**PRIVACIDADE**

**DE DADOS**

*É um dos pilares da segurança da informação, e tem o objetivo de proteger a confidencialidade das informações de uma empresa e seus clientes. Na solução, deve-se definir os dados sensíveis que serão utilizados e descrever algumas atividades importantes que devem ser executadas, visando preservar esses dados e adequá-los à LGPD.*

Em nosso projeto não utilizaremos dados sensíveis, em vista de que a arquitetura desenvolvida trabalhará com dados de caráter aberto/público, ou seja, envolverá dados básicos referentes ao responsável de acesso/controle ao banco de dados, estações de monitoramento, e as demais medições da qualidade do ar advindos dos equipamentos IoT, dos quais não fazem parte do filtro que deve ser mantido em confidencialidade segundo a LGPD. Entretanto, temos ciência da importância de manter boas práticas com os dados sensíveis e quais condutas devem ser executadas para preservamos as informações, que serão descritas abaixo.

**DADOS SENSÍVEIS**

Após entrar em vigor em agosto de 2020, a Lei Geral de Proteção de Dados passou a regulamentar de forma mais clara como os dados do povo brasileiro podem e devem ser lidados. Com isso, informações mais pessoais passaram a ser consideradas como “dados sensíveis” pela LGPD, aumentando a restrição de seu uso.

É comum pensar que qualquer dado pessoal pode ser considerado como “sensível”, já que é algo totalmente direcionado ao indivíduo. Porém, números como RG, CPF e CNH, por exemplo, não fazem parte dessa lista. Mesmo assim, cada uma dessas informações segue regras definidas pela LGPD, garantindo a sua proteção e penalidade para quem utilizá-las sem o devido consentimento.

**Quando se trata especificamente de dados sensíveis, a**[**Lei Geral de Proteção de Dados**](https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd)**brasileira tem uma definição mais clara:**

“Os que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.”

**Para esclarecermos melhor**: Elisabete (nome fictício) tem o CPF de número 888.888.888-0, é cristã, de origem japonesa, vive na Bahia e gosta de música pop.

Nesse caso, o fato de ser cristã e de origem japonesa é o que seriam considerados “dados sensíveis” pelo LGPD.

Com isso em mente, conseguimos entender o motivo pelo qual devemos separar dados pessoais como um endereço de e-mail de algo ainda mais profundo, como uma etnia.

**Mas o que podemos fazer com dados sensíveis, segundo a** [**Lei Geral de Proteção de Dados**](https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd)**(LGPD)?**

O tratamento depende do consentimento explícito do (a) titular dos dados e para um fim definido. E, sem esse consentimento do (a) titular, a LGPD define que somente será possível quando a informação for indispensável em situações relacionadas a uma obrigação legal; políticas públicas; estudos via órgão de pesquisa; exercício regular de direitos; preservação da vida e da integridade física de uma pessoa; tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária e prevenção de fraudes contra o (a) titular.

Qualquer uso fora do descrito acima é considerado ilegal, sobretudo quando são usados para práticas de discriminação ilícita ou abusiva.

As penalidades para quem lidar ou divulgar com os dados sensíveis são variadas. Pode ser uma multa simples de até 2% do faturamento de uma empresa, com limite de até R$ 50 milhões, por exemplo. Porém, em casos mais graves, além da multa, pode ocorrer o bloqueio ou a eliminação dos dados pessoais relacionados, a suspensão do banco de dados e até mesmo a proibição parcial ou total da atividade da empresa ou do indivíduo.

Mas é preciso deixar claro que caso uma companhia deixar vazar os dados pessoais e sensíveis de uma pessoa, ela já estará vigente a receber punições, segundo a LGPD.

**Para proteger os dados sensíveis podemos executar algumas atividades importantes, tais como:**

**- Solicitar autorizações expressas**

Em toda coleta de dados para uso comercial, deve haver uma autorização expressa dada pelo titular. Então, a empresa precisa rever seus formulários de captação de dados e garantir que as explicações são claras e sem ambiguidades.

**- Usar criptografia**

A criptografia é uma das defesas de base para os dados sensíveis e, aliás, para quaisquer arquivos armazenados digitalmente. Quando está criptografado, o arquivo só pode ser lido se a máquina do usuário tiver a mesma chave utilizada no protocolo de proteção. Então, mesmo que haja invasões nos sistemas da empresa, os arquivos não poderão ser acessados. Sem a criptografia, informações confidenciais ficam bastante vulneráveis a ataques cibernéticos.

**- Exigir senhas seguras**

O uso de senhas é fundamental para criar mais uma barreira de segurança no acesso aos dados sensíveis. Porém, para que elas sejam efetivas, não podem ser facilmente descobertas. Por isso, deve ser exigido que todos os usuários criem senhas com um nível mínimo de segurança. Por exemplo:

- Conter números;

- Mesclar letras maiúsculas e minúsculas;

- Ter ao menos um símbolo;

- Evitar sequências numéricas;

- Não utilizar nome próprio ou data de aniversário.

**- Usar Redes Privadas Virtuais**

Os dados sensíveis de clientes, assim como outras informações confidenciais, precisam ser armazenados em redes privadas (VPN, na sigla em inglês), isto é, longe de sites com livre acesso ou de nuvens públicas. Nesses locais, usuários não autenticados não conseguem visualizar os dados, evitando assim o comprometimento à segurança da empresa.

**- Investir na educação dos colaboradores**

Além de todas essas medidas mais técnicas, é importante investir em uma cultura organizacional alinhada às práticas de proteção de dados sensíveis. Pode-se, por exemplo, estabelecer restrições de acesso por setores ou hierarquia, além de investir em orientações escritas e treinamentos.

**- Reforçar as estruturas de segurança de dados**

No contexto da era da informação, os dados valem ouro. Por isso, não só as informações sensíveis de clientes como quaisquer outros arquivos armazenados digitalmente pela empresa precisam ser tratadas com bastante atenção.

Então, além das medidas já citadas, é interessante revisar todo o sistema de segurança dos bancos de dados da empresa. Por exemplo, com um reforço na gestão de TI, investimento em tecnologias mais modernas e elaboração de planos de gerenciamento de riscos.

Além disso, a equipe de TI deve preparar procedimentos para lidar com crises. Isto é, em situações de vazamentos ou problemas de segurança. Para começar, vale a pena ter um bom sistema de identificação de invasões e de identificação de vazamentos, associado a um procedimento padrão eficiente de contenção dos ataques de hackers.

**- Ser proativo e não reativo (prevenir e não remediar)**

Prever e antecipar eventos que possam comprometer a privacidade antes que eles ocorram.

**- Privacidade como configuração padrão**

Por padrão, as configurações referentes à privacidade devem estar definidas considerando a máxima proteção possível da privacidade do usuário.

**- Funcionalidade total: “soma-positiva” em vez de soma-zero**

Esse princípio visa garantir a proteção de dados pessoais em consonância com os legítimos interesses e objetivos daqueles que utilizam as informações, sem a necessidade de se fazer trocas desnecessárias.

**- Segurança de ponta a ponta**

A segurança das informações pessoais deve ser garantida desde a coleta do dado até sua destruição ou seu compartilhamento com um terceiro.

**- Visibilidade e transparência**

Abrange diversos aspectos, como informar ao titular do dado quando e para qual finalidade as suas informações estão sendo coletadas até a abertura da plataforma.

**- SIEM (Security Information and Event Management)**

Gerencia e correlaciona eventos de segurança. Com a centralização e o correlacionamento dos eventos gerados por outras aplicações de segurança (antimalware, firewalls, proxies, IPS, entre outros), possibilita a identificação e resposta aos incidentes.

**- DLP/CASB (Data Loss Prevention / Cloud Access Security Broker)**

Ferramentas ou serviços que garantem a correta utilização, distribuição, transferência ou extração de dados armazenados internamente ou em nuvem.

**Bibliografia:**

<https://blog.qualitor.com.br/dados-sensiveis/>

<https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados>

<https://tecnoblog.net/responde/o-que-sao-dados-sensiveis-segundo-a-lgpd/#:~:text=Os%20dados%20sens%C3%ADveis%20s%C3%A3o%20os,vida%20sexual%20de%20uma%20pessoa>.