Datasafer

LGPD e Nuvem

Implicações e formas de adaptação

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, sancionada em 2018, impulsionou a discussão sobre a temática da segurança da informação e sua importância para as empresas. Com a expansão da tecnologia, os dados se tornaram um ativo fundamental para as corporações. A legislação busca, então, normatizar seu tratamento.

A ideia do regramento é dar mais **autonomia e controle aos usuários sobre as próprias informações pessoais**, elencando como as empresas que as detêm devem realizar a **coleta, uso, armazenamento e compartilhamento**. A partir da LGPD, premissas como o consentimento tornam-se imprescindíveis nesses processos, caso elencada como base legal para a atividade.

Além disso, um dos fatores que impulsiona a criação e implementação da lei é o aumento no número de investidas que visam o roubo ou sequestro de dados. Um **levantamento realizado pela Kaspersky** mostra que a quantidade de ciberataques cresceu 23% no Brasil, em 2021.

Datasafer

Essa é uma das provas da **necessidade de proteção dos dados**, já que indivíduos estão sempre buscando explorar vulnerabilidades em sistemas e descuidos de usuários para aplicar esses golpes.

Uma possibilidade de garantir mais segurança no tratamento de dados de empresas é a nuvem. Apesar de serem necessárias algumas ações para se adequar aos parâmetros da LGPD, a cloud é uma excelente opção de armazenamento para **garantir o gerenciamento de risco e a segurança das informações**. Em boas nuvens, é possível **monitorar os dados, criptografá-los**, além de saber que estão alocados em data centers certificados, para atender às exigências da legislação e de auditoria.

Neste e-book, apresentaremos quais são os aspectos exigidos e descritos na LGPD, como eles influenciam o armazenamento de informações na nuvem e quais os benefícios de utilizá-la ou fornecer esse tipo de serviços para clientes de consultorias de Tecnologia da Informação (TI) e Managed Service Providers (MSPs).

Boa leitura!

Datasafer

Histórico da LGPD

A LGPD determina como devem ser realizados os tratamentos de dados praticados no país, coletados por empresas no território nacional ou que envolvam indivíduos que estão no Brasil. A legislação apresenta os atores nesse processo, as bases para realizá-lo de forma correta e as multas e sanções no caso de descumprimento

.

No Brasil, a primeira consulta pública a respeito do uso de informações pessoais foi realizada em 2010. Esse é um dos primeiros marcos na história da formulação de uma lei a respeito da temática.

Após isso, a criação de outros regramentos sobre assuntos relacionados ao gerenciamento de informações e o universo digital, como o **Marco Civil da Internet** (Lei N° 12.965/14) e a **Lei Carolina Dieckmann** (Lei N° 12.737/12), fizeram com que a pauta se mantivesse em discussão.

Datasafer

Grandes vazamentos de dados e escândalos também influenciaram a elaboração da LGPD. O **caso Snowden** é o principal deles. Em 2013, o ex-funcionário da Agência de Segurança Nacional Norte-Americana (NSA) denunciou o amplo monitoramento realizado pelo país em seus cidadãos e em dados de outros governos, abrindo os olhos do Brasil a respeito da questão.

Nesse mesmo contexto de vazamentos, surge a maior inspiração da LGPD, o Regulamento Geral sobre a Proteção de Dados (GDPR) vigente na União Europeia e no Espaço Econômico Europeu. Promulgada em 2016, a legislação normatiza o tratamento de dados pessoais na Europa e têm parâmetros que influenciaram a construção da lei brasileira.

Após a construção do texto da LGPD, a promulgação ocorreu em 2018, no governo do então presidente Michel Temer. A legislação entrou em vigor dois anos depois, em 2020, e as multas e sanções começaram a ser aplicadas a partir de agosto de 2021.

Datasafer

O que são dados pessoais?

A LGPD define dados pessoais como qualquer informação relacionada a pessoa natural identificada ou identificável. Esse conceito abrange, então, todos os dados que permitam reconhecer e diferenciar pessoas.

Além das informações pessoais mais difundidas, como **nome, CPF, data de nascimento, telefone e endereço**, outros tipos de dados são muito importantes, principalmente no contexto digital.



Informações como **localização de GPS, renda, histórico de pagamentos, fluxos bancários, hábitos de consumo**, além das provenientes de dispositivos e do uso da internet, como **endereço de IP e cookies**, são consideradas dados pessoais nos termos da LGPD.

A legislação ainda conceitua outros dois tipos de dados, a fim de parametrizar o tratamento. Os **dados pessoais sensíveis** são informações como origem racial ou étnica, convicção religiosa, posicionamento político e referentes à saúde, genética ou vida sexual.

Já os **dados anonimizados** são definidos como os relativos a titulares que não possam ser identificados. Por não identificarem a pessoa física, esses dados não são objeto da LGPD.

Datasafer



A importância de proteger dados pessoais

A partir do panorama já apresentado, é possível entender a relevância da proteção dos dados pessoais. Essas informações permitem distinguir os usuários e, por isso, as decisões a respeito de seu uso devem partir exclusivamente deles.

Com a valorização dos dados, faz-se necessário, então, estabelecer os parâmetros para sua utilização. Nesse processo, as legislações como a GDPR e a LGPD vêm dar respaldo aos indivíduos e definir os limites no tratamento de informações.

vem

Datasafer

A perspectiva comum dessas leis é de que os usuários devem ser protagonistas e ter autonomia a respeito da forma como seus dados serão usados. Para isso, **a premissa do consentimento torna-se bastante relevante**, especialmente no que se refere aos dados pessoais sensíveis e às atividades em que a base de tratamento demande um aceite do titular.

Em ambas as legislações e, considerada a atividade realizada, é salientada a necessidade de o indivíduo concordar com o tratamento de suas informações explicitamente e saber para qual finalidade isso irá ocorrer, como e por quanto tempo.

Essa ideia é importante, pois colabora para a criação de uma consciência coletiva a respeito do uso de dados, diminuindo casos de utilizações indiscriminadas e abusivas. Além disso, ajuda a tornar as atividades de tratamento mais seguras, já que estabelece os papéis e as responsabilidades de cada ator no processo.

Datasafer

Com o aumento no número de vazamentos e ataques com intuito de roubo de informações, o amparo jurídico ainda contribui para o entendimento de como proceder no caso de incidentes e violações. Esses padrões e exigências, então, objetivam a construção de um tratamento de dados mais seguro e transparente.

Para isso, o setor de TI é fundamental para se adequar às normas legais, já que é responsável pelo gerenciamento de tecnologias e por garantir a segurança das informações da empresa e, consequentemente, dos usuários. As bases de dados precisam estar protegidas e prontas para serem acessadas quando necessário.

Atores da LGPD

A LGPD determina quatro papéis de atuação possíveis no tratamento de dados. Além disso, há uma denominação que abarca dois deles na definição de responsabilidades. Confira as conceituações a seguir:

Datasafer

Titular

O titular é descrito na legislação como a pessoa natural a quem se referem os dados pessoais objetos de tratamento.

Controlador

Já o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões do tratamento.

Operador

Segundo os parâmetros da LGPD, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento das informações em nome do controlador.

Encarregado

O encarregado é definido como a pessoa indicada pelo controlador e operador para operar como canal de comunicação entre ele, o titular e a Autoridade Nacional de Proteção de Dados (ANPD).

Agentes de tratamento

Na LGPD, os agentes de tratamento são o controlador e o operador.

Datasafer



Princípios da LGPD

A LGPD define uma série de princípios para o tratamento de dados, além da boa-fé. Entre eles, pode-se destacar a **finalidade**, a **adequação**, o **livre acesso**, a **transparência**, a **segurança** e a **não discriminação**. A seguir, elencamos como cada um deles deve reger as atividades:

Finalidade

O princípio da finalidade determina que a realização do tratamento de dados deve ocorrer para propósitos legítimos, específicos e informados ao titular, sem possibilidade de uso posterior incompatível com eles.

Datasafer

Adequação

A adequação é definida como a compatibilidade do tratamento de dados com a finalidade informada ao titular, considerando o seu contexto.

Livre acesso

O princípio do livre acesso estabelece que deve ser garantida aos titulares consulta facilitada sobre a forma e a duração do tratamento, além da integralidade dos dados.

Transparência

Complementando o livre acesso, a transparência é um princípio que estipula a garantia aos titulares de informações precisas e facilmente acessíveis a respeito do tratamento e dos agentes que o realizam.

Segurança

O princípio de segurança estabelece a utilização de medidas técnicas e administrativas para proteger os dados de acessos não autorizados e acidentes de perda, alteração, destruição e difusão.

Datasafer

Não discriminação

A não discriminação determina que a realização do tratamento dos dados não pode ocorrer para fins discriminatórios, ilícitos ou abusivos.
Além desses princípios, a lei ainda estipula que o agente é responsável por comprovar o cumprimento das normas estabelecidas, prestando contas sempre que necessário.

Bases da LGPD

Já as bases legais de tratamento são as que justificam a realização do tratamento de dados. A lei aponta uma série de possibilidades nas quais essas atividades podem ou devem ser desempenhadas.

O maior destaque nesse sentido é o **consentimento**, definido na legislação como a manifestação livre, informada e inequívoca na qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica.

Datasafer

Isso quer dizer que, seguindo os princípios de transparência e adequação, os titulares sempre devem ser informados da finalidade do tratamento de dados e, para determinadas atividades, são convidados a aceitar a respectiva realização, por meio de uma ação (call to action).

Outra base importante é o **cumprimento de obrigação legal ou regulatória do controlador**. Caso a empresa necessite cumprir outra lei que determine o tratamento de dados, as atividades são justificadas.

A **execução de contratos** também é uma possibilidade que respalda o uso de informações pessoais. Se o titular formaliza uma contratação na qual está previsto o tratamento de dados, a empresa pode realizá-lo.

A base de **interesse legítimo do controlador** descrita na LGPD é outro ponto que merece destaque. A legislação prevê que, caso haja finalidade legítima, o tratamento de informações pode ser fundamentado e realizado por empresas para promoção de suas atividades e divulgação de serviços que beneficiem o titular.

Datasafer

No entanto, no tipo de situação descrita acima, a lei ressalta que devem ser respeitados direitos, expectativas e liberdades do titular; somente dados pessoais, não os sensíveis, estritamente necessários devem ser utilizados e as finalidades que orientem as atividades devem ser baseadas em situações concretas.

Sanções da LGPD

A LGPD ainda determina uma série de sanções administrativas que podem ser aplicadas em caso de infrações às normas descritas na lei. A advertência é uma delas e conta com a indicação do prazo para a adoção de medidas corretivas.

A multa simples é outra penalidade que consta na legislação e pode chegar a até 2% do faturamento da empresa, com limite de 50 milhões de reais por infração. Há também a possibilidade da aplicação de **multas diárias**, com o mesmo limite estabelecido na simples.

Estão previstos ainda o bloqueio e a eliminação dos dados pessoais a que se refere a infração, que também pode ser publicizada após sua apuração e confirmação.

Além disso, podem ocorrer suspensões no funcionamento de bancos de dados ou nas atividades de tratamento de informações por um período máximo de seis meses, prorrogável pelo mesmo intervalo de tempo.

A proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados é outro tipo de punição descrito na lei.



Datasafer

Adequação à LGPD

Adequar a gestão de informações de empresas à LGPD pode demandar alguns esforços, mas eles são necessários para **evitar as sanções previstas na legislação**.

O primeiro passo para isso, na corporação, é definir quem será a equipe responsável. Integrar membros da área jurídica, do marketing e da TI é fundamental para elaborar políticas e práticas pautadas nas normatizações.

A partir disso, é possível revisar os processos e trabalhar na conformidade dos documentos da empresa, como a política de privacidade, contratos e termos de consentimento, para mantê-los alinhados com as bases de tratamento previstas na lei.

É preciso que os textos sejam transparentes em relação às atividades e suas finalidades para que os titulares compreendam como elas serão desempenhadas e com quais objetivos.

Datasafer

Estabelecer quem será o encarregado dos dados também é uma parte importante desse processo. Esse ator será a ponte de comunicação entre a corporação, o titular e a ANPD, por isso, deve estar descrito nos documentos e pronto para atuar quando necessário.

Além dessas questões que envolvem as partes jurídicas do tratamento de dados, os aspectos técnicos e práticos precisam ser adequados à legislação.

Manter atualizado um mapeamento do fluxo de dados coletados pela empresa, com o ciclo de vida das informações e detalhamentos a respeito de sua coleta, armazenamento, compartilhamento e descarte é muito importante. Isso facilita realizar ações a pedido do titular quando solicitado.

A segurança dos dados é outro ponto que deve ser priorizado, já que é uma das premissas da LGPD. É preciso garantir que as informações estejam protegidas e não possam ser acessadas por terceiros ou por membros que não deveriam, violadas, excluídas indevidamente e vazadas.

Datasafer



Implicações da LGPD para a nuvem

A nuvem é uma das possibilidades de plataforma de armazenamento de dados, cada vez mais difundida por conta da facilidade de contratação de volume e gerenciamento. A LGPD incide sobre esse tipo de serviço de formas variadas.

As principais implicações da lei na nuvem são no quesito segurança. A legislação ressalta que as informações devem estar protegidas para evitar as ameaças descritas anteriormente e seu uso indevido.

vem

Datasafer

Por isso, **é preciso contar com camadas de segurança que garantam a integridade dos dados**, seu acesso apenas por agentes autorizados e o uso para as finalidades especificadas ao titular.

Caso a empresa tenha uma **nuvem privada**, o controle é gerenciado pela própria corporação, e as informações podem estar alocadas em servidores próprios ou alugados. Sendo assim, a própria empresa é responsável pela adequação às normas da LGPD.

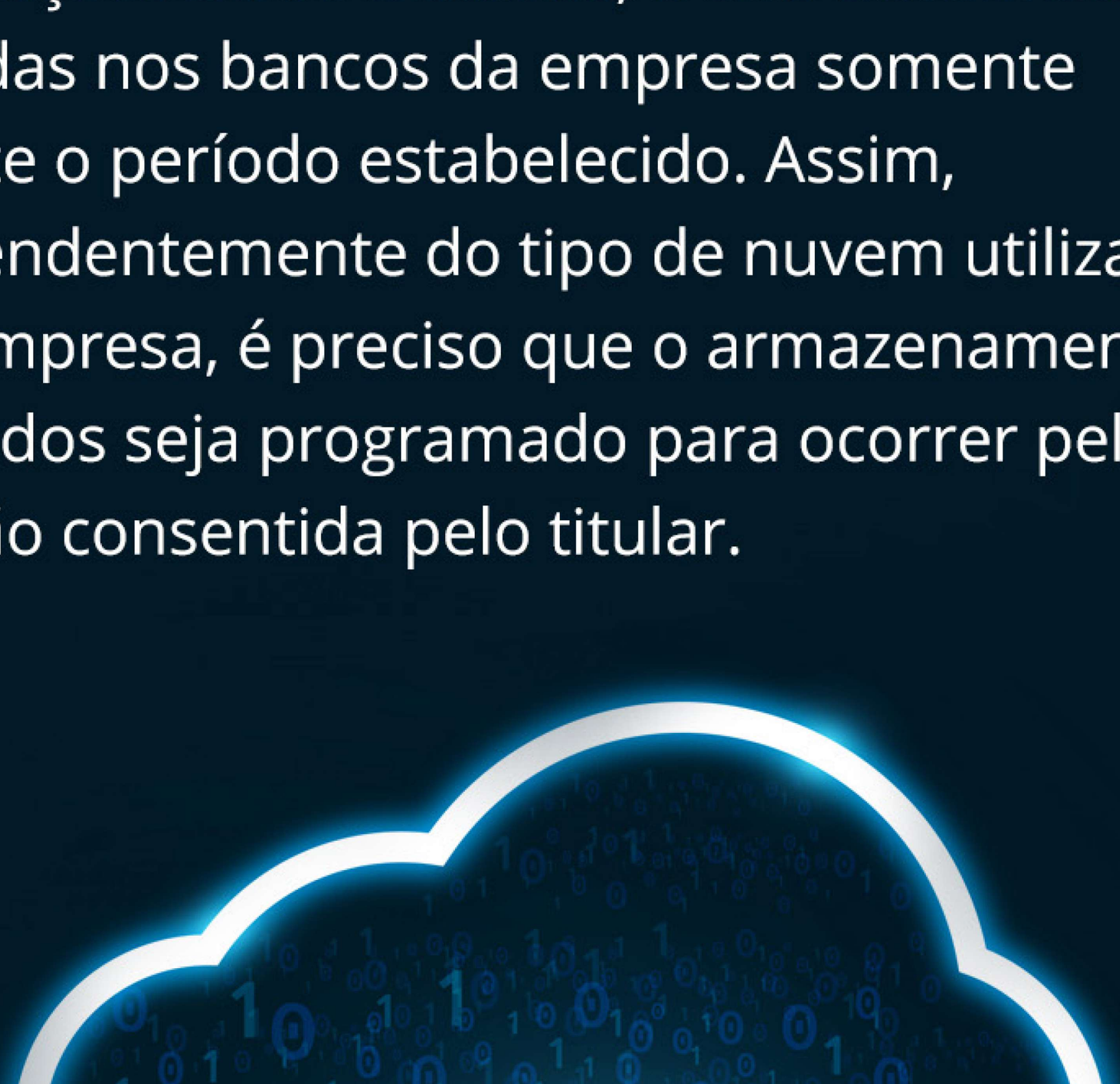
Isso significa que a corporação tem que criar ou utilizar tecnologias de segurança que possam manter os dados protegidos e com acesso disponível para atender demandas quando necessário.

Já no caso das **nuvens públicas**, em que as informações são alocadas em servidores remotos de empresas que disponibilizam o serviço de armazenamento, é preciso saber se o provedor atende aos requisitos de segurança dispostos na LGPD e se é possível controlar os acessos das informações.

Datasafer

Nos **modelos de nuvem híbrida**, em que são combinados os dois tipos de nuvem descritos, é necessário revisar se ambas estão em conformidade com os parâmetros da legislação e se o armazenamento dos dados em uma ou outra também está alinhado com as práticas determinadas.

Além disso, outro ponto importante é a duração do armazenamento dos dados. A lei determina que o usuário saiba por quanto tempo suas informações serão tratadas, e elas devem ser mantidas nos bancos da empresa somente durante o período estabelecido. Assim, independentemente do tipo de nuvem utilizada pela empresa, é preciso que o armazenamento dos dados seja programado para ocorrer pela duração consentida pelo titular.



Datasafer

Benefícios da nuvem para adaptação à LGPD

Bons provedores de nuvem normalmente já contemplam os critérios de segurança estabelecidos pela LGPD. Mas além de atender aos critérios, a cloud pode contar com uma série de benefícios para as empresas que precisam se adequar à legislação.

Listamos alguns deles a seguir:

Criptografia

A criptografia é um fator que ajuda a manter os dados protegidos, já que somente quem tem o código de segurança pode acessá-los, e é um aparato de segurança disponível na maioria das nuvens. É também uma ótima maneira de garantir o sigilo de informações confidenciais e impedir violações.

Datasafer

Mapeamento

Ao utilizar a nuvem, os dados podem ser organizados e mapeados, além de estarem todos em um mesmo ambiente. Isso facilita a localização e o acesso às informações quando o titular solicita uma ação como a exclusão ou portabilidade de seus dados.

Monitoramento

As clouds também ajudam a realizar monitoramentos nas informações de forma mais fácil, o que contribui para a verificação da conformidade das atividades de tratamento com a LGPD e para o reforço da segurança quando necessário.

Controle de acessos

Em conjunto à criptografia dos dados, o controle de acessos é outro ponto forte da nuvem. A partir dele, é possível definir os usuários que poderão acessar os dados e os tipos de permissão que terão, podendo restringi-los ou até bloqueá-los quando preciso.

Datasafer

Ferramentas de proteção avançadas

Boas clouds contam com ferramentas de segurança avançadas para evitar vazamentos de dados e ataques. Esse tipo de tecnologia normalmente tem um custo elevado e contratar uma nuvem pode ser uma boa alternativa para ter acesso a eles, garantindo uma proteção maior às informações.

Datasafer

Backups

A nuvem também pode ser uma ótima maneira de garantir a segurança de seus dados por meio do backup. Manter uma cópia de segurança das informações é uma excelente forma de salvaguardar os dados para eventuais usos ou em caso de acidentes, e as clouds podem tornar esse processo facilitado e adequá-lo à LGPD.

A LGPD estabelece uma série de prerrogativas que devem nortear o tratamento de dados. Realizar essas atividades conforme os parâmetros da legislação é imprescindível para as empresas, a fim de evitar punições e até a interrupção das ações.

A nuvem pode ser uma boa aliada nesse processo. Ao armazenar os dados ou sua cópia de segurança em clouds com bons níveis de proteção, fica mais fácil atender os requisitos de segurança necessários para adequar das operações da empresa.

Datasafer

Sobre a ArtBackup

A ArtBackup é uma **plataforma de backup em nuvem desenvolvida exclusivamente para provedores de serviços de Tecnologia da Informação** (TI) e Managed Service Providers (MSPs). O maior diferencial é o gerenciamento centralizado de clientes, por meio de um portal web e softwares de backup personalizados.

Os volumes são contratados sob demanda, e os data centers em que os dados são armazenados contam com certificação Tier III, atendendo os mais altos níveis de exigência de segurança e auditoria.

São oferecidas **mais de 80 horas de treinamentos gratuitos sobre conceitos de backup e segurança da informação**, além de **suporte especializado**, para acompanhamento da jornada de crescimento da empresa.

Datasafer

A plataforma ajuda a incluir o serviço de backup em nuvem no portfólio de consultorias de TI e MSPs, e conta com uma série de funções para automatizar a cópia dos dados dos clientes. Tudo isso priorizando a compressão, a segurança e a criptografia das informações.

A ArtBackup facilita ainda a geração de relatórios e permite administrar remotamente os agentes de backup, configurando e iniciando-os quando necessário. O processo de vendas também é facilitado, já que é possível criar contas free para que os clientes testem os serviços.

Saiba mais sobre a solução em nosso site e acompanhe-nos nas redes sociais!

Datasafer