LGPD

4 pilares fundamentais a considerar ao escolher soluções em nuvem para sua empresa

Introdução

A lei Geral de Proteção de Dados (LGPD) afirma que as empresas devem lidar com dados pessoais de forma segura, transparente e legal durante todo o ciclo de vida do processamento de dados. Como as empresas estão usando cada vez mais ferramentas de software baseadas em nuvem, garantir que todos esses provedores gerenciem dados pessoais seguindo as rígidas obrigações da LGPD apresenta um desafio significativo para os departamentos de TI, jurídico e de compras. Esteja você planejando mudar para um novo serviço de armazenamento em nuvem ou confirmar que seu provedor atual está em conformidade, você precisa verificar vários aspectos tecnológicos e legais para processar dados pessoais com segurança e atender aos requisitos da LGPD. Este eBook visa ajudá-lo a compreender os Dados Gerais Regulamento de proteção, seus requisitos para gerenciar dados pessoais e por que a LGPD destaca a criptografia como uma medida técnica essencial para proteger os dados. Também resumimos aspectos mais importantes a serem considerados ao escolher serviços de armazenamento em nuvem com conformidade com a LGPD.

4 principais requisitos que os serviços de armazenamento em nuvem devem atender para conformidade com a LGPD

1. Criptografia

A LGPD recomenda que as empresas usem salvaguardas técnicas como criptografia para proteger dados pessoais. A criptografia é uma medida crucial de segurança na nuvem porque minimiza o risco de expor dados pessoais se seus arquivos vazarem devido a um ataque de hacker ou erro humano.

Se a criptografia for feita com segurança, os arquivos criptografados vazados, incluindo dados pessoais, são "ruído branco" ilegível para qualquer parte não autorizada. Se seus dados não puderem ser acessados em um formato legível, você não precisa notificar seus clientes ou funcionários cujos dados você gerencia. Se seus dados pessoais não forem violados, seus direitos de privacidade não serão prejudicados.

A LGPD refere-se à criptografia em várias disposições. No entanto, ele não indica explicitamente qual algoritmo (por exemplo, **AES-256**) e arquitetura ou aplicativo (por exemplo, do lado do servidor ou de **ponta a ponta**) recomenda. Nem todos os tipos de criptografia fornecem o mesmo nível de proteção se seus arquivos acabarem nas mãos erradas. Assim, você deve examinar cuidadosamente as metodologias de criptografia usadas por seus provedores. Além disso, a maneira como as chaves de criptografia são armazenadas e gerenciadas é essencial para decidir se é viável descriptografar e ler os dados vazados.

Com criptografia do lado do servidor (criptografia em trânsito e em repouso), o provedor de armazenamento em nuvem tem acesso às chaves de criptografia e, portanto, aos dados pessoais armazenados nos arquivos.

1. Criptografia

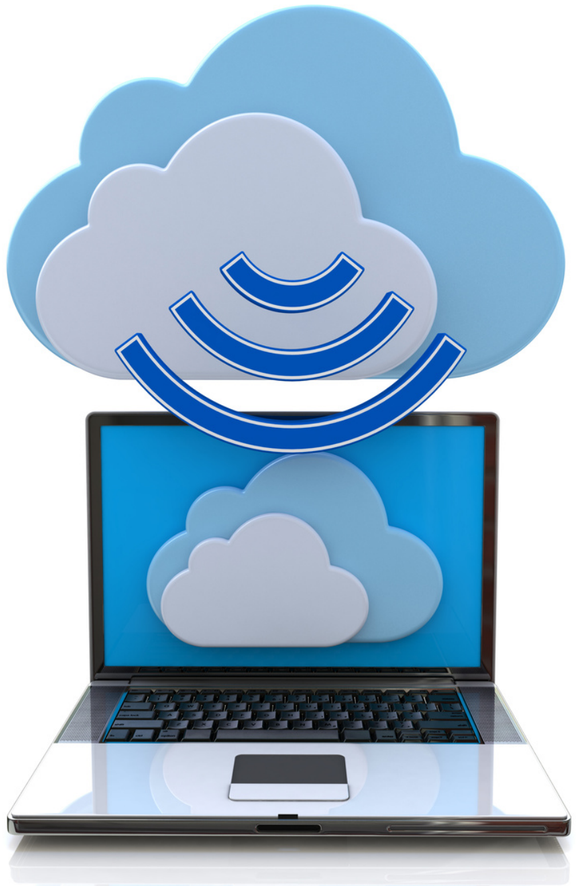
O processo de criptografia/descriptografia acontece na nuvem, em seus servidores. Mesmo que sua empresa use módulos de segurança de gerenciamento de chaves, há uma chance de que o provedor de nuvem tenha acesso às suas chaves de criptografia e aos seus dados. Como resultado, não apenas eles, mas os hackers que violam seus sistemas podem descriptografar seus arquivos que contêm dados pessoais.

Com **criptografia de ponta a ponta**, as chaves são armazenadas nos dispositivos do usuário. Assim, o provedor nunca tem acesso às chaves de texto simples e aos dados pessoais armazenados em arquivos. Como resultado, mesmo que ocorresse uma violação de dados do lado do servidor, os hackers não poderiam ler os arquivos, incluindo dados pessoais. Isso significa que nenhum dado pessoal pode ser exposto devido a um incidente de segurança do lado do servidor.

A criptografia ponta a ponta de conhecimento zero com gerenciamento de chaves do lado do cliente representa uma proteção mais forte para dados pessoais contra violações. Do ponto de vista legal, se você armazenar seus arquivos contendo dados pessoais em provedores de armazenamento em nuvem criptografados de ponta a ponta, esses provedores nem mesmo serão considerados processadores de dados em relação aos dados criptografados.

Também é importante que o provedor use algoritmos padrão do setor, como o AES-256, que são verificados minuciosamente por pesquisadores de criptografia.

Veja aqui como a Enuve atua no quesito segurança



1. Criptografia

- Para obter a proteção mais robusta, certifique-se de que as chaves de criptografia são controlados por você no lado do cliente e a criptografia ocorre no seu dispositivo e não na nuvem.

- Procure **serviços criptografados de ponta a ponta** que nunca tenham acesso as chaves de criptografia de texto simples e o conteúdo do arquivo.

- Verifique se o provedor usa algoritmos padrão do setor, como **AES-256**.

2. Segurança e Controle de Dados

Além de aplicar criptografia forte, seu provedor precisa tomar cuidado com medidas para proteger os dados de seus usuários. Em primeiro lugar, a segurança da conta deve ser levada a sério. Isso inclui gerenciar a autenticação do usuário com segurança, de preferência por meio de conhecimento zero métodos. Existem diferentes níveis de segurança com que um provedor de serviços trata sua senha. O nível mais alto de proteção por senha é o “conhecimento zero” método: seu provedor não tem conhecimento de sua senha. como o serviço provedor não tem conhecimento de sua senha, ela não será comprometida, mesmo se o provedor de serviços for hackeado. Além da proteção por senha, certifique-se de que o provedor oferece multifator autenticação. Isso adiciona camadas extras de proteção ao método de senha simples solicitando a verificação de sua identidade com um dispositivo adicional confiável (por exemplo, com um código gerado por um aplicativo em seu telefone).

A LGPD exige que todas as organizações para implementar políticas abrangentes de proteção de dados. As empresas têm de proteger a confidencialidade e integridade dos dados pessoais: devem ser tratados de forma que garanta a segurança adequada com medidas técnicas e organizacionais. Isso significa ter práticas e políticas de segurança em vigor e aplicá-las diariamente. Quando se trata de colaboração dentro das equipes e manter contato com clientes ou parceiros, essas políticas são essenciais para manter os dados seguros. De acordo com pesquisas, muitas violações de dados são causadas por erros de funcionários. Esses incidentes podem incluir casos em que os dispositivos de trabalho são perdidos, roubados ou quando os funcionários vazam dados de propósito

2. Segurança e Controle de Dados

Certifique-se de que seu provedor oferece amplo controle e governança de dados e recursos para minimizar os riscos desses eventos. Existem vários recursos úteis você deve procurar:

- Gerenciamento de permissão para configurar níveis de acesso granulares para dados sensíveis.
- Painel central para monitorar as atividades da equipe relacionadas ao gerenciamento de arquivos, como quem abriu ou excluiu os arquivos (trilha de auditoria e logs de atividades).
- A possibilidade de criar e monitorar políticas de segurança interna relacionadas à segurança de dados.
- Opções de backup, como recuperação de arquivos excluídos e ferramentas de controle de dispositivos (revogar acesso, limpeza remota, etc.)

3. Transparência

A LGPD afirma que os dados pessoais devem ser processados de forma legal, justa e de forma transparente. Como controlador de dados, você deve certificar-se de que os serviços de terceiros você usa também atende a esses requisitos. De acordo com o princípio da responsabilidade, a responsabilidade final e a obrigação de proteger os dados são suas. No caso de uma auditoria, você deve provar às autoridades que todos os seus fornecedores atendem aos requisitos da LGPD. Para garantir isso, é crucial escolher um armazenamento em nuvem que é transparente sobre como eles gerenciam os dados e fornecem informações claras e informações fáceis de entender sobre isso, incluindo como eles processam dados e quais serviços de terceiros eles usam.

4. Relatórios de logs

Relatórios de logs detalhados são uma ferramenta valiosa para monitorar e auditar a atividade de usuários em um sistema de armazenamento de dados. Esses relatórios fornecem informações importantes sobre uploads, downloads e atividades de login e logout de usuários em um determinado sistema.

Os logs de upload fornecem informações sobre quais arquivos foram enviados para o sistema, quando foram enviados e quem os enviou. Esses logs são úteis para monitorar o fluxo de dados no sistema e identificar qualquer atividade suspeita ou não autorizada.

Os logs de download fornecem informações semelhantes, mas em vez de rastrear o envio de arquivos para o sistema, eles rastreiam o download de arquivos a partir do sistema. Esses logs podem ser usados para rastrear quem está baixando arquivos do sistema e quando eles estão fazendo isso. Isso pode ser útil para fins de auditoria e para monitorar o acesso a dados sensíveis.

Os logs de atividade de login e logout fornecem informações sobre quando os usuários se conectaram e desconectaram do sistema. Esses logs são úteis para monitorar a atividade de usuários em um determinado sistema e identificar qualquer atividade suspeita ou não autorizada. Eles podem ser usados para detectar tentativas de acesso não autorizado ao sistema e monitorar o tempo de atividade de usuários.

Em resumo, os relatórios de logs detalhados fornecem informações valiosas sobre a atividade de usuários em um sistema de armazenamento de dados. Eles são úteis para fins de monitoramento, auditoria e segurança, e podem ajudar a identificar e prevenir atividades não autorizadas ou maliciosas no sistema.

Entre em contato

Website

www.enuve.com.br

Telefone

11 4007 1979

Email

comercial@enuve.com.br

Endereço

Av. Eng. Luiz Carlos Berrini, 1500/74 São Paulo - SP