Pela Comissão Regional Leste de Governança e Riscos

“Pior que não ter controles, é pensar que os tem”. Esta expressão, cujo devido crédito ao autor ficaremos devendo nesta edição, revela a importância do constante monitoramento de todas as ações administrativas tomadas para tornar o dia-a-dia de nossas entidades mais produtivo e seguro.

Uma falsa sensação de segurança com relação ao ambiente de controle resulta em negligência, retardando inexoravelmente a percepção do desastre iminente. É a causa de surpresas desagradáveis e inexplicáveis na gestão de qualquer organização.

Quando mencionamos surpresas desagradáveis e inexplicáveis, estamos nos referindo a danos reputacionais significativos e prolongados, custos de reparação, sanções regulatórias, paralisação de atividades decorrentes de perda de dados, dentre outras consequências que podem transformar a gestão em um verdadeiro pesadelo.

A verificação de conformidade, portanto, é uma atividade imprescindível à manutenção de ambientes de controle eficazes nas organizações, como bem recomendam padrões de boas práticas como o COSO e tantos outros.

Afinal de contas, de nada adianta implantarmos todas – ou boa parte – das ações que vimos sugerindo em edições anteriores de nossos “Saiba Como” se, em contrapartida, não criamos mecanismo de verificação permanentes do seu cumprimento e, quando necessário, de sua revisão para aprimoramento.

Por isso, deixamos – at last but not least – os processos de compliance para a última edição de nosso informativo periódico, lembrando que são implementados para atender tanto a requisitos internos quanto externos.

E como aperitivo, recomendamos acessar o site do Serviço Bloomberg Professional e conhecer os cinco mandamentos de compliance para evitar o pesadelo a que nos referimos. Isto nos faz lembrar, diga-se de passagem, o mais emblemático lema dos jovens escoteiros.

Mandamento nº 1 – Não negligencie o comportamento humano.

O fator humano é um dos quatro fatores de ignição de riscos nas organizações. E um dos mais presentes em nosso segmento. Segundo a Bloomberg, “as violações de segurança cibernética nem sempre são obra de indivíduos nefastos orquestrando um ataque sofisticado … podem resultar de erro humano não intencional.”

Mandamento nº 2 – Priorize a segregação de funções.

A Bloomberg ressalta que “assim como funções e responsabilidades bem definidas são a base de organizações bem administradas, a segregação de funções (SoD, na sigla em inglês) é um componente importante da proteção contra a perda de dados e do gerenciamento de riscos de segurança cibernética.”

Mandamento nº 3 – Utilize autorização e autenticação.

A autenticação é de grande importância. No entanto, a Bloomberg alerta que “embora a autenticação de dois fatores tenha se tornado padrão, ela não elimina os riscos de segurança; por exemplo, os ‘hackers’ podem interceptar códigos enviados para dispositivos móveis. Para levar a segurança um passo adiante, o sistema de autenticação multifator permite que administradores e usuários autorizados realizem acessos com segurança.”

Mandamento nº 4 – Conheça seus dados.

De acordo com a Bloomberg, “a computação em nuvem revolucionou a forma como as empresas coletam, analisam e armazenam dados, mas implica em considerações de risco adicionais. Praticamente todos os fornecedores têm algum tipo de presença na nuvem, cada um com seus próprios pontos fracos e riscos.” Portanto, há muitos fatores de riscos relacionados com fornecedores, com destaque para o modo como os dados são hospedados e protegidos. Due diligences tornam-se fundamentais nessa hora.

Mandamento nº 5 – Aplique uma abordagem minimalista à retenção de dados.

Este mandamento nos remete ao conceito “Privacy by Default”, observado no tratamento de dados pessoais pelos seguidores da L.G.P.D. De acordo com a Bloomberg, “tão importante quanto proteger os dados de sua empresa é saber quando é a hora de eliminá-los. Uma estrutura de dados e segurança cibernética deve abranger uma política de retenção de dados que defina claramente quais dados devem ser armazenados e por quanto tempo”.

E então? Seus procedimentos de compliance monitoram esses cinco mandamentos com o “estado de alerta” típico dos escoteiros? Pois é... como mencionamos, isto é apenas um aperitivo. Vejamos como frameworks de boas práticas podem auxiliar – não limitando-se a – na montagem de um programa de compliance.

1 Identificação da Legislação Aplicável e de Requisitos Contratuais	Começar pela identificação de quaisquer sanções legais potenciais que possam resultar de algumas obrigações omitidas, relativas ao tratamento de dados pessoais ou de contratos, para aplicação de programa de verificação.
2 Proteção de Registros	Realizar análise crítica de políticas e de procedimentos atuais e históricos (ex. situações em que possa haver litígio ou autuação de órgãos de supervisão). Isto pode implicar na retenção de versões anteriores de documentos, quando eles são atualizados.
3 Análise Crítica da Segurança da Informação	Verificar evidências de que a segurança de informação está implementada e é operada de acordo com as práticas e as políticas da organização.
4 Análise Crítica Técnica	Aplicar métodos de análise crítica das ferramentas e componentes relacionados ao tratamento de dados pessoais e de segurança da informação.
5 Inventários de Softwares	Verificar se a lista de todos os softwares autorizados e necessários à empresa, para qualquer finalidade em todos os sistemas, encontra-se atualizada e abrangente.
6 Inventários de Hardwares	Idem, tópico anterior, com relação a equipamentos.
7 Suporte de Softwares	Verificar as condições de suporte de aplicativos, sistemas operacionais e softwares em geral por parte dos fornecedores.
8 Ferramentas de Verificação de Vulnerabilidades	Verificar se as ferramentas de testes de vulnerabilidade estão sendo aplicadas para todos os sistemas nas redes da organização e na frequência estabelecida nos normativos internos.
9 Comunicação e Registro de Incidentes	Verificar se os incidentes de segurança estão sendo reportados e devidamente registrados,

	com as oportunidades de melhoria sendo aplicadas em decorrência desses incidentes.
10 Segregação de Funções	Verificar se a Matriz de Criticidade (ou matriz SoD) está sendo devidamente atualizada e cumprida.

Com isso, chegamos, enfim, à nossa última edição da série de informativos intitulada “Saiba Como”, voltada a prevenção de crimes cibernéticos, acreditando termos contribuído para a mitigação desse risco operacional de grande impacto na gestão das entidades fechadas de previdência complementar.

*** Parte VIII**

Notas

(1) Committee of Sponsoring Organizations of the Treadway Comimission – iniciativa conjunta de cinco organizações profissionais dedicada a ajudar no desempenho das organizações através do desenvolvimento de liderança inovadora que aprimora o controle interno, o gerenciamento de riscos, a governança e a prevenção de fraudes.

(2) https://www.bloomberg.com.br/blog/seguranca-cibernetica-5-mandamentos-para-compliance/

Fonte: Abrapp em Foco, em 26.05.2022.