GUIA ORIENTATIVO SOBRE SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

Em outubro de 2021, a **Autoridade Nacional de Segurança da Informação (ANPD) disponibilizou o "Guia Orientativo sobre segurança da informação para agentes de tratamento de pequeno porte"**, objetivando auxiliar as microempresas, empresas de pequeno porte, startups e empresas de inovação para a adequação aos termos da Lei Geral de Proteção de Dados (LGPD), no que se refere à segurança da informação e ao tratamento de dados pessoais, nos termos dos artigos 46, 47,48 e 49.

Vale ressaltar que a base para essa competência disposta à ANPD está prevista no artigo 55-J, XVIII, da LGPD, como se vê:

> **Art. 55-J. Compete à ANPD:**
>
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

Sendo assim, para que haja o desenvolvimento de um ambiente institucional mais seguro para as micro e pequenas empresas, com um olhar voltado ao desenvolvimento e adequação aos termos legais, os seguintes pontos deverão ser observados, também por estas: (i) a segurança da informação relacionada aos dados pessoais; (ii) obrigações da LGPD.

- Segurança da Informação: tendo como elemento basilar a preservação da confidencialidade, integridade e disponibilidade da informação, a segurança da informação é pautada no gerenciamento de riscos, garantindo um equilíbrio eficiente entre os ganhos da empresa e a minimização de vulnerabilidades e perdas, de modo a prevenir, detectar e combater as ameaças digitais.

- Obrigações da LGPD sobre a segurança da informação a dados pessoais: quanto às obrigações da LGPD, é importante que haja um olhar direcionado ao Princípio da Segurança, previsto no artigo 6º, VII, desta Lei, juntamente aos artigos 46 a 49 que definem sobre as medidas de segurança, técnicas e administrativas de proteção dos dados pessoais; a necessidade de garantia de segurança pelos agentes de tratamento; as obrigações do controlador quanto à comunicação sobre eventuais incidentes que gerem riscos aos titulares dos dados; e a estruturação adequada dos sistemas de tratamento de dados pessoais, sempre atrelados aos requisitos de segurança, boas práticas e governança.

Assim, diante dos requisitos elencados pela LGPD, da complexidade para a implementação para agentes de tratamento de pequeno porte, e verificada a eventual necessidade de um elevado investimento para a adequação, o que poderia conferir um risco para os agentes de tratamento de pequeno porte, o guia apresentou as seguintes sugestões de boas práticas corporativas:

1 Medidas Administrativas

1.1. Política de Segurança da Informação (PSI): essa política é incentivada pela ANPD por evidenciar boa-fé e diligência na segurança de todos os dados pessoais sob custódia dos agentes de tratamento. Nesse viés, a sugestão para a implementação da PSI pode ser exemplificada pelo uso de senhas; cópias de segurança; acesso à informação; compartilhamento de dados; atualização de softwares; uso de antivírus etc.

1.2. Conscientização e treinamento: a informação e sensibilização da equipe responsável pela

gestão do tratamento de dados configura-se como elemento basilar para o sucesso no que se refere à segurança da informação e à proteção de dados pessoais. Assim, dentre as medidas elencadas no guia, destacam-se: (i) orientação sobre como evitar incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, os quais podem ocorrer ao clicar em links desconhecidos; (ii) a preservação de documentos em ambientes seguros, como gavetas ou armários trancados; (iii) não compartilhamento de logins e senhas relacionados ao trabalho; (iv) bloqueio de computadores após o uso; (v) incentivo à comunicação sobre os incidentes e vulnerabilidades detectadas.

1.3. Gerenciamento de Contratos: primeiramente, como medida de segurança contra abusos de privilégio, é recomendável a elaboração de termos de confidencialidade, os quais devem ser assinados pelos funcionários da empresa em prol da não divulgação de informações confidenciais que envolvam dados pessoais. Junto a isso, no caso de terceirização de serviços de TI, é importante que exista um contrato com cláusulas de segurança da informação, a exemplo de regras sobre compartilhamento, regras para fornecedores e parceiros, relações entre controlador-operado, vedação a tratamentos incompatíveis com as orientações do controlador.

2 Medidas Técnicas

2.1. Controle de acesso: consistindo em processos de autenticação, autorização e auditoria, o controle de acesso garante que determinados dados só possam ser acessados por pessoas autorizadas. Nesse ponto, a ANPD sugere que seja implementado um sistema de controle de acesso aplicado a todos os usuários, com níveis de permissões diferenciados na proporção da necessidade de cada funcionário, além do uso de senhas não padronizadas, proibição do compartilhamento de contas e o uso de autenticação multi-fatores (MFA).
2.2. Segurança dos dados armazenados: com observância ao princípio da necessidade previsto no artigo 6º, III, da LGPD, é importante que os agentes de tratamento de pequeno porte coletem e processem apenas os dados pessoais estritamente necessários para o cumprimento de seus objetivos, vez que o armazenamento sem utilidade concreta não representa uma prática

adequada, considerando o princípio da finalidade dessa mesma lei.

Ademais, no que se refere ao tratamento de dados sensíveis, diante da proteção especial prevista na legislação, é de suma importância que haja a implementação de soluções que não permitam a identificação do titular, a exemplo da criptografia.

Dentre outras medidas de segurança, destacam-se: (i) evitar a transferência de dados pessoais para dispositivos de armazenamento externo; (ii) realização de backups regularmente; (iii) formatação de dados anteriormente ao descarte ou destruição física; (iv) contrato de serviço com cláusulas de registro de destruição para empresas que utilizam serviços de terceiros para o descarte.

2.3. Segurança das comunicações: para o estabelecimento de uma comunicação segura, constituem ferramentas eficazes a utilização de conexões cifradas (com uso de TLS/HTTPS) ou aplicativas com criptografia de ponta a ponta. Junto a isso, o tráfego de rede gerenciado e a remoção de dados sensíveis que estejam desnecessariamente em redes públicas, também representam importantes observações.

2.4. Manutenção de programa de gerenciamento de vulnerabilidades: a atualização constante dos sistemas utilizados representa uma medida adicional de segurança, juntamente com a adoção de softwares antivírus e antimalwares.

3 Medidas relacionadas ao uso de dispositivo móvel

Sempre que possível, é recomendável que os agentes de tratamento de pequeno porte façam uma separação entre os dispositivos móveis de uso privado daqueles de uso institucional, tendo em vista a maior vulnerabilidade que os primeiros podem apresentar. Além disso, a implementação de ferramentas que permitam o apagamento remoto dos dados pessoais relacionados à atividade, constitui outra medida eficaz para a proteção da empresa.

4 Medidas relacionadas ao serviço em nuvem

Consistindo em serviços de computação relacionados a servidores, armazenamento, banco de dados, rede, software, análise e inteligência pela internet, a nuvem configura-se como uma alternativa para a segurança dos dados armazenados, sugerindo ao agente de tratamento a realização de um contrato de acordo com o nível de serviço, juntamente ao uso de técnicas de autenticação multi fator em todos os acessos relacionados a dados pessoais.

Você sentiu falta de algum tema ou quer conversar melhor sobre essas mudanças?

Entre em contato agora mesmo com a nossa área de Direito Digital!

www.moraisandrade.com
55 + 11 5555-6128
direitodigital@moraisandrade.com
linkedin.com/company/morais-andrade-advogados/
Al. Casa Branca, 35, 10º andar - cj. 1006/1009 - Jardim Paulista
Cep: 01408-001 - São Paulo - SP