Adendo sobre as Medidas de Segurança da Informação - Dell APEX

Os Serviços Dell APEX utilizam um modelo de responsabilidade compartilhada no que diz respeito à segurança, segundo o qual o Cliente e a Dell têm determinadas responsabilidades, uma vez que os Serviços Dell APEX estão hospedados no local do Cliente ou em um Colocation e, geralmente, não envolvem a hospedagem de Conteúdo de Cliente em servidores localizados em data centers geridos pela Dell. As responsabilidades do Cliente são especificadas na Descrição da Oferta de Serviço aplicável.

A Dell implementou e irá manter as seguintes medidas de segurança empresarial relativamente aos Serviços Dell APEX. Estas medidas, em conjunto com as medidas de segurança referidas na Descrição da Oferta de Serviço aplicável, são a única responsabilidade da Dell no que diz respeito à segurança dos Serviços Dell APEX. Salvo definição em contrário neste documento, todos os termos em maiúsculas utilizados neste documento terão os significados que lhes são atribuídos no Contrato Dell APEX.

Função	Medidas
Programa de Segurança da Informação	A Dell 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, se existentes, dos data centers, dos servidores, dos equipamentos de rede, dos firewalls e dos sistemas de software de hospedagem da Dell que são utilizados para fornecer os Serviços Dell APEX ("**Rede Dell**") e (b) envidar esforços comercialmente razoáveis para mitigar os riscos de segurança identificados na Rede Dell, conforme a Dell considerar apropriado, incluindo através da realização de testes e avaliações de riscos regulares. A Dell nomeou um ou mais responsáveis pela segurança que estão encarregados da coordenação, monitoramento e aplicação do programa de segurança da informação. A Dell irá manter um programa de gestão de ameaças e vulnerabilidades que monitorá a existência de vulnerabilidades na Rede Dell 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 revistas quanto à aplicabilidade no ambiente da Dell. De forma rotineira e regular, são realizadas análises e avaliações de vulnerabilidades na infraestrutura de aplicações da Dell. 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 a Dell está sujeita.
Ciclo de Vida de Desenvolvimento Seguro e Resposta a Vulnerabilidades	A Dell 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 da Dell foram adequadamente avaliadas, desenvolvidas e produzidas de acordo com a estrutura de um programa de governança formal com um ciclo de vida de desenvolvimento seguro definido. Este programa, em conjunto com o programa de segurança da informação da Dell, ajuda a abordar aspectos relacionados com a segurança durante todo o ciclo de desenvolvimento e manutenção do Sistema Dell APEX. A Dell 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 informada no Sistema Dell APEX, a Dell tentará identificar, desenvolver e qualificar uma solução adequada, de acordo com a política de resposta a vulnerabilidades da Dell publicada e, atualmente disponível em https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy. A Dell comunica as soluções aos clientes através de avisos de segurança, sempre que aplicável. A Dell esforça-se por disponibilizar soluções num prazo comercialmente razoável, conforme aplicável. Os prazos de resposta dependerão de diversos fatores, tais como: a gravidade do problema, a complexidade da solução ou o componente afetado.
Gestão de Ativos	A Dell monitora e gera os ativos físicos e lógicos da Rede Dell. Seguem-se exemplos dos ativos que a Dell 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, faixas 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. A Dell 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.
Segurança dos Recursos Humanos	No âmbito do processo de emprego, os funcionários da Dell 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 a Dell 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, a Dell 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. A Dell tenta cumprir os 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 pela Dell, como condição do contrato ou validados como tendo sido verificados pelo contratado de acordo com um processo de verificação aprovado pela Dell. A Dell 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 da Dell.

	A Dell fornece formação anual de segurança a todo o pessoal relevante e exige que os subcontratados aplicáveis também forneçam essa treinamentoao seu pessoal.
Segurança Física	A Dell mantém políticas e controles que restringem o acesso físico às instalações onde se encontram os componentes físicos da Rede Dell somente ao pessoal autorizado, impedindo a entrada não autorizada nas instalações. Existem controles baseados no risco nas instalações onde se encontram componentes físicos da Rede Dell (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 pela Dell.
Segurança de Rede	A Rede Dell é eletronicamente acessível à Dell, conforme necessário para fornecer os Serviços Dell APEX. A Dell manterá políticas e controles de acesso para gerir o acesso permitido à Rede Dell a partir de cada conexão, incluindo a utilização de firewalls e controles de autenticação. A Dell atua contra a utilização maliciosa de ativos e software malicioso na Rede Dell através da implementação de controles com base no risco. Esses controles podem incluir, sem limitação: 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; registo 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. A Dell requer a encriptação dos dados em circulação e inativos onde tal for exigido e em conformidade com o programa de segurança da informação da Dell. A Dell utiliza encriptação e protocolos apropriados (por exemplo, TLS) quando acessa remotamente o sistema de um cliente através de redes abertas. A Dell 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	A Dell implementa controles de acesso adequados concebidos para proteger contra o acesso não autorizado à Rede Dell. Para reduzir o risco de utilização indevida, seja intencional ou não, o acesso é controlado de acordo com os princípios do "menor privilégio" e da "necessidade de conhecer". Os controles de acesso que a Dell 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. A Dell utiliza práticas padrão da indústria, incluindo, quando aplicável, a autenticação de dois fatores, para identificar e autenticar os usuários da Rede Dell. A Dell requer a utilização de senhas fortes na Rede Dell. A Dell (a) proíbe que os usuários da Rede Dell 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. A Dell 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 aceites pela indústria cuja ligação à Internet, se aplicável, é salvaguardada por 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	A Dell 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	A Dell 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. A Dell fará tentativas razoáveis e oportunas, dentro das circunstâncias, para contactar o Cliente caso ocorra uma interrupção de negócio que afete substancialmente o(s) Serviços(s) Dell APEX.