Última atualização: outubro de 2021

Visão geral de segurança

HubSpot

Índice

Visão geral da segurança da HubSpot

Nossa empresa e nossos produtos

A HubSpot é a principal plataforma de marketing inbound, vendas, atendimento, gestão de conteúdo e operações do mundo. Desde 2006, a HubSpot está em uma missão para tornar o mundo mais receptivo. Hoje, mais de 100.000 clientes em mais de 120 países usam os serviços, software e suporte da HubSpot para transformar a maneira de atrair, engajar e encantar clientes.

Os produtos da HubSpot são oferecidos como soluções de software como serviço (SaaS). Essas soluções estão disponíveis para os clientes por meio de aplicativos Web criados para usos específicos, interfaces de programação de aplicativos (APIs) e plug-ins de e-mail.

Segurança e governança de riscos da HubSpot

O foco principal de segurança da HubSpot é proteger os dados dos nossos clientes. 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 oferecer uma estrutura de suporte para dar mais eficácia à gestão de riscos. Nosso diretor de Segurança da Informação supervisiona a implementação de garantias de segurança na HubSpot e em nossos produtos.

Nossos objetivos de segurança e gestão de riscos

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

- Confiança e proteção do cliente: oferecer sempre produtos e serviços de alta qualidade para nossos clientes, protegendo a 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 do serviço: garantir que as informações dos clientes nunca sejam corrompidas ou alteradas inadequadamente.
- Conformidade com as normas: projetamos nosso programa de segurança corporativa com base nas melhores práticas de segurança cibernética do setor, incluindo os Controles Críticos de Segurança do Center for Internet Security (CIS). Nossos controles que regem a disponibilidade, a confidencialidade e a segurança dos dados dos clientes também foram desenvolvidos para atender as normas de SOC 2 dos Princípios de Serviços de Confiança estabelecidos pelo American Institute of Certified Public Accountants (AICPA).

Controles de segurança da HubSpot

Para proteger os dados que são confiados a nós, adotamos técnicas avançadas de defesa para implementar camadas de controles de segurança em toda a organização. As seções a seguir esmiúçam algumas das dúvidas mais comuns em relação aos nossos controles.

Infraestrutura de produto da HubSpot

Segurança de infraestrutura de nuvem

A HubSpot não hospeda nenhum sistema de produto em seus escritórios corporativos. A HubSpot terceiriza a hospedagem de sua infraestrutura de produtos nos principais provedores de infraestrutura em nuvem, Amazon Web Services (AWS). Nossos provedores de hospedagem garantem uma disponibilidade de serviço com tempo de atividade entre 99,95% e 100%, além de redundância para todos os serviços de energia, rede e tecnologia de climatização HVAC (aquecimento, ventilação e ar-condicionado).

A infraestrutura de produto da HubSpot na AWS fica no leste dos EUA. Os dois provedores mantêm um programa de segurança auditado, bem como proteções de segurança físicas, ambientais e de infraestrutura. Os planos de continuidade de negócios e de recuperação de desastres foram validados de forma independente como parte de suas certificações SOC 2 Tipo 2 e ISO 27001.

A documentação de conformidade está disponível ao público na página de Conformidade da AWS.

A HubSpot também oferece um artigo da Central de Conhecimento com perguntas frequentes sobre a infraestrutura de nuvem disponível aqui.

Segurança de rede e proteção de perímetro

A infraestrutura de produto da HubSpot aplica múltiplas camadas de filtragem e inspeção nas conexões feitas em toda a plataforma.

Implementamos listas de controle de acesso no nível da rede para evitar acessos não autorizados à nossa infraestrutura interna. Nossos firewalls são configurados para recusar

conexões de rede que não sejam explicitamente autorizadas por padrão, e monitoramos o tráfego para detectar atividades suspeitas.

Mudanças na segurança da nossa rede são ativamente monitoradas e controladas por processos de controle de alterações padrão. Revisamos os conjuntos de regras de firewall anualmente para garantir que apenas as conexões necessárias sejam configuradas.

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 a capacidade e os recursos da plataforma, conforme o necessário. As instâncias de servidores são rigorosamente controladas do provisionamento ao desprovisionamento, garantindo a detecção e a reversão de desvios dos referenciais de configuração a uma cadência predefinida. Caso um servidor de produção desobedeça aos referenciais de configuração, a correção acontecerá em até 30 minutos.

Todas as configurações do servidor são incorporadas nas imagens e nos arquivos de configuração. 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 patches é feito por ferramentas automatizadas de gerenciamento de configurações ou a partir da remoção de instâncias do servidor que não são mais compatíveis com o referencial esperado e o provisionamento de uma instância substituta. Um gerenciamento de configuração rigoroso e automatizado é incorporado ao nosso processamento de infraestrutura diário.

Alerta e monitoramento

A HubSpot não só automatiza totalmente seus procedimentos de construção como também investe pesado em recursos automatizados 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 automatizados 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 imprevistos. Bloqueio de tráfego, quarentena, encerramento de processos e funções semelhantes são ativadas em parâmetros predefinidos para garantir que a plataforma HubSpot possa se proteger contra uma ampla variedade de situações indesejáveis.

Proteção de aplicativos

Defesas de aplicativos Web

Todo o conteúdo do cliente hospedado na plataforma é protegido por um firewall de aplicativos Web (WAF, na sigla em inglês). O WAF é configurado a partir de uma combinação de padrões do setor e regras personalizadas capazes de ativar e desativar automaticamente controles adequados para proteger melhor os nossos clientes. Essas ferramentas monitoram ativamente o tráfego em tempo real na camada de aplicativos, com a possibilidade de alertar ou vetar comportamentos mal-intencionados com base no tipo e no nível da conduta apresentada.

As regras usadas para detectar e bloquear o tráfego mal-intencionado estão alinhadas às melhores práticas documentadas pelo Projeto de Segurança de Aplicativos da Web Aberta (OWASP), especificamente no OWASP 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.

Desenvolvimento e gerenciamento de lançamentos

Uma das maiores vantagens da HubSpot é um conjunto de recursos que evolui rapidamente, além do fato de aprimorarmos constantemente os nossos produtos 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. Revisões de código, testes (quando for o caso) e aprovação de unificações são feitos antes da implantação. 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.

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.

Usamos gerenciamento amplo de tráfego e barreira de software para controlar recursos com base nas preferências do cliente (beta privado, beta público, lançamento completo). A HubSpot oferece atualizações fluidas e, por seguir o modelo SaaS, não há tempo de inatividade devido a lançamentos. As principais alterações de recursos são comunicadas por meio de mensagens no aplicativo e/ou posts 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 entre o controle de qualidade e os ambientes de produção.

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.

As verificações de vulnerabilidades são configuradas para identificar diariamente vulnerabilidades oportunas. A verificação contínua da execução, que usa listas adaptáveis

de inclusão de verificação, e a atualização contínua das assinaturas de detecção de vulnerabilidade ajudam a HubSpot a ficar à frente de muitas ameaças à sua segurança.

Nós também contratamos empresas independentes reconhecidas no mercado 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.

Além da verificação interna de vulnerabilidades e do teste independente de penetração, a HubSpot gerencia um programa de recompensa por falhas identificadas, em que pesquisadores externos de segurança são convidados a participar na identificação de falhas de segurança nos produtos da HubSpot. 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.

Proteção de dados dos clientes

Separação lógica entre locatários

A HubSpot oferece uma solução SaaS multilocatário altamente escalável. A interface de usuário e as APIs da HubSpot restringem o acesso somente a conteúdos autorizados. A HubSpot segmenta logicamente os dados usando IDs de portal e associa esse ID exclusiva a todos os dados e objetos específicos a um cliente. As informações são disponibilizadas pela interface de usuário ou por APIs a serem produzidas para um portal específico da HubSpot, sem o risco de acesso entre portais ou poluição de dados.

As regras de autorização são integradas à arquitetura de design e validadas continuamente. Além disso, registramos autenticação de aplicativos e alterações associadas, disponibilidade de aplicativos e visualizações de página de usuários.

Informações confidenciais

Os produtos da HubSpot são uma experiência integrada de marketing, vendas, atendimento ao cliente, gestão de conteúdo e operações. Os dados reunidos em nossos produtos são coletados 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 dado a ser coletado e armazenado em seu nome. De acordo com os Termos de Serviço e a Política de Utilização Responsável da HubSpot, nossos clientes são responsáveis por garantir que coletam apenas os dados adequados para auxiliar seus processos de marketing, vendas, atendimento ao cliente, gestão de conteúdo e operações. Os produtos da HubSpot não devem ser 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 habilitação ou outros dados financeiros ou de saúde.

Para mais informações sobre a classificação dos dados usados e aceitos pelo sistema da HubSpot, confira a tabela "Classificação de dados" em nosso Relatório SOC 2.

Criptografia em trânsito e em repouso

Todas as interações sigilosas com os produtos da HubSpot (por exemplo, chamadas de API, sessões autenticadas etc.) são criptografadas em trânsito com TLS 1.2 ou 1.3 e chaves de 2.048 bits ou melhores. O TLS (Transport Layer Security) também é padrão para clientes que hospedam seus sites na plataforma HubSpot.

Veja nosso guia de configuração de sites e nosso artigo da Central de Conhecimento sobre SSL e segurança de domínio para saber como configurar o TLS.

A HubSpot utiliza várias tecnologias para garantir que os dados armazenados sejam criptografados em repouso. Os dados da plataforma são armazenados usando criptografia AES-256. As senhas de usuários recebem hashes conforme as melhores práticas do setor e ficam criptografadas em repouso. Certos recursos de e-mail funcionam fornecendo um nível adicional de criptografia em repouso e em trânsito.

Gestão de chaves

As chaves 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 Gestão de Chaves (KMS) reforçado. A frequência do rodízio de chaves depende do grau de confidencialidade dos dados criptografados. Os certificados de TLS são geralmente renovados uma vez ao ano.

No momento, a HubSpot não pode usar as chaves de criptografia fornecidas por clientes.

Backup de dados e recuperação de desastres

Confiabilidade e recuperação do sistema

A HubSpot cumpre o compromisso de garantir a disponibilidade de seus sistemas adotando medidas comercialmente razoáveis para atender a tempo de atividade do serviço de 99,95% para nosso Serviço de Assinatura em um determinado mês. Para ter mais informações, leia a Seção 7 dos Termos Específicos de Produtos.

Além disso, disponibilizamos atualizações em tempo real e dados históricos sobre segurança e status do sistema no site de status da HubSpot.

Todos os serviços dos produtos da 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.

Recuperação de desastres

A HubSpot mantém um plano de recuperação de desastres testado anualmente como parte dos nossos controles SOC 2. Para ter mais informações, consulte o nosso Relatório SOC 2 (disponível para download em hubspot.com/security).

Estratégia de backup

BACKUPS DE SISTEMAS

Fazemos backups de sistemas obedecendo a cronogramas e periodicidades pré-estabelecidos. Backups de sete dias de dados são mantidos para qualquer banco de dados como forma de garantir que a restauração possa ocorrer com facilidade. O bom funcionamento da execução dos backups é monitorado, com geração de alertas no caso de eventuais exceções. Os alertas de falha são encaminhados, investigados e resolvidos.

Os backups locais de dados acontecem diariamente. Além disso, os backups são copiados periodicamente para uma região separada da AWS para fins de recuperação em caso de pane da região principal. Há monitoramento e alerta para falhas de replicação, com a devida triagem.

Todos os conjuntos de dados de produção são armazenados em uma instalação de hospedagem de arquivos com alta disponibilidade, como o S3 da Amazon.

ARMAZENAMENTO FÍSICO DE BACKUPS

Por utilizarmos os serviços de nuvem pública para hospedagem, backup e recuperação, a HubSpot não implementa infraestrutura ou mídias físicas de armazenamento em seus produtos. A HubSpot não produz nem usa outros tipos de mídias físicas (por exemplo, papel, fita etc.) como parte da disponibilização dos nossos produtos aos clientes.

PROTEÇÕES DE BACKUPS

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.

OPÇÕES DE BACKUP PARA CLIENTES

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 exportação, e a biblioteca de APIs públicas da HubSpot pode ser usada para sincronizar seus dados com outros sistemas. Para detalhes sobre como fazer backup dos seus dados, consulte nosso artigo da Central de Conhecimento sobre como exportar o seu conteúdo.

Controle de acesso e identidade

Gestão de usuários

Os produtos da HubSpot oferecem regras minuciosas de autorização. Os clientes têm autonomia para criar e gerenciar os usuários de seus portais e atribuir os privilégios que são apropriados para suas contas, limitando o acesso aos recursos de dados.

Para saber mais sobre as funções de usuários, consulte o Guia de Funções e Permissões do Usuário HubSpot.

Proteções de login

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 o logon único (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.

A opção "Entre com sua conta Google" está disponível para todos os clientes da HubSpot. Recursos mais avançados de SSO baseados em SAML integrados com qualquer IDP baseado em SAML estão disponíveis em todos os hubs de categoria empresarial.

Os clientes que usam um provedor de SSO podem configurar o logon único para seus usuários. As instruções para configurar o SSO estão disponíveis neste artigo da Central de Conhecimento e na HubSpot Academy. Os usuários de logon único e de 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.

Autorização de APIs dos produtos

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 saber mais sobre o uso da API, consulte o portal de Desenvolvedores em HubSpot.com.

Acesso à infraestrutura de produção

O acesso aos sistemas da HubSpot é estritamente controlado e segue o princípio do menor privilégio. Os colaboradores da HubSpot têm acesso com base no modelo de controles de acesso baseados em função (RBAC).

O acesso cotidiano é restrito apenas às pessoas que realmente precisarem dele para realizar suas funções. Para conceder acesso de emergência (por exemplo, resposta a alertas/solução de problemas) 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. Cada solicitação JITA é registrada, e os registros são monitorados continuamente para solicitações fora do padrão. Após o limite configurado de sessão, o acesso à conta expira e é revogado automaticamente.

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.

O acesso de colaboradores aos recursos corporativos e de produção está sujeito à análise automática diária e, pelo menos, uma revalidação manual de certificação semestral.

Acesso de colaboradores da HubSpot a portais de clientes

O Suporte ao Cliente, Atendimento e outras equipes que interagem diretamente com os clientes 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 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.

Autenticação e autenticação corporativas

O acesso à rede corporativa, tanto remoto quanto presencial, exige uma autenticação multifator (MFA) e eventuais aplicativos no modelo SaaS em uso pela HubSpot exigem SSO com MFA para facilitar o controle de acesso centralizado.

As políticas de senhas seguem as melhores práticas da indústria quanto à quantidade de caracteres, complexidade e frequência de troca.

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 corporativa e de produto várias vezes ao dia para garantir que as concessões de permissão estejam adequadas; gerenciar eventos de colaboradores; revogar contas e acessos 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.

Segurança corporativa e organizacional

Verificações de antecedentes e onboarding de colaboradores

Todos os colaboradores da HubSpot nos EUA passam por uma abrangente verificação de antecedentes realizada por terceiros antes de receberem oferta formal de emprego. Especificamente, são realizadas verificações de histórico profissional, formação e

antecedentes criminais de todos os colaboradores em potencial. Fora dos EUA, verificamos o histórico profissional. A verificação de referências é conduzida a critério do gerente de contratação.

No ato da contratação, todos os colaboradores devem ler e aceitar a Política Corporativa de Utilização Responsável da HubSpot (PUR) e o Código de Uso do Bom Senso (CUBS). Esses documentos ajudam a definir as responsabilidades de segurança dos colaboradores na proteção dos ativos/dados da empresa (incluindo, sem restrição, a proteção de dispositivos móveis e de equipamentos corporativos).

Gestão de políticas

Para que todos os nossos colaboradores estejam em sintonia em relação à proteção de dados, a HubSpot mantém documentadas diversas políticas e procedimentos. A HubSpot mantém uma Política de Segurança da Informação por Escrito, que aborda requisitos de tratamento de dados, considerações sobre privacidade e respostas a violações, entre vários outros assuntos.

As políticas são revisadas e aprovadas pelo menos uma vez ao ano e armazenadas na Wiki da empresa. As políticas que precisam da ciência dos colaboradores são incorporadas ao treinamento anual obrigatório.

Treinamento de conscientização de segurança

Para nós, nossos colaboradores são nossa primeira linha de defesa. Por isso, garantimos que sejam bem treinados para desempenhar suas funções. A HubSpot oferece um treinamento de conscientização de segurança que abrange melhores práticas de segurança a todos os novos colaboradores no momento da admissão e uma vez ao ano. Além desse treinamento, a HubSpot mantém os colaboradores a par das notícias ou iniciativas mais atuais sobre segurança com artigos internos.

Depois do treinamento inicial, conteúdos mais especializados são disponibilizados com base na função ou no acesso de cada colaborador. Por exemplo, a HubSpot tem um programa de Defensores da Segurança, em que os desenvolvedores das equipes de produto têm mais oportunidades de treinamento em desenvolvimento na área de segurança e riscos, ameaças e problemas comuns.

Gestão de riscos

A HubSpot tem um programa de Gestão de Riscos Corporativos (ERM, na sigla em inglês) que inclui uma política documentada de ERM, avaliações contínuas de riscos e um registro formal de riscos. Ações de mitigação e reparação de riscos são monitoradas por um sistema de tíquetes e analisadas a uma frequência predefinida.

Encontre mais detalhes sobre nossa avaliação de riscos e nosso programa de gestão de riscos no Relatório SOC 2, disponível para download em hubspot.com/security.

Gestão de fornecedores

Usamos diversos prestadores de serviços terceirizados que aumentam a capacidade dos produtos da HubSpot em atender às suas necessidades de marketing, vendas, atendimento ao cliente, gestão de conteúdo e operações. 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 análise de programas de segurança dos fornecedores que prestam suporte à HubSpot.

Proteções apropriadas são avaliadas com relação ao serviço que está 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. Nossas equipes de Segurança e Conformidade e nosso Departamento Jurídico trabalham em estreita colaboração com nossos stakeholders como parte do processo de análise de gestão de fornecedores.

Também mantemos uma lista dos nossos Suboperadores em nosso Acordo de Tratamento de Dados (ATD).

Segurança física corporativa

Os escritórios da HubSpot são protegidos de diversas formas. Contratamos agentes de segurança para cada escritório internacional da HubSpot para ajudar a criar um ambiente seguro para os colaboradores. O acesso às portas é controlado usando tokens RFID individuais, que são desativados automaticamente em caso de perda ou situação em que deixem de ser necessários (por exemplo, demissão, uso pouco frequente etc.). Vigilância

por vídeo e muitas outras medidas de proteção são implementadas nos escritórios da HubSpot.

Proteções da rede corporativa

A HubSpot implanta firewalls de aplicativos com gerenciamento centralizado para fins de alta de disponibilidade em seus escritórios corporativos. Nossas redes de visitantes ficam separadas da rede corporativa e são atendidas por firewalls separados. Os firewalls são configurados para filtrar tráfego de entrada da Internet não autorizado, bem como para recusar conexões de rede que não sejam explicitamente autorizadas por uma regra.

A HubSpot faz verificações de conformidade do sistema antes de autorizar a conexão de um dispositivo à rede corporativa. Os dispositivos não autorizados são desconectados automaticamente ou movidos para VLANs de contenção.

Proteção de terminais e proteção contra vírus e malware

A HubSpot usa recursos de detecção e resposta de terminais (EDR, na sigla em inglês) para proteger seus sistemas. Assim, temos ampla visibilidade sobre comportamentos anormais dos sistemas e conseguimos investigar e tomar as medidas adequadas rapidamente por acionadores de eventos automatizados ou contenção manual de um sistema. Nossa plataforma de EDR tem integração com outras ferramentas em nosso conjunto de segurança, criando um ecossistema versátil e otimizado para proteger nossa empresa de forma eficiente.

Gestão de incidentes

Resposta a incidentes

A equipe da Central de Operações de Segurança (SOC, na sigla em inglês) da HubSpot oferece cobertura 24h 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. Fornecemos atualizações periódicas, conforme necessário, para garantir a solução apropriada do incidente.

Nosso diretor de Segurança da Informação 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.

Além da SOC, a HubSpot também uma equipe interna Caçadora de Ameaças que trabalha para descobrir sistematicamente eventuais vulnerabilidades e garantir que as melhores práticas estão sendo seguidas para proteger o nosso produto.

Conformidade

Lei Sarbanes-Oxley (SOX)

Por ser uma sociedade de capital aberto, os principais controles de TI da HubSpot passam por auditorias regulares como parte do cumprimento da Lei Sarbanes-Oxley.

As informações sobre o cumprimento da Lei Sarbanes-Oxley por parte da HubSpot estão disponíveis em nossas declarações à SEC. Mais informações estão disponíveis em nossa página de Relações com investidores: https://ir.hubspot.com/

Controles de sistemas e organizacionais (SOC 2)

A HubSpot passa por rigorosas auditorias anuais de SOC 2 Tipo 2 e SOC 3 para atestar os controles que aplicamos para reger a disponibilidade, a confidencialidade e a segurança dos dados dos clientes seguindo os Princípios de Serviços de Confiança estabelecidos pelo American Institute of Certified Public Accountants (AICPA). Temos orgulho da excelência dos nossos controles e convidamos você a obter uma cópia do nosso relatório SOC 2 Tipo 2 entrando em contato com seu representante da HubSpot. Nosso Relatório SOC 3 está disponível para download na página da HubSpot sobre segurança (hubspot.com/security).

Tratamento e armazenamento de dados sensíveis

Consulte os nossos Termos de Serviço (https://legal.hubspot.com/terms-of-service) para saber mais sobre os tipos de dados proibidos. Os produtos da HubSpot não devem ser 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 habilitação ou identificadores semelhantes, ou dados de histórico profissional, financeiros ou de saúde.

Muitos clientes da área da saúde utilizam a HubSpot para suas necessidades de front-office sem incorporar dados sensíveis de saúde. No entanto, a HubSpot não deve ser considerada uma solução para tratar ou armazenar informações eletrônicas protegidas de saúde (ePHI), não segue a HIPAA nem tem certificação HITRUST.

Da mesma forma, embora nossos clientes peguem o serviço usando cartão de crédito, a HubSpot não armazena, processa ou coleta dados de cartão de crédito enviados a nós pelos clientes e não segue os padrões PCI-DSS. Usamos os serviços de processadores de cartões de pagamento de confiança e que seguem os padrões PCI para garantir que as nossas próprias transações de pagamento aconteçam com segurança.

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.

Retenção e exclusão de dados

Os dados do cliente ficarão retidos enquanto você permanecer como um cliente ativo. A plataforma da HubSpot oferece aos clientes ativos ferramentas para excluir seus dados

(consulte a seção "Exclusão ou devolução de Dados Pessoais" em nosso ATD) ou exportá-los (consulte o artigo da Central de Conhecimento sobre como exportar seus conteúdos e dados).

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.

No momento, a HubSpot não oferece aos clientes a possibilidade de definir políticas personalizadas de retenção de dados.

Gestão do programa de privacidade

A equipe de Segurança, o Departamento Jurídico e várias outras equipes da HubSpot colaboram para garantir um programa de privacidade eficaz e implementado de forma robusta. As informações sobre o nosso compromisso com a privacidade dos seus dados estão descritos em mais detalhes nos nossos documentos a seguir:

- Política de Privacidade
- Política de Privacidade de Produtos
- Acordo de Tratamento de Dados

Resposta a violações

Para mais informações, consulte as nossas políticas, processos e obrigações de divulgação de violações em nosso Relatório SOC, na seção "Resposta a incidentes".

Nós também deixamos claras as nossas obrigações sobre violações de dados pessoais em nosso ATD.

GDPR

A plataforma da HubSpot tem diversos recursos para permitir que nossos clientes cumpram as exigências do GDPR e mantenham a conformidade com a lei com facilidade, incluindo a possibilidade de fazer as exclusões de dados previstas no GDPR em resposta a solicitações de acesso de titulares dos dados (DSARs) (consulte o artigo da Central de Conhecimento aqui). Nossa página sobre o GDPR está disponível aqui.

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.