalidades acima indicadas na IBM, noutras empresas IBM e suas subcontratadas, onde quer que a IBM ou as suas subcontratadas façam negócios, em conformidade com a legislação aplicável. A IBM respeitará os pedidos de funcionários e subcontratados do Cliente para aceder, atualizar, corrigir ou eliminar as respetivas informações de contacto.

5.3 Localizações Beneficiárias Derivadas

Sempre que aplicável, os impostos têm por base a(s) localização(ões) que o Cliente identifica como beneficiária(s) do IBM SaaS. A IBM irá aplicar impostos com base no endereço profissional indicado, ao encomendar um IBM SaaS, como principal localização beneficiária, salvo se o Cliente facultar informações adicionais à IBM. O Cliente é responsável por manter tais informações atuais e indicar quaisquer alterações à IBM.

Apêndice A

1. Descrição Geral do IBM Application Security on Cloud

O IBM Application Security on Cloud faculta um local único para prestar assistência ao Cliente na identificação de vulnerabilidades de segurança (tais como Injeção de SQL Injection, Scripting entre Sites e Fuga de Dados) para uma grande variedade de aplicações. O serviço inclui vários tipos de técnicas de pesquisa de segurança de aplicações, sendo que cada uma das quais identifica problemas de segurança nessa aplicação.

O IBM Application Security on Cloud faculta as seguintes funcionalidades:

- Pesquisa de vulnerabilidades de segurança em Aplicações Móveis. Esta funcionalidade é executada através de tecnologias de análise de segurança dinâmicas (blackbox) e Interativas (glassbox).
- Pesquisa de vulnerabilidades de segurança em Websites de produção e pré-produção. Esta funcionalidade é executada através de técnicas de análise de segurança dinâmicas (blackbox).
- Pesquisa de vulnerabilidades de segurança em fluxos de dados em aplicações da Web e de Ambiente de Trabalho. Esta funcionalidade é executada através de técnicas de análise de segurança estáticas (whitebox).
- Relatórios de vulnerabilidade de segurança detalhados que incluem resumos de elevado nível das conclusões e passos de reparação que podem ser seguidos pelos programadores.
- Integração com várias plataformas DevOps, como Maven e IBM UrbanCode