Visão geral sobre segurança

Última atualização: Outubro de 2019

Índice

1 Nossa empresa e produtos 3

2 Segurança e governança de risco da HubSpot 3

3 Objetivos da nossa segurança e gestão de risco 3

4 Controles de segurança da HubSpot 4

4.1 Infraestrutura de produto da HubSpot 4

4.1.1 Segurança do data center 4

4.1.2 Segurança de rede e proteção de perímetro 4

4.1.3 Gerenciamento de configurações 5

4.1.4 Alerta e monitoramento 5

4.1.5 Acesso à infraestrutura 5

4.2 Proteção de aplicativos 6

4.2.1 Defesas de aplicativos web 6

4.2.2 Desenvolvimento e gerenciamento de lançamentos 6

4.2.3 Verificação de vulnerabilidades, testes de penetração e recompensa por falhas identificadas 7

4.3 Proteção de dados de cliente 8

4.3.1 Informações confidenciais nos produtos da HubSpot 8

4.3.2 Proteção de informações de cartão de crédito 8

4.3.3 Criptografia em trânsito e em repouso 8

4.3.4 Proteção do login do usuário 9

4.3.5 Autorização de usuário e API 9

4.3.6 Acesso de funcionários ao HubSpot 9

4.4 Privacidade 10

4.4.1 Política de retenção de dados 10

4.4.2 Gerenciamento do programa de privacidade 10

4.5 Continuidade dos negócios e recuperação de desastres 11

4.5.1 Confiabilidade e recuperação do sistema 11

4.5.2 Estratégia de backup 11

4.6 Segurança corporativa da HubSpot 12

4.6.1 Autenticação e autorização de funcionários 12

4.6.2 Gerenciamento de acesso 12

1 Visão geral de segurança e gerenciamento de risco da HubSpot

4.6.3 Verificações de antecedentes 13
4.6.4 Segurança corporativa da HubSpot 13
4.6.5 Gerenciamento de fornecedores 13
4.6.6 Conscientização e políticas de segurança 13
4.7 Gerenciamento de incidentes 14
5 Recursos de segurança de produtos 14
5.1 HubSpot Marketing Hub 14
5.2 HubSpot CRM 15
5.3 HubSpot Sales Hub 16
5.4 HubSpot Service Hub 16
6 Conformidade 16
7 Escopo e uso do documento 17

Visão geral sobre segurança na HubSpot

1 Nossa empresa e produtos

A HubSpot é a principal plataforma de marketing, vendas e serviços de inbound do mundo. Desde 2006, a HubSpot está em uma missão para tornar o mundo mais receptivo. Hoje, dezenas de milhares de clientes em mais de 90 países usam o software, os serviços e o suporte da HubSpot para transformar a maneira como atraem, envolvem e encantam seus clientes. O software de inbound marketing da HubSpot, classificado como o número 1 pela VentureBeat, GetApp, Capterra e G2Crowd, inclui publicação e monitoramento de mídias sociais, blogs, SEO, gerenciamento de conteúdo de sites e e-mail marketing, além de relatórios e análises, tudo em uma só plataforma. O HubSpot Sales Hub e o CRM, aplicativos de vendas premiados da HubSpot, permitem que equipes de vendas e atendimento tenham conversas mais eficazes com leads, prospects e clientes. O HubSpot Service Hub é a melhor solução para criar experiências agradáveis e sem atritos para os cliente.

Os produtos HubSpot são oferecidos como soluções de Software como Serviço (SaaS). Essas soluções estão disponíveis para os clientes por meio de aplicativos web criados especificamente para uso, interfaces de programação de aplicativos (APIs) e plug-ins de e-mail.

2 Segurança e governança de risco da HubSpot

O foco principal de segurança da HubSpot é proteger os dados de todos os nossos clientes e usuários. Esta é a razão pela qual a HubSpot tem investido em recursos e controles adequados para proteger e atender as necessidades dos nossos clientes. Esse investimento inclui a criação de equipes dedicadas de Segurança Corporativa e Segurança de Produto. Essas equipes são responsáveis pelo extenso programa de segurança da HubSpot e pelo processo de gestão. Nosso foco é definir novos controles e aperfeiçoar os já existentes, implementar e gerenciar a estrutura de segurança da HubSpot, além de fornecer uma estrutura de suporte para facilitar um gerenciamento de riscos eficaz. Nosso Diretor de Segurança, que se reporta ao Diretor de Operações, supervisiona a implementação de garantias de segurança na HubSpot e em seus produtos.

3 Objetivos da nossa segurança e gestão de risco

Desenvolvemos nossa estrutura de segurança usando as melhores práticas do ramo de Software como Serviço (SaaS). Nossos principais objetivos são:

- Confiança e proteção do cliente - fornecer consistentemente produtos e serviços de alta qualidade para nossos clientes, protegendo ao mesmo tempo sua privacidade e a confidencialidade de suas informações.
- Disponibilidade e continuidade do serviço - garantir a disponibilidade contínua do serviço e dos dados a todos os indivíduos autorizados e minimizar proativamente os riscos de segurança que ameacem sua continuidade.
- Integridade de informações e serviço – garantir que as informações dos clientes nunca sejam corrompidas ou alteradas inadequadamente.
- Conformidade com as normas - implementar processos e controles que estejam de acordo com as atuais diretrizes internacionais de regulamentação e com as melhores práticas do setor. Projetamos nosso programa de segurança com base nas melhores diretrizes para segurança na nuvem. Especificamente, utilizamos padrões como COBIT, a matriz de controles de nuvem da Cloud Security Alliance e alinhamos nossas práticas com o ISO 27001 e NIST SP 800-53.

4 CONTROLES DE SEGURANÇA DA HUBSPOT

Para garantir a proteção dos dados que nos foram confiados, implementamos uma variedade de controles de segurança, que permitem um alto nível de eficiência dos funcionários sem empecilhos artificiais e minimizando os riscos. As seções a seguir descrevem um subgrupo de controles. Para mais informações sobre o programa de segurança da HubSpot, acesse https://br.hubspot.com/security.

4.1 INFRAESTRUTURA DE PRODUTO DA HUBSPOT

4.1.1 SEGURANÇA DO DATA CENTER

A HubSpot terceiriza a hospedagem de sua infraestrutura de produtos nos principais provedores de infraestrutura em nuvem, em especial, na Amazon Web Services (AWS) e no Google Cloud Platform (GCP) para hospedagem. Essas soluções oferecem altos níveis de segurança física e de rede, assim como uma diversidade de fornecedores de hospedagem. Atualmente, as instâncias do servidor em nuvem do AWS da HubSpot residem em localidades dos EUA, enquanto as instâncias da nuvem do GCP residem na Alemanha. Ambos fornecedores possuem um programa de segurança auditado, incluindo conformidade com o SOC 2 e com o ISO 27001. A HubSpot não hospeda nenhum sistema de produto em seus escritórios corporativos.

Esses provedores de infraestrutura de alto padrão utilizam as mais avançadas infraestruturas de instalações, como energia, rede e segurança. O tempo de atividade das instalações é garantido entre 99,95% e 100% e as instalações garantem um mínimo de redundância N+1 para todos os serviços de energia, rede e tecnologia de climatização HVAC (aquecimento, ventilação e ar-condicionado). O acesso às instalações desses fornecedores é altamente restrito, tanto o acesso físico quanto o acesso eletrônico por meio de redes públicas (Internet) e privadas (intranet), a fim de eliminar quaisquer interrupções indesejadas por nossos clientes em nosso serviço.

As proteções de segurança física, ambiental e de infraestrutura, incluindo planos de continuidade e de recuperação, foram validadas de forma independente como parte de suas certificações SOC 2 Tipo II e ISO 27001. Os certificados estão disponíveis no site de conformidade do AWS e no site de segurança do Google Cloud Platform.

4.1.2 SEGURANÇA DE REDE E PROTEÇÃO DE PERÍMETRO

A infraestrutura de produto da HubSpot foi construída com proteções de segurança para Internet em grande escala. As proteções de segurança de rede foram projetadas especificamente para impedir o acesso não autorizado à rede e dentro da infraestrutura interna do produto. Esses controles de segurança incluem roteamento a nível corporativo e listas de controle de acesso à rede (firewall).

As listas de controle de acesso ao nível da rede foram implementadas nos grupos de segurança AWS Virtual Private Cloud (VPC) da Amazon ou nas regras de firewall do GCP do Google, que aplicam proteções no nível da porta e do endereço a cada uma das instâncias do servidor na infraestrutura. Essas tecnologias de firewall não permitem tráfego não intencional por padrão e todo o tráfego de rede é registrado e usado para informar nossos sistemas de monitoramento (leia mais sobre isso na Seção 4.1.4). Essas regras de acesso à rede permitem um controle minucioso do tráfego da rede de uma rede pública, bem como entre instâncias do servidor no interior da infraestrutura. Nela, as restrições de rede interna possibilitam uma abordagem em várias camadas para garantir que apenas os tipos apropriados de dispositivos possam se comunicar.

Alterações no modelo de segurança de rede são constantemente monitoradas e controladas por processos de controle de alterações padrão. Todas as regras e alterações existentes são avaliadas quanto ao risco de segurança e captadas adequadamente.

4.1.3 *Gerenciamento de configurações*

A automação impulsiona a possibilidade da HubSpot de se adequar às necessidades dos nossos clientes. A infraestrutura de produto é um ambiente altamente automatizado que potencializa de maneira flexível a qualidade e as habilidades da plataforma, conforme necessário. As instâncias do servidor são totalmente manipuláveis, o que significa que a configuração de qualquer servidor é rigorosamente controlada desde a criação até sua desabilitação.

Todas as configurações do servidor são incorporadas nas imagens e nos arquivos de configuração do Puppet. O gerenciamento de configuração no nível do servidor é tratado usando essas imagens e scripts de configuração quando o servidor é construído. As alterações na configuração e nas imagens padrão são gerenciadas por meio de um processo controlado de gerenciamento de mudanças. Cada tipo de instância inclui sua própria configuração reforçada, dependendo da implantação em questão.

O gerenciamento de fragmentos (patches) e o controle de configuração geralmente são feitos a partir da remoção de instâncias do servidor que não são mais compatíveis com a linha de base esperada e fornecendo uma instância de substituição em seu lugar. Um gerenciamento de configuração rigoroso e automatizado é incorporado ao nosso processamento de infraestrutura diário.

4.1.4 *Alerta e monitoramento*

A HubSpot não só automatiza totalmente seus procedimentos de construção, como também investe muitos recursos em tecnologias automatizadas de monitoramento, alerta e resposta para tratar continuamente de possíveis problemas. A infraestrutura de produto da HubSpot é equipada para alertar engenheiros e administradores quando algo fora do comum acontece. Especialmente quando se trata de taxas de erro, casos de abuso, ataques a aplicativos e outras anormalidades que acionam respostas automáticas e alertas às equipes mais adequadas a responder, investigar e corrigir. À medida que atividades inesperadas ou mal intencionadas ocorrem, os sistemas acionam as pessoas certas para garantir que o problema seja resolvido com o máximo de agilidade.

Muitos gatilhos automatizados também foram projetados no sistema para responder imediatamente a situações previsíveis. Bloqueio de tráfego, quarentena, encerramento de processo e funções semelhantes são ativadas em parâmetros predefinidos para garantir que a plataforma HubSpot possa se proteger contra uma ampla variedade de situações indesejáveis.

O poder por trás da capacidade da HubSpot de detectar e resolver anomalias está no nosso programa de monitoramento 24x7x365 e registro extensivo. Nossos sistemas capturam e armazenam registros que incluem todas as tecnologias que compõem nossos produtos. Na camada do aplicativo, todos os logins, visualizações de página, modificações e outros acessos aos portais da HubSpot também são registrados. No back-end de infraestrutura, registramos tentativas de autenticação, alterações de permissão horizontais e verticais, integridade da infraestrutura e solicitações realizadas, entre muitos outros comandos e transações. Registros e eventos são monitorados em tempo real e os eventos são escalados imediatamente a qualquer hora do dia para que desenvolvedores, profissionais de segurança e engenheiros possam tomar medidas adequadas.

4.1.5 *Acesso à infraestrutura*

Categorias inteiras de possíveis eventualidades relacionadas à segurança são evitadas com um modelo de controle de acesso rigoroso, consistente e bem projetado. Nesse sentido, o acesso aos sistemas da HubSpot é estritamente controlado. Os funcionários da HubSpot têm acesso a serviços corporativos,

portais de vendas e marketing da plataforma e infraestrutura de produtos com base em suas áreas de atuação, usando um modelo de controle de acesso baseado em suas funções. Mais informações sobre o modelo RBAC da HubSpot referente à toda a empresa estão disponíveis na seção 4.3.

O acesso a ferramentas de infraestrutura, servidores e serviços similares é restrito, apenas, às pessoas que realmente precisarem dele para realizar suas funções. Para conceder acesso de emergência e acesso a funções administrativas, o sistema da HubSpot usa um modelo JITA (Acesso Na Hora Certa) no qual os usuários podem solicitar acesso a funções privilegiadas por um período limitado.

Os usuários recebem os privilégios para fazer solicitações de JITA por unidade comercial e equipe. Quando o acesso de emergência não padrão é necessário, como o acesso "sudo" em um servidor Linux, o usuário faz uma solicitação JITA. A solicitação JITA é registrada e os registros são monitorados continuamente para solicitações fora do padrão. O acesso à função privilegiada é concedido e a pessoa pode continuar seu trabalho.

Além disso, é proibida a conexão direta de rede a dispositivos de infraestrutura de produto por meio de Secure Shell (SSH) ou protocolos semelhantes e é necessário que os engenheiros se autentiquem primeiro através de um host de bastiões (Bastion Host) ou “jump box” antes de acessar o controle de qualidade ou os ambientes de produção. A autenticação no nível do servidor usa chaves SSH exclusivas do usuário e autenticação de dois fatores baseada em token.

4.2 Proteção de aplicativos

4.2.1 Defesas de aplicativos web

Como parte do seu compromisso com a proteção de dados e sites de clientes, a HubSpot implementou um Firewall de Aplicativo Web (WAF) reconhecido pelo setor. O WAF identifica ameaças e protege automaticamente os produtos HubSpot ou sites de clientes hospedados na plataforma contra eventuais ataques. O WAF da HubSpot protege o acesso à plataforma HubSpot (por exemplo, os recursos que você pode acessar emhttps://app.hubspot.com ou ao se integrar com as APIs disponíveis em https://api.hubapi.com). Além disso, todo o conteúdo do cliente hospedado na plataforma também é protegido automaticamente. As regras usadas para detectar e bloquear o tráfego malicioso estão alinhadas às diretrizes de práticas recomendadas e documentadas pelo Projeto de Segurança de Aplicativos da Web Aberta (OWASP) em seu Top 10 e em recomendações semelhantes. Proteções contra Ataques Distribuídos de Negação de Serviço (DDoS) também são incorporadas, ajudando a garantir que os sites dos clientes e outros recursos dos produtos da HubSpot estejam sempre disponíveis.

O WAF foi configurado a partir de uma combinação de regras personalizadas do setor, capazes de ativar e desativar automaticamente os controles adequados para melhor proteger nossos clientes. Essas ferramentas monitoram ativamente o tráfego em tempo real na camada de aplicativos, com a possibilidade de alertar ou vetar comportamentos maliciosos com base no tipo e no nível da conduta apresentada.

4.2.2 Desenvolvimento e gerenciamento de lançamentos

Uma das maiores vantagens da HubSpot é um conjunto de recursos que evolui rapidamente, além do fato de que fornecemos produtos que são constantemente melhorados por meio de uma moderna abordagem de entrega contínua referente ao desenvolvimento de software. Milhares de vezes todos os dias, novos códigos são propostos, aprovados, combinados e implantados. Equipes especializadas de engenheiros com amplo conhecimento da plataforma HubSpot são responsáveis por analisar e garantir a qualidade dos códigos, à medida que são desenvolvidos. A aprovação é controlada pelos proprietários de repositório encarregados. Depois de aprovado, o código é enviado automaticamente ao ambiente de integração contínua da HubSpot, onde ele é compilado, embalado e testado. Se tudo for aprovado, o novo código será implantado automaticamente na camada do aplicativo.

Todas as implantações de código geram pastas com arquivos da fase de produção do código já instalado, para o caso de serem detectadas falhas após a sua implantação. A equipe de implantação administra as notificações sobre a integridade de seus aplicativos. Se ocorrer uma falha, a correção é imediatamente acionada.

Como parte do modelo de implantação contínua, usamos amplo gerenciamento de tráfego e bloqueio de software para controlar os recursos com base nas preferências do cliente (beta privado, beta público, lançamento completo). As principais alterações de recursos são comunicadas por meio de mensagens no aplicativo e/ou postagens de atualização de produto.

O código recém-desenvolvido é implantado primeiro no ambiente dedicado e reservado ao controle de qualidade da HubSpot para o último estágio de teste antes de ser encaminhado à produção. A segmentação no nível da rede impede o acesso não autorizado e indesejável entre o controle de qualidade e os ambientes de produção. Os dados do cliente nunca são usados pela HubSpot no ambiente de controle de qualidade, assim como em nenhum outro teste.

4.2.3 *Verificação de vulnerabilidades, testes de penetração e recompensa por falhas identificadas*

A equipe de Segurança da HubSpot gerencia uma abordagem composta por várias camadas para a verificação de vulnerabilidades, usando uma variedade de ferramentas reconhecidas pelo setor para garantir uma cobertura abrangente das nossas tecnologias aplicadas. Realizamos centenas de atividades de verificação de vulnerabilidades e testes de penetração contra nós mesmos o tempo todo. Além disso, realizamos a busca por vulnerabilidades continuamente em nossas redes internas, aplicativos e infraestrutura corporativa. As verificações de vulnerabilidade de rede e do aplicativo são realizadas pelo menos uma vez ao dia para garantir que fraquezas mais recentes sejam identificadas e corrigidas. A análise de código estático revisa automaticamente o código mais atual para detectar possíveis falhas de segurança no início do ciclo de vida do desenvolvimento.

A verificação contínua da execução, as listas adaptáveis de inclusão de verificação e a atualização contínua das assinaturas de vulnerabilidade ajudam a HubSpot a ficar à frente de muitas ameaças à sua segurança. Para obter uma segunda opinião sobre nossa capacidade de identificar e responder a riscos de segurança, contratamos empresas terceiras reconhecidas pelo setor para realizar quatro testes anuais de penetração. O objetivo desses programas é identificar iterativamente falhas que apresentam riscos à segurança e resolver quaisquer problemas com agilidade. Os testes de penetração são

realizados nas camadas de aplicativos e de rede das tecnologias aplicadas na HubSpot. Para isso os testadores de penetração recebem acesso interno ao produto HubSpot e/ou às redes corporativas para potencializar as espécies de possíveis vetores que devem ser avaliados.

Além da varredura interna de vulnerabilidades e do teste independente de penetração, a HubSpot gerencia um programa de recompensa por falhas identificadas. Pesquisadores de segurança independentes são convidados a participar na identificação de falhas de segurança nos produtos da HubSpot e são recompensados por suas contribuições. Os membros da comunidade de segurança e os clientes da HubSpot são convidados a realizar testes de segurança em portais de teste. Informações sobre o programa de recompensas da HubSpot estão disponíveis em https://bugcrowd.com/hubspot.

4.3 Proteção de dados de cliente

4.3.1 Informações confidenciais nos produtos da HubSpot

Os produtos HubSpot são uma experiência integrada de marketing, vendas e atendimento ao cliente. As informações reunidas em nossos produtos são coletadas por meio da interação com o cliente ou lead, diretórios públicos e fontes de terceiros respeitáveis. As ferramentas da HubSpot permitem que os clientes definam o tipo de informação a ser coletada e armazenada em seu nome. De acordo com os Termos de Serviço e a Política de Utilização Responsável da HubSpot, nossos clientes podem se certificar de que serão coletadas apenas as informações apropriadas para auxiliar seus processos de marketing, vendas e atendimento. Os produtos HubSpot não são usados para reunir ou coletar dados confidenciais, como números de cartão de crédito ou débito, informações pessoais de contas financeiras, CPF, números de passaporte, dados da carteira de motorista ou outros documentos de identificação semelhantes ou até mesmo informações referentes a emprego, finanças ou estado de saúde.

4.3.2 Proteção de informações de cartão de crédito

Muitos clientes da HubSpot pagam pelo serviço com cartão de crédito. Porém, a HubSpot não armazena, processa ou coleta informações de cartão de crédito submetidas pelos clientes. Utilizamos fornecedores de pagamento confiáveis e de conformidade PCI para garantir que as informações de cartão de crédito dos clientes sejam processadas com segurança e de acordo com as devidas regulamentações e os padrões do setor.

4.3.3 Criptografia em trânsito e em repouso

Todas as interações confidenciais com os produtos HubSpot (por exemplo, chamadas de API, login, sessões autenticadas no portal do cliente, etc.) são criptografadas em trânsito com chaves TLS 1.0, 1.1, 1.2 ou 1.3 e 2.048 bits ou superior. O TLS (Transport Layer Security) também está disponível por padrão para clientes que hospedam seus sites na plataforma HubSpot. Consulte o nosso guia de configuração de site para obter mais informações sobre como configurar o TLS. Os clientes que desejam limitar os protocolos de criptografia usados nas conexões HTTPS podem iniciar o processo entrando em contato com o Suporte ao Cliente ou com o Gerente de Sucesso do Cliente.

A HubSpot utiliza várias tecnologias para garantir que os dados armazenados sejam criptografados em repouso. Os discos rígidos físicos e virtualizados usados pelas instâncias do servidor do produto HubSpot, bem como as soluções de armazenamento de longo prazo, como o AWS S3, usam criptografia AES-256. Além disso, certos bancos de dados ou informações de campo são criptografados em repouso,

com base na sensibilidade das informações. Por exemplo, as senhas dos usuários são protegidas e certos recursos de e-mail funcionam fornecendo um nível adicional de criptografia em repouso e em trânsito.

As chaves de criptografia para criptografia em trânsito e em repouso são gerenciadas com segurança pela plataforma HubSpot. As chaves privadas TLS para criptografia em trânsito são gerenciadas através do nosso parceiro de entrega de conteúdo. As chaves de criptografia em nível de volume e campo para criptografia em repouso são armazenadas em um Sistema de Gerenciamento de Chaves (KMS) reforçado. As teclas são alternadas e a frequência varia de acordo com o tipo de tecla, a sensibilidade da tecla e os dados que ela protege. Em geral, os certificados TLS expiram a cada dois anos.

4.3.4 Proteção do login do usuário

Os produtos da HubSpot permitem que os usuários façam login em suas contas HubSpot usando o login interno da HubSpot, a opção "Entre com sua conta Google" ou a Autenticação Única (SSO). O login interno aplica uma política de senha uniforme, que requer um mínimo de 8 caracteres e uma combinação de letras maiúsculas e minúsculas, caracteres especiais, espaço em branco e números. As pessoas que usam o login interno da HubSpot não podem alterar a política de senha padrão. Os clientes que usam um provedor de autenticação única (SSO) podem configurar o login baseado em SSO para seus usuários. As instruções para configurar o SSO estão disponíveis no blog HubSpot Academy. Os usuários de autenticação única e login do Google podem configurar uma política de senha no provedor de SSO ou nas contas do Google.

Os clientes que usam o login da HubSpot também são incentivados a configurar a autenticação de dois fatores para suas contas. Além disso, os administradores do portal podem configurar seus portais HubSpot para garantir que todos os usuários fiquem com a autenticação de dois fatores ativa.

4.3.5 Autorização de usuário e API

Os clientes podem atribuir permissões granulares para suas contas e limitar o acesso aos seus recursos de dados. Para obter mais informações sobre funções de usuário, consulte o Guia de Funções e Permissões do Usuário HubSpot.

O acesso à interface de programação de aplicativos (API) é ativado por meio da chave da API ou da autorização do protocolo Oauth (versão 2). Os clientes têm a possibilidade de gerar chaves de API para seus portais. Estas chaves devem ser usadas para reproduzir integrações personalizadas rapidamente. A implementação Oauth (protocolo de autorização) da HubSpot é um direcionamento mais seguro para autenticar e autorizar solicitações de API. Além disso, o Oauth é necessário para todas as integrações em destaque. A autorização para solicitações ativadas por Oauth é estabelecida por escopos definidos. Para mais informações sobre o uso da API, consulte o portal de Desenvolvedores em HubSpot.com.

4.3.6 Acesso de funcionários ao HubSpot

A HubSpot controla o acesso individual aos dados em seu ambiente corporativo e de produção. Um seleto grupo de funcionários da HubSpot recebe acesso aos dados de produção com base em sua função na empresa, por meio de controles de acesso baseados em função (RBAC) ou, conforme necessário, por meio do JITA (Acesso na Hora Certa).

Os engenheiros e membros das equipes de Operações podem ter acesso a vários sistemas de produção, como uma função do seu cargo. As necessidades comuns de acesso incluem alertas de resposta e solução de problemas, além da análise de informações para decisões de investimento em produtos e suporte ao produto. O acesso à infraestrutura do produto é limitado pelo controle de acesso à rede e autenticação e autorização do usuário. O acesso às funções de rede é estritamente limitado a indivíduos cujos trabalhos exigem esse acesso, que está sujeito à revisões contínuas.

O Suporte ao Cliente, Atendimento e outras equipes de engajamento do cliente com necessidades especiais podem solicitar o JITA para acessar os portais do cliente por tempo limitado. As solicitações de acesso são restritas às responsabilidades de trabalho associadas ao suporte e manutenção de nossos clientes. As solicitações são limitadas ao acesso JITA ao portal de um cliente específico por um período máximo de 24 horas. Todas as solicitações de acesso, logins, consultas, visualizações de página e informações semelhantes são registradas.

Todo o acesso dos funcionários aos recursos corporativos e do produto está sujeito à revisão automática diária e, pelo menos, uma revalidação manual de certificação semestral para garantir que a autorização concedida seja apropriada para a função e para as necessidades do trabalho do funcionário.

4.4 PRIVACIDADE

A privacidade dos dados de nossos clientes é uma das principais considerações da HubSpot. Conforme descrito em nossa Política de Privacidade, nunca vendemos seus dados pessoais a terceiros. As proteções descritas neste documento e outras proteções implementadas foram projetadas para garantir que seus dados permaneçam privados e íntegros. Os produtos da HubSpot são projetados e construídos com as necessidades do cliente e considerações de privacidade em primeiro lugar. Nosso programa de privacidade incorpora as melhores práticas, as necessidades dos clientes e de seus contatos, bem como os requisitos regulamentares.

Nesse sentido, a HubSpot é certificada sob as estruturas de proteção de privacidade UE-EUA e Suíça-EUA. Mais informações sobre nossa certificação estão disponíveis no site do Escudo de Privacidade. A HubSpot também alcançou e mantém a certificação de Privacidade Corporativa da TRUSTe.

4.4.1 POLÍTICA DE RETENÇÃO DE DADOS

Os dados do cliente ficarão retidos enquanto você permanecer um cliente ativo. A plataforma HubSpot fornece aos clientes ativos as ferramentas para apagar seus dados, conforme considerem necessário. Os dados de ex-clientes são removidos dos bancos de dados ativos, mediante solicitação por escrito do cliente ou após um período estabelecido posteriormente ao término de todos os contratos do cliente. Os dados dos clientes Freemium são eliminados quando o portal não é mais usado ativamente e os dados de antigos clientes pagantes são eliminados 90 dias após o término de todos os relacionamentos com os clientes. As informações armazenadas em cópias, capturas instantâneas e backups não são eliminadas ativamente, mas envelhecem naturalmente à medida que o ciclo de vida dos dados ocorre. A HubSpot retém certos dados, como registros e metadados relacionados, a fim de atender às necessidades de segurança, conformidade ou regulamentação.

4.4.2 GERENCIAMENTO DO PROGRAMA DE PRIVACIDADE

O Jurídico, Segurança e várias outras equipes da HubSpot colaboram para garantir um programa de privacidade eficaz e implementado de forma consistente. As informações sobre o nosso compromisso com a privacidade dos seus dados estão disponíveis com mais detalhes em nossa Política de Privacidade e Acordo de Processamento de Dados.

4.5 CONTINUIDADE DOS NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

A HubSpot mantém planos de continuidade de negócios e recuperação de desastres, com foco tanto na prevenção de interrupções por meio de redundâncias de telecomunicações, sistemas e operações comerciais, quanto em estratégias de recuperação rápida no caso de um problema de disponibilidade ou desempenho. Sempre que ocorrem situações que impactam o cliente, o objetivo da HubSpot é isolar e resolver o problema de maneira rápida e transparente. Os problemas identificados são publicados no site de status da HubSpot e atualizados posteriormente até que o problema seja resolvido.

4.5.1 CONFIABILIDADE E RECUPERAÇÃO DO SISTEMA

O teste de continuidade de negócios faz parte do processamento normal da HubSpot. Os processos de recuperação da plataforma são validados continuamente por meio de processos normais de manutenção e suporte. Seguimos os princípios de implantação contínua e criamos ou destruímos muitas instâncias de servidor diariamente como parte de nossa manutenção e crescimento regulares. Também usamos esses procedimentos para se recuperar de instâncias comprometidas e outras falhas, que nos permite praticar nosso processo de recuperação todos os dias.

A HubSpot conta principalmente com redundância de infraestrutura, replicação em tempo real e backups. Todos os serviços do produto HubSpot são criados com redundância total. A infraestrutura do servidor é estrategicamente distribuída em várias zonas de disponibilidade distintas e em redes de nuvem virtual privada, dentro de nossos provedores de infraestrutura. Além disso, todos os componentes web, aplicativos e banco de dados são implantados com um mínimo de n+1 instâncias ou reservatórios de servidor de suporte.

4.5.2 ESTRATÉGIA DE BACKUP

A HubSpot garante que dados sejam copiados e protegidos em vários armazenamentos de dados duráveis. O período de retenção dos backups depende da natureza dos dados. Os dados também são copiados entre zonas de disponibilidade e localizações de infraestrutura para proporcionar tolerância a falhas, bem como escalabilidade e recuperação responsiva, quando necessário.

- Dados de cliente (produção) são armazenados em backup utilizando diversas cópias on-line dos dados para promover proteção imediata. Todos os bancos de dados de produção têm pelo menos uma versão primária (mestre) e uma cópia (escravo) dos dados ativos em qualquer ponto do tempo. Backups de sete dias de dados são mantidos para qualquer banco de dados como forma de garantir que a restauração possa ocorrer com facilidade. Capturas de tela são feitas e armazenadas em um serviço secundário pelo menos uma vez por dia e, quando possível, a cópia em tempo real é usada. Todos os conjuntos de dados de produção são armazenados em uma instalação de hospedagem de arquivos distribuída, como o S3 da Amazon.

- Por utilizarmos os serviços de nuvem privada para hospedagem, backup e recuperação, a HubSpot não implementa infraestrutura física ou mídia de armazenamento física em seus produtos. A HubSpot também não produz ou usa outros tipos de mídia física (por exemplo, papel, fita etc.) como parte da disponibilização dos nossos produtos aos clientes.
- Por padrão, todos os backups são protegidos com restrições de controle de acesso nas redes de infraestrutura de produto da HubSpot, listas de controle de acesso nos sistemas de arquivos que armazenam os arquivos de backup e/ou com proteções de segurança de banco de dados.
- Para clientes que, adicionalmente, desejarem fazer backup dos seus dados, a plataforma HubSpot oferece diversas formas de garantir que você tenha o que precisa. Muitos dos recursos dentro do portal da HubSpot possuem a opção de exportar e a biblioteca de APIs públicas da HubSpot pode ser usada para sincronizar seus dados com outros sistemas. Para detalhes sobre backup dos seus dados, consulte nosso artigo da base de conhecimento sobre como exportar o seu conteúdo.

4.6 SEGURANÇA CORPORATIVA DA HUBSPOT

4.6.1 AUTENTICAÇÃO E AUTORIZAÇÃO DE FUNCIONÁRIOS

A HubSpot impõe uma política de senha corporativa padrão do setor. Essa política exige a alteração das senhas pelo menos a cada 90 dias. Ela também requer um tamanho de senha mínimo de 8 caracteres e tem requisitos de complexidade, incluindo caracteres especiais, caracteres em letra maiúscula e minúscula e números. A HubSpot proíbe o compartilhamento de conta e senha entre vários funcionários.

Geralmente, os funcionários autenticam-se à infraestrutura de produto da HubSpot usando chaves SSH. Nos casos em que senhas são permitidas, a política exige senhas de 12 caracteres. Além disso, muitos dos recursos usados na criação dos produtos da HubSpot usam autenticação multifator ou são protegidos por soluções de login único que impõem autenticação multifator.

4.6.2 GERENCIAMENTO DE ACESSO

A HubSpot organizou e automatizou procedimentos de autenticação e autorização para o acesso de funcionários aos sistemas, incluindo as plataformas de marketing e vendas. Todo acesso é registrado. Com frequência, o acesso é concedido conforme um modelo de controle de acesso baseado em função. O acesso na hora certa é integrado em procedimentos automatizados em torno de um conjunto de mecanismos de autorização rigorosos.

Desenvolvemos um conjunto de sistemas de suporte completo para simplificar e automatizar nossas atividades de gerenciamento e conformidade com segurança. Além de muitas outras funções, o sistema verifica nossa infraestrutura de produto e corporativa várias vezes ao dia para garantir que as concessões de permissão sejam adequadas; gerenciar eventos de funcionário; revogar contas e acesso quando necessário; compilar registros de solicitações de acesso; e capturar comprovação de conformidade para cada um dos nossos controles de segurança de tecnologia. Esses sistemas internos verificam a infraestrutura para validar que ela siga as configurações aprovadas a cada 24 horas.

4.6.3 *Verificações de antecedentes*

Todos os funcionários da HubSpot passam por uma verificação completa de antecedentes realizada por terceiros antes de receberem oferta formal de emprego. Especificamente, são realizadas verificações de emprego, formação e antecedentes criminais para todos os funcionários em potencial. A verificação de referências é conduzida a critério do gerente de contratação. Todos os funcionários devem cumprir Acordos de Não Divulgação e Política de Utilização Responsável como parte do acesso às redes corporativa e de produção.

4.6.4 *Segurança corporativa da HubSpot*

Os escritórios da HubSpot são protegidos de diversas formas. Guardas de segurança são contratados em cada endereço global da HubSpot para ajudar a criar um ambiente seguro para os funcionários. O acesso às portas é controlado usando tokens RFID vinculados aos indivíduos, que são desativados automaticamente caso sejam perdidos ou quando não forem mais necessários (por exemplo, demissão de funcionários, uso pouco frequente etc.). Vigilância por vídeo e muitas outras medidas de proteção são implementadas nos escritórios da HubSpot.

4.6.5 *Gerenciamento de fornecedores*

Usamos um pequeno número de prestadores de serviços terceirizados que aumentam a capacidade dos produtos da HubSpot em atender às suas necessidades de marketing e vendas. Mantemos um programa de gestão de fornecedores para garantir que os controles apropriados de segurança e privacidade estejam em vigor. O programa inclui inventariação, rastreamento e revisão de programas de segurança dos fornecedores que oferecem suporte à HubSpot.

Proteções apropriadas são avaliadas com relação ao serviço sendo prestado e o tipo dos dados trocados. A conformidade contínua com as proteções esperadas é gerenciada como parte do nosso relacionamento contratual com eles. Nossa equipe de segurança, Conselho Geral e a unidade comercial que detém cada contrato coordena considerações exclusivas para nossos fornecedores como parte do gerenciamento de contratos.

4.6.6 *Conscientização e políticas de segurança*

Para que todos os nossos engenheiros, atendentes de suporte e demais funcionários estejam em sintonia em relação à proteção dos seus dados, a HubSpot desenvolveu e mantém uma Política de Segurança da Informação por Escrito. A política aborda requisitos de tratamento de dados, considerações sobre privacidade e respostas a violações, entre vários outros assuntos.

Com essa política e a variedade de proteções e padrões em vigor, também garantimos que os HubSpotters estejam bem treinados para suas funções. Vários níveis de treinamento em segurança são oferecidos aos funcionários da HubSpot com base em suas funções e acesso resultante. O treinamento em conscientização de segurança, em geral, é oferecido a todos os novos funcionários e aborda os requisitos de segurança da HubSpot. Depois do treinamento inicial, módulos de treinamento diferentes são disponibilizados com base na função de cada funcionário. Treinamento específico para desenvolvedores é oferecido e adaptado pelas equipes de engenharia da HubSpot. O treinamento de conscientização de segurança específico da função para Atendimento e Suporte, Vendas e muitas outras

funções é adaptado às considerações exclusivas da função. Um treinamento recorrente é fornecido regularmente com atualizações, avisos e publicações na wiki interna.

4.7 Gerenciamento de incidentes

A HubSpot fornece cobertura 24x7x365 para responder rapidamente a todos os eventos de segurança e privacidade. O programa de resposta rápida a incidentes da HubSpot é responsivo e pode ser reproduzido. Tipos de incidente pré-definidos, baseados em tendências históricas, são criados para facilitar o rastreamento imediato de incidentes, a atribuição consistente de tarefas, o encaminhamento e a comunicação. Muitos processos automatizados alimentam o processo de resposta a incidentes, incluindo alertas de atividade mal-intencionada ou anomalia, alertas de fornecedor, solicitações de cliente, eventos de privacidade e muitos outros.

Ao responder a qualquer incidente, primeiro determinamos a exposição das informações e a origem do problema de segurança, se possível. Comunicamos o cliente (e quaisquer outros clientes afetados) por e-mail ou telefone (se e-mail não for suficiente). Fornecemos atualizações periódicas, conforme necessário, para garantir a solução apropriada do incidente.

Nosso Diretor de Segurança revisa todos os incidentes relacionados à segurança, suspeitos ou comprovados, e nós coordenamos esforços com os clientes afetados usando os meios mais apropriados, dependendo da natureza do incidente.

5 Recursos de segurança de produtos

O programa de segurança da HubSpot foi criado para proteger todos os produtos da HubSpot. Cada produto se utiliza das melhores práticas de segurança recomendadas para o desenvolvimento de aplicativo, bem como segurança de infraestrutura e configurações de alta disponibilidade.

Não importa se nossos produtos são gratuitos ou pagos, com poucos ou muitos recursos, a HubSpot se esforça para manter a privacidade dos dados que você confia a nós. Os dados que você armazena na HubSpot são seus. Colocamos nosso programa de segurança em prática para protegê-los e os usamos somente para fornecer o serviço da HubSpot para você. Nós nunca compartilhamos os seus dados com clientes e nunca os vendemos.

5.1 HubSpot Marketing Hub

Sobre: O produto de marketing da HubSpot é nossa solução de automação de marketing líder do setor. Ele fornece ferramentas eficazes e fáceis de usar para gerenciar sua estratégia de inbound marketing.

Hospedagem: A infraestrutura principal do Sistema de Gerenciamento de Conteúdo (CMS) está hospedada na Amazon Web Services e no Google Cloud Platform. A estratégia de hospedagem da HubSpot oferece recursos adicionais de redundância, flexibilidade de arquitetura e capacidade de resposta de infraestrutura. Nossos processos de implantação fornecem recursos de segurança de rede, segurança de servidor e disponibilidade, descritos acima.

Firewall de aplicativos web: Os sites de clientes hospedados nos produtos da HubSpot utilizam as proteções do nosso firewall de aplicativos web (WAF) de alto nível. Por padrão, o seu site, blogs, landing pages e outra peças de presença on-line hospedados pela HubSpot são protegidos contra ataques de negação de serviço distribuído (DDoS) e demais ataques a aplicativos web. Quando ocorrem eventos de segurança, as equipes de operações e técnica da HubSpot realizam ações imediatas para garantir que seus sites continuem protegidos 24x7x365.

Segurança da Camada de Transporte (TLS): Os clientes de marketing da HubSpot têm a capacidade de ativar e configurar serviços de TLS para seus sites, landing pages e engajamentos relacionados aos visitantes. Por padrão, os certificados TLS usam nomes alternativos de assunto e são gerenciados pelo nosso provedor de distribuição de conteúdo, a Akamai. Para obter mais informações sobre como começar, confira este artigo da Academy.

Opções de criptografia: Por padrão, os sites de clientes que usam HTTPS são configurados para permitir TLS 1.0, 1.1 e 1.3. É possível remover o suporte a um ou mais desses protocolos. Os clientes também podem escolher ativar o Segurança Estrita de Transporte HTTP (HSTS) para seu domínio hospedado pela HubSpot. Para fazer essas alterações, entre em contato com o Suporte da HubSpot ou com seu Gerente de Sucesso do Cliente.

5.2 HubSpot CRM

Sobre: O HubSpot CRM é um dos muitos produtos que sua equipe de vendas vai adorar. Os profissionais de vendas podem começar usando o CRM sem custos e sem complicações. Para começar a usar, basta conferir a página de produto do HubSpot CRM.

Seguro por padrão: O CRM tira vantagem das mesmas medidas de segurança sofisticadas que ajudam a proteger os outros produtos da HubSpot. Usamos os processos de desenvolvimento de software seguros e avançados, o gerenciamento de infraestrutura e as metodologias de alerta que foram aperfeiçoados durante os anos de desenvolvimento de produto.

Integrações de e-mail e caixa de entrada conectada: Como usuário do CRM, você pode conectar sua conta do Gmail, Office365 ou conta de e-mail habilitada para IMAP. As integrações do Gmail e Office365 são autorizadas e protegidas pelos recursos de integração nativos dessas plataformas. A integração com IMAP permite que sua conta de e-mail conectada sincronize as mensagens de outros serviços de e-mail com seu CRM. Quando um usuário configura uma integração com IMAP, os produtos da HubSpot agem como um cliente de IMAP. Os serviços que aceitam integrações com IMAP têm muitas proteções incluídas: os dados são criptografados em trânsito de uma extremidade à outra; os dados são criptografados em repouso no nível do campo e no nível do banco de dados; e controles de acesso garantem somente acesso autorizado aos dados.

Privacidade: Não importa se os nossos produtos são gratuitos ou pagos, com muitos ou poucos recursos, a HubSpot sempre mantém a privacidade dos dados que você confia a nós. Os dados que você armazena na HubSpot são seus. Nós os usamos somente para fornecer o serviço da HubSpot para você.

Hospedagem: A infraestrutura do CRM está hospedada na Amazon Web Services, aproveitando a redundância de infraestrutura e a flexibilidade que existe em toda a infraestrutura da HubSpot. Nossa

estratégia de hospedagem também ajuda a garantir disponibilidade e segurança de rede e infraestrutura de alto nível.

Controle de acesso: O HubSpot CRM fornece funções intuitivas e fáceis de gerenciar que dão o acesso certo aos membros certos da equipe comercial. Consulte nosso artigo da base de conhecimento para obter mais informações sobre funções de usuário.

5.3 HubSpot Sales Hub

Sobre: Os produtos do HubSpot Sales também incluem um conjunto de ferramentas de vendas premiadas que ajuda os profissionais a se envolver melhor com seus leads e melhorar a conversa.

Hospedagem: A principal infraestrutura de back-end do Sales está hospedada na Amazon Web Services. Nossa estratégia de hospedagem aproveita a redundância de infraestrutura e a flexibilidade que existe em toda a infraestrutura da HubSpot.

Armazenamento de dados: O HubSpot Sales armazena metadados de mensagem de e-mail para fornecer serviços de rastreamento de e-mail, inserção de link e conexões. Os dados são gravados em armazenamentos protegidos na infraestrutura da HubSpot e o acesso aos dados é rigorosamente controlado. O acesso aos armazenamentos de dados é atribuído a um pequeno grupo de funcionários da HubSpot baseado em suas funções e o acesso é limitado aos indivíduos que precisam dele para responder a perguntas de suporte do cliente e solicitações relacionadas.

Atualização sem interrupções: As ferramentas de vendas foram desenvolvidas para ajudar a aumentar a sua produtividade. Uma medida que tomamos para melhorar sua experiência é a atualização de plugin automática. Em vez de ser interrompido com notificações recorrentes para atualizar o software, o plugin cuida de seu processo de atualização sem atrapalhar você.

5.4 HubSpot Service Hub

Sobre: O HubSpot Service Hub inclui todos os recursos necessários para encantar seus clientes. O Service Hub inclui a possibilidade de monitorar conversas de forma fluida e empoderar visitantes com uma sofisticada tecnologia bot.

Hospedagem: A principal infraestrutura de back-end do Service Hub está hospedada na Amazon Web Services. Nossa estratégia de hospedagem aproveita a redundância de infraestrutura e a flexibilidade que existe em toda a infraestrutura da HubSpot.

Atualização sem interrupções: As ferramentas do Service Hub foram projetadas para ajudar a manter clientes engajados no serviço oferecido. As ferramentas do Service Hub são atualizadas automaticamente e com regularidade para garantir que você tenha os recursos certos para as suas necessidades de atendimento ao cliente.

6 Conformidade

A HubSpot tem certificação TRUSTe para Privacidade Corporativa e mantém conformidade com o Escudo de Privacidade UE-EUA. A plataforma da HubSpot também contém recursos que permitem que

nossos clientes atinjam e mantenham facilmente seus requisitos de conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR). Mais informações sobre conformidade com a privacidade e os produtos HubSpot estão disponíveis em nosso conteúdo de conformidade com GPDR e no HubSpot DPA.

Os produtos da HubSpot estão hospedados nos provedores de infraestrutura de nuvem de classe mundial Amazon Web Services e Google Cloud Platform. Os provedores de infraestrutura da HubSpot têm certificação SOC 2 Tipo II e ISO 27001 e mantêm instalações protegidas contra invasão eletrônica e física.

7 ESCOPO E USO DO DOCUMENTO

A HubSpot valoriza a transparência nas formas como oferecemos soluções aos nossos clientes. Este documento foi criado com essa transparência em mente. Estamos sempre aprimorando as proteções que implementamos e, nesse mesmo sentido, as informações e dados neste documento (incluindo quaisquer comunicações relacionadas) não são destinados a criar uma obrigação vinculativa ou contratual entre a HubSpot e quaisquer partes, nem corrigir, alterar ou revisar quaisquer acordos existentes entre as partes.