Google™ Apps for Business

6 mitos sobre a segurança na nuvem

Cinco milhões de empresas usam o Google Apps for Business, aumentando a produtividade e o trabalho em equipe e diminuindo custos. Mas alguns empresários ainda se preocupam com a segurança. Nós entendemos. Quando o assunto é a sua empresa, você não quer correr riscos.

Há muitos mitos sobre a segurança na nuvem. Vamos desvendar alguns deles:

Mito: o Google vende minhas informações.

Fato: com o Google Apps, você é proprietário dos seus dados.
A menos que você use os serviços para isso, não compartilhamos seus dados (exceto em casos especiais descritos na política de privacidade). Não vendemos, trocamos nem alugamos dados pessoais identificáveis do usuário. Suas informações são suas — e continuam assim.

Mito: tudo o que está na Internet é mais vulnerável a hackers.

Fato: seus dados estão mais seguros na nuvem que no seu escritório.
Protegemos dados em movimento na Internet com a criptografia SSL. A equipe de segurança das informações monitora constantemente nossa rede global de datacenters para manter seus dados em segurança. Nossos controles de administração e segurança passaram por auditoria ISAE 3402 tipo II e nosso sistema de mensagens e colaboração foi o primeiro a receber a certificação US FISMA (Lei federal de gerenciamento de segurança das informações). Além da senha, você também pode usar a autenticação em duas etapas para dificultar ainda mais o acesso não autorizado.

Mito: se mudar de ideia, não poderei recuperar meus dados.

Fato: os dados podem ser exportados onde e quando você quiser.
Manteremos seus dados enquanto você tiver conta conosco. Mas se você quiser, temos ferramentas para ajudá-lo a exportar seus e-mails, diários, contatos, documentos e sites. Por exemplo, é possível exportar seus documentos para vários formatos compatíveis com Microsoft. Saiba mais na Google Data Liberation Front.

Google™ Apps for Business

Mito: Não posso usar o Google porque meus dados poderão ser armazenados fora dos EUA.

Fato: o Google está registrado no programa Safe Harbor dos EUA e da UE.
O Google adota os princípios de privacidade de notificação, escolha, transferência, segurança, integridade de dados, acesso e aplicação do Safe Harbor dos EUA e está registrado no programa Safe Harbor do departamento de comércio dos EUA. A estrutura Safe Harbor foi desenvolvida para garantir que as empresas possam transferir dados pessoais da UE para os EUA, mantendo a proteção de dados de acordo com os sete princípios fundamentais da UE.

Mito: o Google pode ler meus e-mails e documentos.

Fato: o Google não pode ler seus e-mails nem documentos.
Os empregados do Google não podem acessar os dados da sua conta, exceto em casos muito especiais — e mesmo assim precisamos da sua permissão (Consulte nossa política de privacidade).

Mito: os sistemas da maioria das empresas são seguros o suficiente.

Fato: nem tanto.
Nossa pesquisa mostrou que a maioria dos proprietários e gerentes de pequenas empresas sobrevaloriza seu nível de segurança. Eles não possuem backups recentes e não os protegem externamente (com o Google Apps, o backup dos dados é feito automaticamente em nossos datacenters globais. Assim, ficam protegidos contra perda acidental, roubo e incêndios). Eles não têm planos de recuperação de desastres (nós garantimos 99,9% de tempo de funcionamento* e oferecemos recuperação de desastres robusta e integrada — melhor que a maioria dos hardwares e softwares internos). E eles não criptografam os dados valiosos (com o Google Apps, todos os dados são criptografados em movimento e o acesso é protegido pela autenticação em duas etapas. Isso significa que os dados ficam muito mais seguros em nossa nuvem que armazenados localmente em um laptop).

*SLA Garanta 99,9% de disponibilidade sem tempo de inatividade agendado