Elaborado pela Comissão Regional Leste de Governança e Riscos da Abrapp

Os investigadores de acidentes aéreos utilizam uma expressão muito chocante, mas bem apropriada, que revela a importância que o setor da aviação civil e militar atribui à documentação dos processos de segurança de fabricação, manutenção e uso das aeronaves, assim como do controle do tráfego aéreo: – "**Regulamento Se Escreve Com Sangue**"[**1**]. De fato, o aprendizado obtido com falhas ocorridas tem um valor inestimável para o estabelecimento de melhores práticas e consequente aprimoramento contínuo dos processos praticados em qualquer área do conhecimento humano.

Em nossa publicação anterior, buscamos conscientizar as EFPC acerca da importância da realização de diagnóstico de suas áreas de tecnologia para conhecimento do nível de aderência de seus processos às melhores práticas de prevenção a ameaças cibernéticas. Como passo seguinte, a partir desta edição, vamos explorar capítulos desse repertório de melhores práticas, iniciando com o estabelecimento de políticas e demais normativos internos de segurança.

Certamente, você já enfrentou várias ameaças de diversas naturezas. Talvez não tão dramáticas quanto àquela que nos referimos na introdução deste assunto, mas que não deixam de ser ameaças. O que elas têm em comum? O fato de provocarem dois questionamentos imediatos diante da ocorrência: – O *que* fazer? *Como* fazer? E deles derivam outras questões bem significativas, como quem, quando, onde, quanto e por quê fazer, que podem orbitar tanto nos níveis estratégicos quanto operacionais de gestão. Estamos diante, como pode ver, das famosas questões 5W2H, ferramenta de gestão de grande ajuda no desenvolvimento de soluções e tomada de decisões. Mas você pretende esperar o incidente acontecer para iniciar este processo? Certamente, não. Tudo isto deve estar previamente estabelecido para que as chances de ocorrência de falhas sejam remotas e, caso venham a ocorrer, para que você não saia tomando decisões precipitadas ou impróprias para a ocasião. Lembre-se, nessa hora você estará no "olho do furacão".

A importância da documentação de processos, vale salientar, vai muito além de uma tábua de salvação para momentos de crise. Ela garante o perfeito funcionamento de dois ambientes de controle cruciais para as organizações, descritos no COSO[**2**]: – O Ambiente de Autorização e o Ambiente de Orientação (ou Comunicação). A harmonia entre esses dois ambientes é que vai nos permitir usufruir dos benefícios das decisões baseadas no 5W2H. Então, convidamos nossas entidades a darem um passeio pelo "mundo dos controles internos", fascinante para alguns, entediante e burocrático para outros, mas obrigatório para todos que buscam, através da mitigação de riscos, evidenciar o ato regular de gestão. Nesse momento, vale revisitar o Manual de Controles Internos, publicado pela Comissão Técnica de Controles Internos e Compliance da Abrapp, para melhor compreensão dos conceitos que serão aqui utilizados.

Vamos iniciar falando de política, documento associado à questão "o que" fazer, do nosso 5W2H. Questão como esta tem elevado valor estratégico e, por isso, expressa interesses dos proprietários na condução dos seus negócios; ou seja, resultados desejados. A política estabelece, portanto, diretrizes a serem seguidas pela gestão, sem entrar no mérito de "como" executá-las. Por este motivo, o documento deve, necessariamente, ser conciso, claro, objetivo e formalmente aprovado em instância superior da administração, onde os interesses dos proprietários do negócio encontram se representados, ou seja, no Conselho Deliberativo. E por estabelecerem diretrizes de atuação abrangentes, devem ser publicados de forma a garantir o amplo conhecimento por parte de todos os colaboradores da organização, inclusive prestadores de serviços. Sendo uma espécie de mandato, não pode ser descumprido, em hipótese alguma, sob pena de ficar evidente um ato irregular de gestão. Lembre-se, então, de que na política devem estar contidas proposições de ações objetivas e não detalhes de funcionamento.

Na sequência, falaremos dos demais documentos que, de acordo com as estruturas de cada entidade, podem apresentar diferentes nomenclaturas. Estamos nos referindo a manuais

operacionais, processos organizacionais, instruções normativas, instruções de trabalho, descrições de procedimento, enfim, todos aqueles documentos necessários ao entendimento do “como” fazer. Trata-se, portanto, de um elenco de documentos de caráter operacional, vinculados incondicionalmente às determinações da(s) política(s). Este elenco de documentos deve estabelecer, de forma clara e no requerido nível de detalhe, a forma como os gestores irão conduzir suas ações visando atingir os objetivos estratégicos da organização.

Então, mãos à obra!

Políticas

É recomendável que compreendam, pelo menos, justificativa, alinhamento corporativo, responsabilidades, alçadas, resolução de conflitos, comprometimento da alta administração, reporte de desempenho, análise crítica e melhoria contínua. Além disso, reiteramos, devem ser aprovadas pela instância máxima de deliberação da EFPC e amplamente divulgadas a todas as suas partes interessadas. Seguem algumas sugestões de políticas:

• Política de Segurança da Informação – Para alcançar sua finalidade de estabelecer princípios que nortearão as ações relacionadas à segurança da informação e alinhamento com o gerenciamento estratégico de riscos da EFPC, é recomendável que sua elaboração leve em consideração, além de boas práticas, os requerimentos legais, regulatórios e contratuais associados à segurança da informação.

• Política de Privacidade e Tratamento de Dados Pessoais – Com o propósito de definir diretrizes voltadas para assegurar que o uso de dados pessoais tratados pela EFPC restrinja-se, apenas, às finalidades consentidas, direta ou indiretamente pelos seus titulares, nos termos da Lei Geral de Proteção de Dados – LGPD, a EFPC evidencia seu compromisso com o devido sigilo dos dados utilizados. Por isso, às vezes é tratada, simplesmente, como Política de Privacidade. O uso de “cookies” deve ser abordado.

• Política de Gestão de Documentos e Dados – Com foco no princípio de Privacy by Default, o documento estabelece diretrizes para a devida manipulação de informações dentro da EFPC, levando em consideração a sua criticidade, o sigilo, o ciclo de vida dos dados e as condições de armazenamento e descartes. Atenção deve ser dada às questões contratuais relacionadas com os tratamentos de dados, notadamente em função dos compartilhamentos a que estão sujeitos.

• Política de Resposta a Incidentes de Segurança – Com o propósito de definir responsabilidades e ações que garantam uma resposta rápida e eficiente aos incidentes de segurança. Tais diretrizes devem permitir a identificação dos tipos, volumes e custos derivados dos incidentes, bem como a coleta e armazenamento de evidências, permitindo tanto o aprendizado com as falhas ocorridas quanto a realização de diligências de responsabilização – administrativa ou judiciais – aplicáveis.

Com vistas a racionalizar a publicação, o uso e a manutenção de políticas envolvendo a área de tecnologia, a EFPC pode adotar, como prática, a elaboração de um único documento – Política de Segurança da Informação – passando as demais sugeridas a compor Apêndices desta.

Demais Documentos

Para implementação das diretrizes aprovadas pelos proprietários do negócio torna-se necessário o estabelecimento de procedimentos operacionais que permitam o devido cumprimento. Tais documentos compõem o Ambiente de Controle Interno conhecido por Ambiente de Orientação (Comunicação). Devem, portanto, estar perfeitamente alinhados com as políticas, definindo “como” colocá-las em prática.

Conforme comentado anteriormente, não é nosso propósito, nesta publicação, padronizar as nomenclaturas dos documentos operacionais. Portanto, os documentos listados a seguir estão referenciados pelos seus conteúdos.

• Inventário de softwares e *hardwares* – O tratamento adequado dos dados requer a identificação e documentação de todos os "ativos" associados a recursos de processamento de informações. A localização de um equipamento – assim como de um sistema – deve ser definida de forma a minimizar o acesso não autorizado à área de trabalho (acesso desnecessário, ângulo de visão etc) e a assegurar que não saiam da organização sem autorização prévia.

• Inventário de dados pessoais – Também conhecido por Mapa de Tráfego de Dados Pessoais, este levantamento tem por objetivo montar um banco de dados que assegure a conformidade da EFPC em relação à Lei Geral de Proteção de Dados. Reúne informações relacionadas com descrição da tarefa, processo ao qual pertence, dados pessoais necessários, finalidade do tratamento, forma de autorização de uso, compartilhamento, local de armazenamento, dentre outras informações necessárias ao cumprimento da LGPD.

• Procedimentos de registro, tratamento e comunicação de incidentes de segurança – Apresentando os detalhes das providências a serem tomadas na hipótese de ocorrência de incidentes relacionados com a segurança da informação e do seu ambiente de gerenciamento. Quando relativos a dados pessoais, devem abranger as regras definidas pela Lei Geral de Proteção de Dados Pessoais.

• Procedimentos de acessos físicos e lógicos – Envolvendo regras e condições de liberação de acessos a ambientes físicos e lógicos da EFPC.

• Procedimentos de documentação de sistemas – Com o objetivo de detalhar, para usuários e administradores, o modo como os sistemas são operados e como realizar as suas manutenções.

• Procedimentos de produção e desenvolvimento – Envolvendo regras de desenvolvimento, produção e testes, inclusive de gestão da mudança.

• Procedimentos de homologação de produtos – Registros formais de que, além da área de tecnologia, os usuários ou áreas solicitantes testaram e aprovaram as soluções desenvolvidas.

• Plano de contingências e continuidade de negócios – Contendo regras para recuperação de desastres e para assegurar a operacionalidade da EFPC diante de eventos que causem interrupção parcial ou total de suas atividades. Recomenda-se que testes de intrusões e contingências estejam previstos no documento como procedimentos regulares.

• Matriz de Segregação de Funções – Também conhecida por Matriz SOD, ela garante o estabelecimento de restrições de acesso a funcionalidades de cada sistema de forma que as operações realizadas por uma mesma pessoa não gerem conflitos de interesses.

Acha que está bem documentado? Então já podemos avançar em nossas publicações. Não perca, na próxima edição: – saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos – Parte I.

[**1**] Série de TV "Mayday, desastres aéreos! " – National Geographic.

[**2**] *Committee of Sponsoring Organizations of the Treadway Commission* – 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.

Fonte: Abrapp em Foco, em 16.07.2021