AMPLIANDO A CONSISTÊNCIA DO NEGÓCIO: LGPD

Luis Miguel - 565324

Adeilson Laureano - 566282

Carlos Eduardo de Sousa - 565094

Luan Antônio Gomes Pereira – 552638

Versão 1

SUMÁRIO

Sumário

LEI GERAL DA PROTEÇÃO DE DADOS

1 CONTEXTUALIZAÇÃO DO PAPEL DA TI EM RELAÇÃO À LGPD

1.1 Aplicação da LGPD nas tarefas da TI

Cabe à TI, mais especificamente o time de SI e Privacidade, desenvolver, implementar e monitorar controles técnicos e administrativos que garantam a confidencialidade, integridade e disponibilidade dos dados pessoais.

Na prática, a TI deve:

- Implementar políticas de acesso baseado em papéis (RBAC).
- Gerenciar logs e auditorias de acesso aos sistemas internos.
- Automatizar processos de consentimento e gestão de dados sensíveis.
- Garantir criptografia de dados em repouso e em trânsito.
- Controlar cópias de backup e sua retenção segura.

Com isso, a TI assegura que dados de colaboradores, registros de atendimento e controle de acessos sejam tratados com responsabilidade, mantendo a empresa em conformidade com a LGPD.

1.2 Aplicação da LGPD na plataforma de eCommerce

A TI deve garantir que o tratamento de dados dos consumidores ocorra conforme os princípios da LGPD: finalidade, adequação, necessidade, segurança e transparência.

Dentre as práticas recomendadas:

- Criptografia de dados pessoais e sensíveis (ex.: CPF, endereço, raça).
- Políticas claras de privacidade e consentimento expresso no uso do site.
- Uso de firewalls, WAFs (Web Application Firewall), DLP e testes de segurança (pentests).
- Implementação de autenticação multifator (MFA) para usuários administradores.

2 RECOMENDAÇÕES DE PROTEÇÃO AOS DADOS

2.1 Recomendação 1: Implementação do DLP – Data Loss Prevention e CASB – Cloud Access Security Broken

Descrição: Estabelecer ferramentas de monitoramento em tempo real como o DLP para envio de arquivos, mapeamento e bloqueio de URLs. Além disso, estabelecer uma ferramenta para gerenciar serviços de nuvem como o Exchange, OneDrive e SharePoint que encontra envio de dados para emails pessoais, compartilhamento via link, entre outros...

Benefícios:

- Reduz o risco de vazamentos acidentais.
- Controle total de tudo que entra e sai da empresa.
- Permite uma análise aprofundada do ambiente geral para melhorias.
- Facilita auditorias e investigações internas.
- Aumenta a conformidade com os princípios de necessidade e minimização da LGPD.

2.2 Recomendação 2: Implantação de criptografia ponta-a-ponta

Descrição: Adotar mecanismos de criptografia para proteger dados pessoais identificáveis e sensíveis, como CPF, raça, RG e Religião.

Benefícios:

- Garante a segurança dos dados mesmo em caso de vazamento ou acesso indevido.
- Reforça a conformidade com o artigo 46 da LGPD sobre segurança e proteção dos dados pessoais.
- Protege a reputação da empresa e fortalece a confiança do consumidor.

2.3 Recomendação 3: Implantação do Framework Empresarial TOGAF

Descrição: Adotar o framework TOGAF (The Open Group Architecture Framework) para estruturar e gerenciar a arquitetura corporativa da organização, alinhando tecnologia da informação aos objetivos estratégicos do negócio.

Benefícios:

- Estabelece uma visão clara e integrada da arquitetura de TI e dos processos de negócio.
- Facilita a tomada de decisões estratégicas com base em informações consolidadas e alinhadas à governança corporativa.
- Aumenta a eficiência na gestão de mudanças e na implementação de novas tecnologias.
- Contribui para a conformidade com boas práticas de governança e segurança da informação.

- Promove a padronização, reutilização de recursos e redução de custos operacionais.

2.4 Recomendação 4: Implantação Proteção de Rede

Descrição: Incluir mecanismos de proteção de dados trafegados pela rede como FireWall, VPN e SCP.

Benefícios:

- Bloqueia arquivos maliciosos que tentam trafegar pela rede corporativa.
- Ciptografa dados que saem e entram pela rede.
- Monitoramento em tempo real e total controle.

3 ANONIMIZAÇÃO

3.1 Definição de Dados para Anonimização

• Dado 1: CPF

Justificativa: O CPF é um dado altamente sensível e diretamente vinculável ao titular. Anonimizá-lo impede a identificação direta do cliente em análises e relatórios.

• Dado 2: Endereço IP

Justificativa: O IP pode ser usado para rastrear a localização e identificar padrões comportamentais. Anonimizá-lo é essencial para proteger a privacidade do usuário e reduzir riscos de profiling.

• Dados Sensíveis

Justificativa: Dados que remetem a raça, religião, opnião política, vida sexual ou saúde são extremamente sensíveis, uma vez que podem ser usados para discriminação e preconceito. Anonimizá-los é obrigatório.

REFERÊNCIAS

LAUDON, K. C.; LAUDON, J. P. Sistemas de Informação Gerenciais. São Paulo: Pearson, 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD.

FIAP. Fase 3 - Data Science: Capítulo 15 - LGPD - Lei Geral de Proteção de Dados. Disponível na plataforma FIAP.

FIAP. Fase 3 - Data Science: Capítulo 14 - LGPD - Lei Geral de Proteção de Dados. Disponível na plataforma FIAP.