

Centro de Dados DoohNow & Segurança de Rede

SEGURANÇA FÍSICA	
Instalações	<p>Os serviços DoohNow são hospedados e gerenciados dentro de centros de dados seguros da Amazon e utiliza tecnologia Amazon Web Service (AWS). A Amazon atua em gestão de risco e avaliações recorrentes para assegurar a conformidade de acordo com a indústria de padrões tecnológicos. As operações de data center da Amazon são credenciados em:</p> <ul style="list-style-type: none">• ISO 27001• SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)• PCI Level 1• FISMA Moderate • Sarbanes-Oxley (SOX)
Segurança Local	<p>A DoohNow está em centro de dados ISO 27001 e FISMA certificados e geridos pela Amazon. Os centros de dados da AWS estão alojados em instalações de extensa vigilância que mantém controle de perímetro a nível militar bem como proteções de fronteira natural.</p> <p>O acesso físico é estritamente controlado tanto no perímetro quanto no prédio com pontos de acesso pessoal de segurança, através de vídeo, detecção de intrusos e outros meios eletrônicos. O pessoal autorizado deve passar por autenticação em dois fatores não menos do que três vezes para acessar pisos do centro de dados. Todos os visitantes e prestadores de serviços são obrigados a apresentar a identificação e são continuamente escoltados por pessoal autorizado.</p>
Localização	<p>Os centros prestadores de serviços de dados DoohNow atualmente em uso estão localizados nos Estados Unidos e Brasil.</p>

SEGURANÇA DE REDE

<p>Proteção</p>	<p>Toda infra-estrutura e gestão de firewalls são fornecidos pelo nosso serviço de provedores: Amazon AWS.</p> <p>Firewalls são utilizados para restringir o acesso a sistemas de redes externas e entre os sistemas internamente. Por padrão, todo o acesso é negado e só portas e protocolos explicitamente permitidos são aceitos com base em necessidade específicas. Cada sistema é atribuído a um grupo de segurança firewall com base na função do sistema necessária. Os grupos de segurança restringem o acesso a portas e protocolos exigindo função específicas de sistema a fim de conter riscos.</p> <p>Firewalls baseados em hardware também fornecem a capacidade de limitar ainda mais as conexões de entrada e de saída, conforme necessário, atribuindo assim maior segurança em toda camada de acesso a rede DoohNow.</p>
<p>Exploração de Vulnerabilidades</p>	<p>Os firewalls gerenciados evitam ataques de spoofing IP, MAC e ARP na rede e entre hosts virtuais para garantir que não seja possível a falsificação da identidade na rede. Pacotes sniffing são impedidos pela infra-estrutura, incluindo também com que máquinas virtuais não trafeguem em uma interface de rede na qual a mesma não seja destinada. Nosso serviço provedor utiliza isolamento de aplicativos, restrições do sistema operacional e conexões criptografadas para garantir ainda mais o risco em todos os níveis.</p> <p>Varreduras de portas são proibidas e todos os casos relatados são investigados pelo nosso provedor de infra-estrutura. Quando são detectados varreduras de portas, elas são imediatamente bloqueadas.</p>
<p>Testes de Invasão e Avaliações de Vulnerabilidade</p>	<p>A terceirização de testes de nossos provedores de serviço de segurança são realizadas por empresas de consultoria de segurança independentes e respeitáveis. As conclusões de cada avaliação são revisadas com os avaliadores, o risco é classificado e são atribuídos as equipes responsáveis.</p>
<p>Incidentes de Eventos de Segurança</p>	<p>No caso de um incidente de segurança, nossos engenheiros são chamados para recolher extensos registros de sistemas críticos de host e analisá-los para responder ao incidente.</p> <p>O recolhimento e análise de informação de log é fundamental para a investigação e solução de problemas. Nosso fornecedor de serviços nos permite analisar três principais tipos: Sistema, Aplicativos e Logs de API.</p>

SEGURANÇA DE REDE

Contenção de DDos	A infra-estrutura de nossos prestadores de serviços fornecem técnicas de mitigação DDoS incluindo cookies TCP Syn e taxa de conexão limitadas além de manter múltiplas conexões e largura de banda interna com capacidade que excede a largura de banda de Internet fornecida ao cliente. Nós trabalhamos em estreita colaboração com os nossos fornecedores para responder rapidamente a eventos e permitir controles de mitigação DDoS avançados quando necessário.
Acesso Lógico	O acesso à rede de aplicações DoohNow é restrito, na qual é estreitamente controlada por nossa equipe de engenheiros. Os funcionários que acessam a rede das aplicações DoohNow são obrigados a usar múltiplos fatores de autenticação.

ENCRIPTAÇÃO

Encriptação em Trânsito	As comunicações entre você e servidores DoohNow são criptografados pelas melhores práticas da industria (HTTPS).
Encriptação em Repouso	A DoohNow suporta criptografia de dados de clientes em repouso.

DISPONIBILIDADE E CONTINUIDADE

Uptime (Tempo em atividade)	<p>A disponibilidade dos servidores DoohNow durante o último semestre foi de 100% (Excluso períodos de rápido interrompimento das aplicações durante atualizações emergenciais para melhoramento do produto)</p> <p>Os relatórios de disponibilidade não estão disponíveis em nosso site, mas podem ser fornecidos mediante solicitação.</p>
Redundância	Nosso serviço de clustering e redundância de rede elimina qualquer ponto de falha.

DISPONIBILIDADE E CONTINUIDADE

Recuperação de Desastres

A plataforma de nossos prestadores de serviços restaura automaticamente ao cliente aplicações e bases de dados no caso de uma interrupção. O provedor foi projetado para implantar dinamicamente aplicações dentro de sua nuvem, monitorar falhas e recuperar a falha de componentes incluindo aplicações e bancos de dados.

Segurança de Aplicação

DESENVOLVIMENTO SEGURO (SDLC)

QA (Garantia de Qualidade)

Nosso departamento de QA revisa e testa nossa base de código. Dedicados engenheiros de aplicação na equipe identificam, testam e fazem uma triagem de segurança e vulnerabilidades no código.

Ambientes Separados

Ambientes de teste são separados do nível de produção. O ambiente de alocação de dados do cliente não é usado para fins de desenvolvimento ou testes.

VULNERABILIDADE DE APLICAÇÕES

Análise Estática de Código

Nossos repositórios de código fonte são continuamente verificados por problemas de segurança através da nossa ferramenta de análise estática integrada.

Recursos de Segurança do Produto

DESENVOLVIMENTO SEGURO (SDLC)

Opções de Autenticação	A DoohNow suporta autenticação Single sign-on (SSO) e acesso via Token.
Segurança de Credenciais de Armazenamento	A DoohNow segue as melhores práticas de armazenamento de credenciais, protegido para não armazenar senhas em formato legível.
Autenticação e Seguranda de API	DoohNow API funciona somente via SSL, assim qualquer requisição é aceita somente através de usuário autenticado. Esta autorização é feito por Token liberado em painel de acesso exclusivo pelo cliente.

ELEMENTOS ADICIONAIS DE SEGURANÇA DO PRODUTO

Regras de Acesso e Privilégios	O acesso aos dados dentro da sua conta DoohNow é regido por direitos de acesso e podem ser configurados de acordo com a necessidade de seu uso. A plataforma DoohNow tem vários tipos de permissões e controle de níveis de organizacionais por função.
Segurança de Transmissão	Todas as comunicações com os servidores de provedores de serviços DoohNow são criptografados usando padrão da indústria HTTPS. Isso garante que todo o tráfego entre você e a DoohNow seja seguro durante o transporte.

Metodologias Adicionais de Segurança

CONSCIENTIZAÇÃO DE SEGURANÇA

Políticas	A DoohNow desenvolveu um conjunto abrangente de políticas de segurança cobrindo diversos tópicos importantes. Estas políticas são compartilhadas e colocadas à disposição de todos membros da equipe, assim como para profissionais terceirizados.
Treinamentos	Todos os novos funcionários recebam um treinamento de conscientização de segurança, e nossa equipe de engenheiros fornecem atualizações de sensibilização para a segurança através de comunicados internos de uso restrito a equipe, assim como em apresentações durante eventos internos.

HABILITAÇÃO DE FUNCIONÁRIOS

Pré Verificação	A DoohNow realiza verificações de antecedentes sobre todos os novos funcionários, em conformidade com as leis locais. A verificação de antecedentes inclui criminal, educacional e verificação de empregos anteriores. Isso é aplicado a qualquer cargo não importando seu papel na empresa.
Acordos de Confidencialidade	Todos os novos contratados são selecionados através de processo de contratação e obrigados a assinar acordos de confidencialidade.