Ajustes propostos para a Política de Backup

Av. Ministro Geraldo Barreto, 2100, sala 1506
Jardins - Aracaju/SE - CEP: 49.026-010
contato@grupoadx.com.br
+55 79 3013-4140

Sumário

I – Do Objeto da Análise.

Visando adequar a Política de Backup atualmente vigente no SENAC-AL às melhores práticas do mercado e à LGPD, serão propostas melhorias na operação do backup e no documento "09_Procedimento de Backup.docx"

II – A Lei Geral de Proteção de Dados – Lei 13.709/18.

Antes de adentrar a necessidade da adequação do documento, cabe tecer breves comentários sobre a lei de proteção de dados e o que traz a sua importância para a aplicação nas relações jurídicas que tratam de dados pessoais.

A Lei Geral de Proteção de Dados (Lei nº. 13.709/18), traz no seu **artigo 5º** os conceitos dos termos utilizados no tratamento de dados e, dentre eles, os principais para entender a base de tratamento é o conhecimento dos significados de dado pessoal: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável"; ou mesmo dado pessoal sensível: "dado pessoal sensível: dado pessoal sobre 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".

A lei de proteção de dados ainda prevê em seu **artigo 6º** princípios que devem ser observados no tratamento de dados pessoais, dentre eles os princípios da boa-fé, da finalidade, da adequação, da necessidade, da segurança e da transparência em relação a qualquer forma de utilização dos dados pessoais.

Além da observância aos princípios, a lei prevê que qualquer tratamento de dado pessoal deve ter requisitos que justifiquem a coleta dos dados para a finalidade que pretende alcançar. Dessa forma, no **artigo 7º e 11** da lei constam as bases legais que justificarão o tratamento para dados pessoais e dados pessoais sensíveis, respectivamente. Acrescenta-se ainda que o **artigo 14** dispõe sobre o tratamento de dados pessoais de crianças e adolescentes, com os devidos deveres a serem observados pelo agente de tratamento dos dados pessoais coletados.

É imprescindível observar também o **artigo 18** do LGPD, que traz os direitos dos titulares dos dados pessoais, bem como deveres a serem cumpridos pela pessoa que tratará os dados.

Os **artigos 23 a 30** se referem ao tratamento de dados pessoais pelo Poder Público, o que deve ser observado em razão das especificações quanto às condições que envolver os agentes públicos.

Os **artigos 37 a 40** dispõem sobre os agentes de tratamento, sempre necessário o entendimento para traçar as relações jurídicas nos contratos entre empresa e empregados e entre empresa e colaboradores/fornecedores, afinal definirá as reponsabilidades de cada agente pelo uso de dados pessoais coletados para cada finalidade jurídica contratual.

Ponto importante da lei é definir quem terá o papel de encarregado de proteção de dados, cuja definição legal se dá no **artigo 5º, VIII**: "pessoa indicada pelo controlador e operador para atuar como canal de

comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)", dispondo o **artigo 41** sobre suas funções.

Ademais, é dever da empresa a que se dirige este parecer a segurança de todas as informações coletadas a título de dados pessoais, devendo manter um programa de adequação à lei a fim de estar em conformidade, buscando boas práticas de segurança e governança de dados a fim de prevenir e mitigar os incidentes de segurança relacionados ao vazamento de informações, evitando ou diminuindo suas responsabilidades e sanções administrativas e/ou jurídicas.

III – Da necessidade de adequação da política de backup à LGPD.

De forma geral os itens a serem ajustados no documento são os seguintes:

- Adicionar referência à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, destacando que todos os colaboradores, parceiros e fornecedores tem obrigação de cumprir os seus requisitos;
- Adicionar ao documento uma referência à Política de Privacidade Interna e que descreve todos os dados pessoais coletados dos colaboradores, estagiários ou menores aprendizes, as suas finalidades, com quem os dados são compartilhados, seus períodos de retenção etc.;
- Incluir cláusula indicando um encarregado de proteção de dados, assim como explicando sua função, e como este poderá ser localizado;
- Incluir cláusula informando a finalidade e a necessidade dos dados pessoais que possam ser coletados nos procedimentos de backup.

IV. Análise técnica da Política de Backup

Foi realizada uma auditoria no documento que compõem a política de backup, segundo melhores práticas do mercado e alguns pontos precisam ser ajustados. São eles:

- Cabem aos administradores preverem a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias. A frequência desses testes deve estar registrada no documento;
- A administração dos backups deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento. É interessante ter um anexo descrevendo os tempos de execução de cada job de backup para monitoramento continuo das janelas;

- Os dispositivos de armazenamentos deverão ser protegidos em cofre anti-incêndio, anti-impacto e com controle de umidade, em localidade diversa da origem dos dados (backup off-site/ backup na nuvem). Os dados que serão transportados ao backup off-site deverão estar criptografados;

- Os dispositivos de armazenamento defeituosos ou inservíveis devem ser encaminhados para incineração, destruição física, procedimentos de sobrescrita de dados (low level format) ou outro procedimento que impossibilite a recuperação dos dados por terceiros;

- As solicitações de restauração de arquivos deverão ser comunicadas ao setor de TI formalmente por e-mail ou via Service Desk, informando os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso;

- Uma vez desenvolvida, implantada e documentada, a política de backup deve ser amplamente divulgada e disponibilizada em local de fácil acesso a todos os envolvidos no processo de backup e, também, àqueles que podem porventura necessitar fazer solicitações de dados armazenados nos backups;

- Os logs de backups devem ser analisados ao final de cada Job para garantir a inexistência de falhas e integridade do backup. É importante ter o registro do nome do operador que realizou o procedimento com a data e hora do teste;

- O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore. Os tempos médios de restore devem ser registrados em um anexo da política;

- AS rotinas de backup deverão ser atualizadas quando houver:
    - I – Novas aplicações ou sistemas forem desenvolvidas ou instaladas;
    - II – Novos locais de armazenamento de dados ou arquivos forem criados;
    - III – Novas instalações de bancos de dados;
    - IV – Outras informações que necessitem de proteção através de backups deverão ser informadas e avaliadas pelo administrador de backup.
- Quaisquer procedimentos programados nos equipamentos computacionais, físicos ou virtuais, e que impliquem riscos de funcionamento com interrupção dos sistemas e serviços essenciais da empresa somente deverão ser executados após a realização do backup dos seus dados. Em casos excepcionais em que a urgência justifique, desde que autorizados e avaliados os impactos pelo Gerente de TI, os procedimentos mencionados poderão ser executados sem a realização de backup;
- O descarte de qualquer mídia inservível ou inutilizável, caso utilizada na realização dos backups, deverá ser realizado de forma a garantir sua total destruição, impedindo sua reutilização ou acesso indevido por pessoas não autorizadas;

- É recomendada a implementação da regra de backup 3-2-1, ou seja, manter 3 cópias dos dados, sendo que dessas cópias 2 devem ser armazenadas em locais diferentes, e um desses locais deve ser off-site. Os detalhes da regra estão a seguir:
    - Crie três cópias distintas dos dados (1 cópia da produção e 2 cópias para backups).
    - Essas cópias devem ser armazenadas em dispositivos fisicamente independentes sem sincronização de dados cruzados, nem acesso de qualquer tipo. Ex.: uma cópia colocada em um disco rígido interno e a segunda armazenada em uma unidade HD externo ou unidade de fita.
    - A terceira e última parte da regra de backup 3-2-1 é que pelo menos uma cópia dos seus dados exista em um local externo, o que significa que está fisicamente localizado em um local diferente das outras cópias. Portanto, se duas cópias dos dados estiverem armazenadas na rede interna da Casa Vieira (uma em um servidor de produção e a outra em um disco rígido externo, por exemplo), recomendamos o armazenamento da terceira cópia em um site diferente – como outro escritório ou em um data center baseado em nuvem.

V - Conclusão

A política de Backup enviada pelo cliente foi analisada à luz dos requisitos da LGPD e de acordo com as melhores práticas de segurança da informação do mercado. Após a realização dos ajustes propostos no documento e na operação de backup, a empresa alcançará um maior nível de maturidade de segurança da informação e proteção de dados.

Av. Ministro Geraldo Barreto, 2100, sala 1506
Jardins - Aracaju/SE - CEP: 49.026-010

contato@grupoadx.com.br

+55 (79) 3013-4140