SAGRES
POLÍTICA E GESTÃO ESTRATÉGICA APLICADAS

Comitê LGPD
Maria Verônica Korilio Campos
Jacintho Mendes Lopes Júnior
Artur Reis de Souza
Humberto de Sá Garay
José do Carmo Ferreira
José Osmar Monte
Rafael Romualdo Clarindo Silva
Juliane Michelle Marucci Lopes
Adrian Nicolaiev Pereira dos Santos

Adequação das Organizações à LGPD baseada na Governança Corporativa

Com os riscos de multas, prejuízo da imagem institucional, do bloqueio, dos vazamentos e da destruição de dados pessoais, a entrada em vigor da Lei nº **13.709, de 14 agosto de 2018,** Lei Geral de Proteção de Dados Pessoais (LGPD), mesmo que postergada, causa uma enorme expectativa, uma vez que a grande maioria das empresas ainda não se adequou a essas novas exigências legais.

A expectativa aumenta em razão do pouco tempo disponível até a entrada em vigor da nova lei, prevista para agosto de 2020, aliada à incerteza causada pelo fato de a Autoridade Nacional de Proteção de Dados, ANPD, ainda não ter entrado em funcionamento, resultando na falta das regulamentações mandatórias e por conseguinte, gerando insegurança em relação às mudanças que serão provocadas.

Embora exista quem diga que a nova lei não irá ter a força necessária para produzir seus efeitos e/ou será adiada, é importante que todas as organizações se preparem para o cenário mais difícil, com a entrada da lei em vigor na data prevista. Mesmo em cenários onde a aplicação desta lei seja adiada, ainda há que se considerar a atuação do Ministério Público, que, baseado no Código de Defesa do Consumidor, já autuou várias organizações que desrespeitaram os princípios da LGPD.

O Instituto SAGRES tem analisado as melhores práticas ligadas ao tema, aprimorando-as para melhor executar o processo de adequação a essa Lei e parte desse aprendizado está hoje contemplado no presente trabalho.

POR ONDE COMEÇAR?

As normas ISO (tanto a 27.001 quanto a 31.000) demandam que haja o comprometimento da alta gestão, principalmente com a elaboração das diretrizes da organização, a fim de se ter, não apenas a participação desses atores (sócios, acionistas, conselho administrativo, diretores, etc.), como também seu envolvimento, sua visão e suas sugestões e propostas para a definição dos rumos que a organização deverá seguir, em consonância com o planejamento estratégico.

Daí derivam as diversas políticas institucionais, dentre as quais se destacam a de Segurança da Informação, de *Compliance* e a de Gestão de Riscos, que orientam grande parte do processo de adequação das organizações. Com essas políticas, vale observar como podem ser atendidos os princípios da Governança Corporativa em relação ao uso de dados, aplicando a LGPD:

- A utilização dos dados pessoais deve ser *transparente* e estar sempre disponível aos seus respectivos proprietários.
- O tratamento dos dados pessoais deve ser feito de forma a preservar a *equidade* das pessoas em relação aos seus direitos. Apesar de haver o respeito à equidade em relação aos direitos, tal não ocorrerá em relação ao acesso a dados ou funcionalidades em função do perfil utilizado pelos usuários de um sistema, no qual diferentes perfis poderão ter diferentes acessos a funcionalidades ou dados.
- A *prestação de contas* alusiva aos tratamentos realizados será sempre registrada e deve estar permanentemente disponível.
- A organização se *responsabiliza* pela correta utilização dos dados pessoais por ela coletados, pela sua segurança e por suas atualizações

Certamente, aspectos como comportamento dos funcionários, fornecedores, clientes e outros *stakeholders* ou até a arquitetura dos contratos serão abordados em um Programa de *Compliance* sempre revisado com

base em *checklists* específicos, a fim de se alinhar com o novo diploma legal.

Por se tratar de uma mudança de legislação, haverá também a necessidade de um plano de ação específico para se adequar os modelos de contratos e se negociar a revisão dos contratos e termos de uso e/ou privacidade vigentes, a fim de ajustá-los ao novo arcabouço legal. Outro aspecto importante é uma análise das leis e normas específicas de cada ramo de negócio em relação à LGPD, principalmente no que se refere a todo o tratamento de dados pessoais.

Essas mudanças afetam as pessoas que compõem grupos e que possuem uma cultura específica dentro da organização, demandando também um esforço para ajuste dos hábitos de trabalho e das próprias crenças e valores, tudo isto a fim de se minimizar os riscos inerentes à adaptação à LGPD.

Seguindo a orientação lógica, chega-se a Organização, Sistemas e Métodos, uma área clássica da ciência da Administração a qual preocupa-se com a análise e desenvolvimento de sistemas e lidam com um conjunto de técnicas cujo objetivo principal é de ajustar e aperfeiçoar o funcionamento das organizações. Por exemplo, *in case*, adequar à LGPD os processos, sistemas organizacionais, instalações e o tratamento de dados (tanto físicos quanto digitais nos diversos formatos), abordados na Política de Segurança da Informação, que, por sua vez, receberão tratamento minucioso junto aos níveis Tático e Operacional das organizações, aplicando-se *checklists* específicos como instrumentos de controle e avaliação.

A aplicação de *checklists* baseados em perguntas ajuda a se trabalhar os diversos aspectos a serem observados e selecionados para tratamento posterior, se houver necessidade.

O levantamento de todas as necessidades de ajustes compõe o Diagnóstico da organização, uma vez que permite observar os seus pontos fracos em relação à privacidade e à proteção de dados, que constituem parte das oportunidades de melhoria, viabilizando um *marketing* em relação ao respeito à comunidade (principalmente clientes e fornecedores).

Fig. 1 - Diagnóstico

O relacionamento entre os pontos fracos e as possíveis ameaças (aspecto que demanda uma análise à luz da doutrina de Inteligência) permite identificar os riscos inerentes a cada vulnerabilidade.

O diagnóstico oferece uma visão sobre os diversos pontos frágeis, que podem extrapolar, em muito, as possibilidades da organização, principalmente em relação às de pequeno e médio porte, tornando necessário haver uma priorização para sequenciamento das soluções.

COMO MELHORAR?

Considerando-se que normalmente os meios necessários à adequação são limitados, recomenda-se a aplicação de métodos multicritérios para a priorização de toda a lista de vulnerabilidades. É essencial que, mesmo indiretamente, os riscos, tanto os que se referem aos pontos fracos quanto às implementações das correções, sejam considerados, com vistas a se elaborar ajustes iterativos, concentrando-se inicialmente nas vulnerabilidades que mais afetam a segurança dos dados tratados e ensejem sanções. É importante ressaltar e ter conscientização de que, por melhores que sejam os recursos e implementações utilizados na gestão dos riscos, estas iniciativas nunca resultarão em 100% de segurança, o que significa existir sempre um risco residual que deverá ser coerente com o apetite da organização.

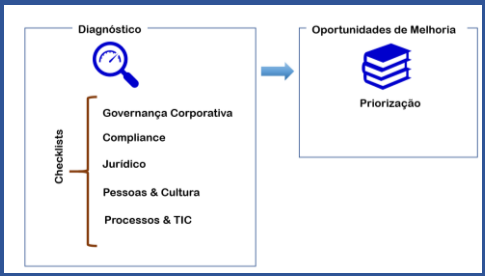

Fig. 2 – Obtenção das Oportunidades de Melhoria

O processo de adequação, por sua vez, deve ser feito iterativamente, com planejamento, selecionando-se um grupo de vulnerabilidades a serem tratadas e implementando as correções necessárias, as quais devem ser auditadas internamente, durante o encerramento da iteração. Caso alguma adaptação ainda demande uma correção apontada pela auditoria, esta deve constar da lista da iteração seguinte.

Recomenda-se que, no encerramento da última iteração, haja uma auditoria externa a fim de assegurar que todas as operações tenham sido realizadas em conformidade com a legislação, minimizando-se os riscos de sanções ou de inconvenientes para a imagem da organização, decorrentes de violações ou vazamentos de dados.

A identificação de novas correções a serem realizadas pode dar ensejo a novas iterações, demonstrando que o resultado que não é estático.

O processo de adequação se torna infinito, considerando-se a dinâmica das normas e das leis, e ainda, a evolução das tecnologias, processos e do ambiente, incluindo-se novas ameaças. Apesar de poder haver grande queda na frequência com que as iterações ocorram, elas se tornarão fundamentais quando houver um incidente de violação ou vazamento de dados ou mesmo que surja a percepção de um risco desse gênero.

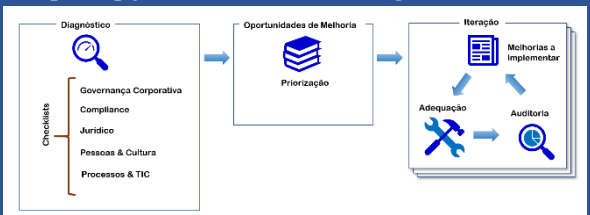

Fig. 3 – Visão Geral do Método Proposto

Sempre que aplicável, as melhorias a implementar deverão ter subfases de Governança Corporativa, Compliance, Jurídico, Pessoas & Cultura e Processos & TIC, atentando-se para a importância de se planejar a implementação de forma integrada, e utilizando, sempre que possível, a Governança Corporativa como base, a fim de que os esforços aplicados sejam compatíveis e as ações, mesmo que em paralelo (quando recomendável), sejam sempre sinérgicas e complementares, conforme a ilustra a Fig. 4.

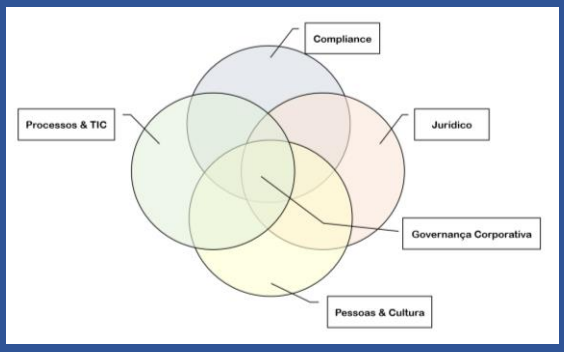

Fig. 4 – Integração das melhorias a serem implantadas

O presente ensaio mostrou que a adequação à LGPD é um processo exigente, multidisciplinar, envolvendo, desde a cultura organizacional até os diversos fatores técnicos, todos orientados pela Governança Corporativa e que pode ser sintetizado numa figura, onde cada aspecto é uma coluna que sustenta e é integrada pela Governança Corporativa.

Fig. 5 -Visão Geral do Processo de Adequação

Em conclusão, foi mostrado que a Governança Corporativa se apresenta como uma base fundamental para o processo de adequação à LGPD, ressaltando-se que qualquer caminhada segura na direção correta começa já no primeiro passo.

Os autores agradecem ao Sr. Walfrido Brito as sugestões recebidas para a elaboração deste ensaio.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Associação Brasileira de Normas Técnicas. *Gestão de Riscos – Diretrizes – ISO 31.000: 2018*. São Paulo: ABNT, 2018.

BRASIL. Associação Brasileira de Normas Técnicas. *Sistemas de Gestão de Segurança da Informação – Requisitos – ISO 27.001: 2013*. São Paulo: ABNT, 2013.

BRASIL. Associação Brasileira de Normas Técnicas. *Sistemas de Gestão de Compliance — ISO 19.600: 2014*. São Paulo: ABNT, 2014.

BRASIL. Instituto Brasileiro de Governança Corporativa. *Código das Melhores Práticas em Governança Corporativa*. São Paulo: IBGC, 2015. 5. ed.

BRASIL. Presidência da República. Lei 13.709, de 14 de agosto de 2018*Lei Geral de Proteção de Dados Pessoais (LGPD)*.. Brasília: Casa Civil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jul. 2019.

BRASIL. Presidência da República. Lei 13.853, de 08 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Brasília: Casa Civil, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm. Acesso em: 01 ago. 2019.