Anexo de Assinaturas de Nuvem

Adendo sobre as Medidas de Segurança da Informação

O Fornecedor implementou e manterá as medidas de segurança a seguir. Estas medidas, em conjunto com as medidas de segurança descritas na Especificação da Assinatura aplicável, são a única responsabilidade do Fornecedor no que diz respeito à segurança das Ofertas do Fornecedor. Salvo definição em contrário neste documento, todos os termos em maiúsculas utilizados neste documento terão os significados que lhes são atribuídos no Anexo de Assinaturas de Nuvem.

Função	Medidas
Programa de Segurança da Informação	O Fornecedor implementou e irá manter um programa de segurança da informação (incluindo a adoção de políticas e padrões internos) concebido para os seguintes efeitos: (a) identificar riscos de segurança razoavelmente previsíveis para as partes dos data centers, dos servidores, dos equipamentos de rede, dos firewalls e dos sistemas de software de hospedagem que estão sob o controle do Fornecedor e são utilizados para disponibilizar a Oferta do Fornecedor ("**Rede do Fornecedor**") e (b) mitigar os riscos de segurança identificados, sempre que considere adequado, incluindo através da realização de testes e avaliações de riscos regulares. O Fornecedor nomeou um ou mais responsáveis pela segurança que estão encarregados da coordenação, monitoramento e aplicação do programa de segurança da informação. O Fornecedor irá manter um programa de gestão de ameaças e vulnerabilidades que monitorará a existência de vulnerabilidades na Rede do Fornecedor de forma contínua. As vulnerabilidades são identificadas através de diversos métodos/fontes, que podem incluir fornecedores, investigadores de segurança, análises de vulnerabilidades, atividades da equipe de segurança ofensiva ou Red Team, testes de penetração e relatórios dos funcionários. As vulnerabilidades de terceiros divulgadas publicamente são revisadasquanto à aplicabilidade no ambiente do Fornecedor. De forma rotineira e regular, são realizadas análises e avaliações de vulnerabilidades na infraestrutura de aplicações do Fornecedor. Estes processos visam permitir a identificação e a remediação de vulnerabilidades de forma proativa, bem como cumprir os requisitos regulamentares e de conformidade aos quais o Fornecedor está sujeito.
Ciclo de Vida de Desenvolvimento Seguro e Resposta a Vulnerabilidades	O Fornecedor implementou e mantém um programa de ciclo de vida de desenvolvimento seguro, o qual define os passos que devem ser seguidos para garantir que as ofertas foram adequadamente projetadas, desenvolvidas e produzidas de acordo com a estrutura de um programa de governança formal. Este programa, em conjunto com o programa de segurança da informação do Fornecedor, ajuda a abordar aspectos relacionados com a segurança durante todo o ciclo de desenvolvimento e manutenção da Oferta do Fornecedor. O Fornecedor utiliza um processo rigoroso para avaliar e melhorar continuamente as respectivas práticas de desenvolvimento seguro e de resposta a vulnerabilidades, as quais são regularmente comparadas com as práticas padrão da indústria. Após investigar e validar uma vulnerabilidade relatada na Oferta do Fornecedor, o Fornecedor tentará identificar, desenvolver e qualificar uma solução adequada, de

	acordo com a política de resposta a vulnerabilidades do Fornecedor publicada e, atualmente disponível em: Política de Resposta a Vulnerabilidades do Fornecedor | Fornecedor nos EUA. O Fornecedor comunica as soluções aos clientes através de avisos de segurança, sempre que aplicável. O Fornecedor esforça-se por disponibilizar soluções num prazo comercialmente razoável. Os prazos de resposta dependerão de diversos fatores, tais como: a gravidade da vulnerabilidade, a complexidade da solução ou o componente afetado.
Gestão de Ativos	O Fornecedor monitora os ativos físicos e lógicos da Rede do Fornecedor. Seguem-se exemplos dos ativos que o Fornecedor pode monitorar e dos controles que pode implementar: (a) ativos de software, tais como aplicações e software do sistema, (b) ativos físicos, tais como servidores, desktops/computadores portáteis, fitas de cópia de segurança/arquivo, impressoras e equipamento de comunicações, e (c) ativos de informação, tais como bases de dados, planos de recuperação de desastres, planos de continuidade de negócio, classificação de dados e informações arquivadas. O Fornecedor classifica os ativos com base na criticidade para o negócio e/ou na sensibilidade da classificação dos dados. Essa classificação permite que o acesso aos ativos seja adequadamente restrito e gerenciado.
Segurança dos Recursos Humanos	No âmbito do processo de emprego, os funcionários do Fornecedor têm que assinar um contrato de confidencialidade quando da contratação e submeter-se a um processo de verificação, em conformidade com a legislação aplicável. Embora o Fornecedor se reserve o direito de rever as respectivas políticas e implementar medidas de segurança do pessoal a seu exclusivo critério, ao abrigo da política atual e sujeita à legislação e à disponibilidade locais, o Fornecedor realiza uma ou mais das seguintes verificações no âmbito do emprego: teste de drogas, verificação das informações da Seguro Social, pesquisa de registos criminais, verificação da formação académica e dos antecedentes profissionais e verificação da elegibilidade para o emprego. O Fornecedor busca cumpriros padrões atuais seguidos por empresas semelhantes que operam na mesma indústria, mas não pode adaptar as respectivas medidas de segurança do pessoal ou processo de verificação para satisfazer as expectativas específicas de um determinado Cliente. Os terceiros ou os contratantes externos são verificados pelo Fornecedor, como condição do contrato ou validados como tendo sido verificados pelo contratado de acordo com um processo de verificação aprovado pelo Fornecedor. O Fornecedor mantém um processo disciplinar para tomar medidas em relação ao pessoal que não cumpra os requisitos do programa de segurança da informação, incluindo, entre outros, os requisitos estabelecidos para cumprir os compromissos e requisitos de segurança, disponibilidade e confidencialidade. O Fornecedor disponibiliza formação anual de segurança a todo o pessoal relevante e exige que os subcontratados aplicáveis também forneçam esse treinamento ao seu pessoal.

Segurança Física	Existem controles baseados no risco nas instalações onde se encontram componentes físicos da Rede do Fornecedor (por exemplo, data centers). Os controles de acesso podem incluir guardas, registos de segurança, monitoramento, alarmes, acesso limitado a áreas protegidas, proteção das vias de acesso, videovigilância, cartões-chave e/ou autenticação de dois fatores. Esta disposição aplica-se aos Colocations geridos pelo Fornecedor e data centers gerenciados pelo Fornecedor que hospedam serviços de nuvem pública.
Segurança de Rede	A Rede do Fornecedor estará eletronicamente acessível ao pessoal do Fornecedor conforme necessário para disponibilizar a Oferta do Fornecedor. O Fornecedor manterá políticas e controles de acesso para gerir o acesso permitido à Rede do Fornecedor a partir de cada conexão, incluindo a utilização de firewalls e controles de autenticação. O Fornecedor atua contra a utilização maliciosa de ativos e software malicioso na Rede do Fornecedor através da implementação de controles com base no risco. Esses controles podem incluir, mas não se limitam a: políticas de segurança; controles de acesso restritivos; ambientes separados para desenvolvimento e testes; detecção de malware nos servidores, desktops e computadores portáteis; análise de anexos de e-mail para detectar malware; análises de conformidade do sistema; monitoramento para a prevenção de intrusões e resposta a intrusões; registro e alerta de eventos suspeitos importantes; procedimentos de processamento de informações baseados no tipo de dados, aplicação de e-commerce e segurança de rede; utilização de ativos externos; e análise de vulnerabilidades dos sistemas e das aplicações. O Fornecedor requer a encriptação dos dados em circulação e inativos onde tal for exigido e em conformidade com o programa de segurança da informação. O Fornecedor utiliza encriptação e protocolos apropriados (por exemplo, TLS) quando acessa remotamente o ambiente de um cliente ou ao transmitir dados do cliente por meio de redes abertas. O Fornecedor armazena as respectivas chaves de encriptação, quando não são utilizadas, em soluções aprovadas concebidas para proporcionar práticas de gestão de chaves aceitas pela indústria.
Controles de Acesso	O Fornecedor implementa controles de acesso adequados concebidos para proteger contra o acesso não autorizado à Rede do Fornecedor. Para reduzir o risco de utilização indevida, seja intencional ou não, o acesso à Rede de Fornecedor é controlado de acordo com os princípios do "menor privilégio" e da "necessidade de conhecer". Os controles de acesso que o Fornecedor pode utilizar incluem revisões de acesso, manutenção de contas de serviço e acesso privilegiado às aplicações, definições ao nível do sistema para acesso e geração de relatórios relacionados com o acesso. O Fornecedor utiliza práticas padrão da indústria, incluindo, quando aplicável, a autenticação de dois fatores, para identificar e autenticar os usuários da Rede do Fornecedor. O Fornecedor requer a utilização de senhas fortes na Rede do Fornecedor. O Fornecedor (a) proíbe que os usuários da Rede do Fornecedor compartilhem, escrevam, enviem por mensagem instantânea ou armazenem senhas não encriptadas em qualquer sistema e (b) bloqueia as contas após várias tentativas consecutivas de acesso com uma senha incorreta. Quando apropriado, o Fornecedor utiliza práticas padrão da indústria para melhorar os controles de acesso, incluindo: (a) interrupção automática das sessões dos usuários se permanecerem inativas após um determinado período;

	(b) requisito de identificação e introdução da senha para reiniciar a sessão; (c) proteção contra o acesso externo através de firewalls padrão aceitospela indústria cuja ligação à Internet, se aplicável, é protegidapor uma ligação VPN; (d) mascaramento das senhas quando são mostradas ou introduzidas, conforme o caso; e (e) encriptação apropriada e de acordo com os padrões da indústria das senhas quando forem transmitidas.
Gestão de Incidentes	O Fornecedor utiliza uma estrutura de resposta a incidentes para preparar, responder, gerir e minimizar os efeitos dos eventos de segurança. A estrutura inclui os procedimentos a serem seguidos caso ocorra um incidente de segurança, incluindo: (a) uma equipe interna de resposta a incidentes com um líder responsável pela resposta; (b) uma equipe de investigação que realize a análise da causa raiz e identifique as partes afetadas; (c) processos internos para a elaboração de relatórios e processo de notificação; (d) documentação das ações de resposta e dos planos de remediação; e (e) uma revisão pós-incidente dos eventos.
Gestão da Continuidade de Negócio	O Fornecedor mantém planos de continuidade de negócio ("**PCN(s)** ou **BCP**") para recuperar uma interrupção de negócio e retomar as operações comerciais normais logo que seja razoavelmente possível. O Fornecedor fará tentativas razoáveis e oportunas, dentro das circunstâncias, para contactar o Cliente caso ocorra uma interrupção de negócio que afete substancialmente os clientes do Fornecedor.