



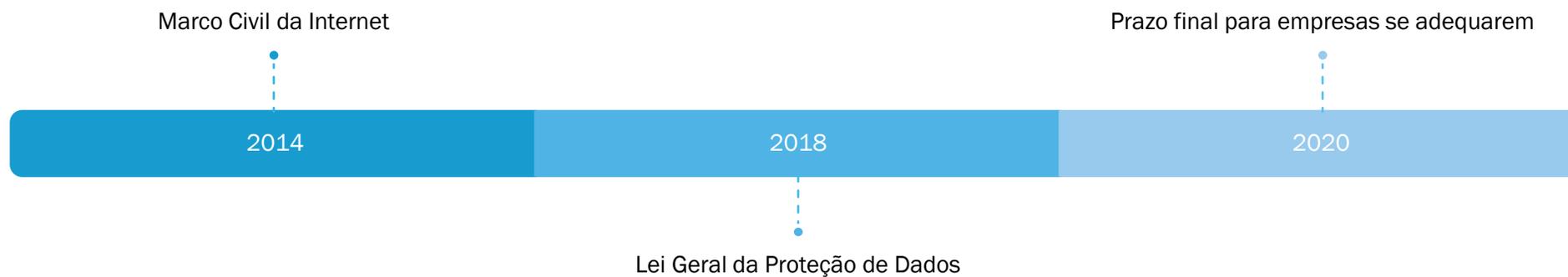
PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ENTENDA A IMPORTÂNCIA PARA SUA EMPRESA





POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – *TIMELINE*





POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Estamos vivendo uma completa mudança de cenário graças à [transformação digital](#) e a entrada de novas tecnologias dentro das empresas. Mas, se antes o foco quando o tema era segurança estava só na parte de infraestrutura e equipamentos, hoje em dia, é preciso contar com uma **política de segurança da informação, ou PSI**.
- E, com a criação no Brasil da [Lei Geral de Proteção de Dados \(LGPD\)](#), é cada vez mais urgente a criação de uma política de segurança da informação. Segundo a lei, as empresas precisam se adequar aos termos até 2020. E para quem não estiver em conformidade, as multas são bem altas.
- Na prática, essa política que deve ser documentada possui 3 principais pilares:
 - Categorização de dados;
 - Termos de privacidade dos dados;
 - Segurança da informação.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **O que é uma política de segurança da informação?**
- Uma política de segurança da informação **é um plano de ação que guia sua organização**, garantindo que seus dados e sua rede sejam protegidos contra possíveis ameaças de segurança e criando normas para acessos aos dados armazenados, principalmente relacionados aos clientes da sua empresa.
- Pense nessa política, que deve ser feita em forma de documento, como um elo entre seus colaboradores, processos internos, segurança e tecnologia. Quando uma violação de segurança acontecer, por exemplo, é muito provável que um dos termos estipulados na PSI falhou.
- Para garantir que você esteja efetivamente protegendo seus dados, é necessário que:
 - Normas técnicas funcionem para evitar violações;
 - Seja possível detectar possíveis ameaças;
 - Crie regras de acesso às informações;
 - Analise atividades suspeitas;
 - Forneça correção rápida no caso de problemas.
- Por isso, a política de segurança da informação deve ser informada a todos os seus times internos, abordando o que se espera deles e ajudando a educá-los em novos procedimentos de segurança que eles devem seguir.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Como começa a implementação da PSI na prática?**
- Essa política deve abranger uma variedade de atividades práticas, como:
 - Atualizar seus termos de privacidade;
 - Configuração das estações de trabalho da sua organização;
 - Atualização de login dos colaboradores;
 - Criação de novos procedimentos de acesso a dados.
- O primeiro passo, que é atualizar seus termos de privacidade, é essencial para deixar claro qual o nível de cada usuário (gerencial, administrativo, visitante), deixando todos cientes das práticas seguras de acesso e compartilhamento de dados para cada um desses níveis.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Por que a PSI é importante para minha empresa?**
- Sofrer uma violação de segurança é algo realmente caro para qualquer tipo de empresa. E pelas regras da LGPD, se houver vazamento indevido das informações pessoais de clientes, que deveriam ser protegidas de acordo com as políticas de privacidade, as [multas podem variar](#) entre R\$ 50 milhões e 2% do faturamento total da empresa.
- Com um alto nível de risco como esse, fica claro que ter uma política de segurança de da informação em vigor é essencial!
- Mas não é apenas esse lado financeiro que pesa nessa decisão de implementar a PSI. Aqui separamos mais **4 pontos que comprovam a importância desse documento na sua empresa.**
- **1. Ajuda você a melhorar a postura geral de segurança de sua organização**
- Isso significa que há menos incidentes de segurança quando as organizações usam o PSI, já que os problemas são evitados preventivamente.
- **2. Prepara melhor para ter os requisitos de auditoria e conformidade**
- Ao passar por um processo de fiscalização, fica muito mais fácil comprovar quais os protocolos e as normas de segurança utilizadas.
- **3. Melhora o nível de responsabilidade por parte dos usuários**
- As partes mais interessadas na segurança da sua organização são os clientes, que não querem ter seus dados expostos indevidamente. E usar a política de segurança da informação melhora o reconhecimento da sua empresa no mercado por conta desse quesito.
- **4. Fornece à sua organização uma estrutura sólida de segurança**
- Em torno da comunicação interna e externa, haverá sempre uma estratégia bem definida em termos de segurança, o que ajuda a manter uma estrutura sólida por trás das [informações corporativas](#).



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- 6 medidas para sua empresa se adequar à nova lei de proteção de dados
- Em agosto de 2018, o Brasil passou a fazer parte do grupo dos poucos países que contam com uma [legislação específica para proteger os dados](#) e a privacidade de seus cidadãos. Com isso, as organizações terão que mudar diversos processos referentes à coleta, armazenagem e eliminação dessas informações.
- O prazo para adequação à lei de proteção de dados vai até 2020. No entanto, é preciso começar desde já, visto que esse processo envolve mudanças profundas e quem não cumprir as novas normas poderá arcar com [multas pesadas](#).
- Confira a seguir 6 medidas para sua empresa se adequar à Lei Geral de Proteção de Dados (LGPD):
- **1. Realize uma análise**
- Comece consultando um especialista jurídico para entender todos os pontos da lei de proteção de dados e como eles podem afetar seu negócio. Então, olhe para os sistemas que você já possui e descubra onde existem pontos fracos e quais [tendências de segurança digital](#) podem ser aplicadas para saná-los.
- Além disso, revise como você obtém o consentimento para coletar dados e os mecanismos que utiliza para excluí-los.
- **2. Eduque toda a equipe**
- Os colaboradores devem ser instruídos sobre as responsabilidades que eles têm quando lidam com informações pessoais de funcionários, clientes, parceiros e contratados.
- Da mesma forma, é especialmente importante garantir que toda a equipe de gestores entenda por que a proteção das informações e as mudanças exigidas pela lei de proteção de dados precisam ser uma prioridade no [orçamento](#).
- **3. Procure um especialista**
- As empresas devem considerar a nomeação de uma empresa responsável pela adequação à lei de proteção de dados. Esses profissionais devem se encarregar de revisar as constantes mudanças na legislação que sejam pertinentes ao tema.
- Lembre-se que atender às exigências legais é uma abordagem contínua e não somente um evento pontual.
- Todas as empresas precisam identificar um ponto de contato principal que deve servir como suporte para todas as áreas que, de alguma forma, lidam com os dados de usuários da internet.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4. Categorize seus dados

- Determine quais dados da sua empresa são afetados pelas diretrizes dessa nova legislação. Por exemplo, informações de cidadãos brasileiros podem estar em contratos, documentos de RH, registros financeiros ou histórico de pedidos de compra.
- Veja onde esses dados estão armazenados, como são processados e quem tem acesso a eles. A partir daí, você pode definir políticas para toda a empresa sobre como essas informações devem ser manipuladas.

5. Revise sua Política de Privacidade

- Não se esqueça de revisar e atualizar sua Política de Privacidade atual. Este é o primeiro lugar que as pessoas procurarão para verificar se sua empresa está em conformidade com a lei de proteção de dados.
- Em sua política, você deve informar a base legal para o processamento dos dados, os períodos de retenção, o direito do cliente de revogar a permissão para o uso de suas informações e outras exigências previstas na lei.
- Além disso, você deve fornecer as informações em linguagem concisa, fácil de entender e clara.
- Não se esqueça que se a sua empresa processa dados de indivíduos menores de idade, você deve garantir a existência de procedimentos adequados para verificar as idades individuais e coletar o consentimento dos responsáveis, quando aplicável.

6. Invista em segurança da informação

- Com a lei de proteção de dados, as empresas passam a ser totalmente responsáveis pela segurança das informações que elas coletam, processam, transmitem e armazenam.
- Ou seja, além de investir na adequação às novas normas, é necessário que as empresas reforcem seus procedimentos de segurança dos dados. Caso contrário, elas poderão pagar multas que podem variar entre R\$ 50 milhões e 2% do faturamento total da empresa.
- Criar políticas internas de proteção de dados com nível de privilégios para acesso a sistemas e arquivos.
- Por isso, não corra riscos. Comece agora mesmo a implementar soluções que tornem sua atividade mais segura. Assim, você evita perder informações e dinheiro.
- A **LG3INFO** oferece uma [ampla gama de produtos e serviços](#) que visam à segurança dos seus dados. Você pode contar, por exemplo, com serviço de [gerenciamento de segurança](#), armazenamento em nuvem e muito mais.
- **Como o advento da lei de proteção de dados, a segurança das informações, mais do que nunca, deve ser um dos principais itens de preocupação das organizações.**