A Gestão da Informação Aplicada na Proteção e Privacidade de Dados: Estudo de Multicasos

Claudio Pessoa[1], George Jamil[2], Sónia Estrela[3]

[1]Escola Superior Dom Helder Câmara (BRASIL)
[2]InfoAction Academy (BRASIL)
[3]Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro (PORTUGAL)

Resumo

A informação é um ativo essencial e crítico para o sucesso das organizações pelo que deve ser gerido eficazmente ao longo de todo o seu ciclo de vida. Esta realidade associada ao desenvolvimento tecnológico, que em muito tem contribuído para o aumento da produção, circulação, processamento, armazenamento e utilização da informação, conduziram à criação e aplicação de leis para proteger informações (dados) referentes a cidadãos e evitar o seu uso de forma indevida por terceiros. Neste sentido, este estudo de multicasos tem objetivo principal demonstrar como a aplicação de um modelo de gestão de informação contribui para a proteção eficaz de informações e para a criação de uma cultura de proteção nas organizações.

O trabalho apresenta o modelo de Modelo de alinhamento de Gestão de Informação e Conhecimento, a metodologia seguida e os resultados obtidos em cinco empresas de dimensões e áreas de atividade diferentes no Brasil. Foi aplicado um inquérito no início e doze meses após a implementação do modelo a fim de aferir os impactos nos requisitos de segurança da organização. Os resultados evidenciam o impacto positivo que as empresas que aplicaram o Modelo melhoraram os seus indicadores de segurança de forma significativa, sobretudo nas que houve um maior sensibilização e envolvimento dos gestores de topo. As restantes tiveram resultados menos satisfatórios e não conseguiram atingir os patamares desejados dentro do prazo pré-definido.

Palavras-chave: Proteção e Privacidade da Informação, Gestão da informação, Alinhamento estratégico.

1 INTRODUÇÃO

É possível acompanhar, a nível mundial, a criação e evolução de leis com o intuito de proteger informações (dados) referentes a cidadãos, os designados dados pessoais. Leis como a *General Data Protection Regulation* (GDPR), que posteriormente serviu de base para a lei brasileira, denominada *Lei Geral de Proteção de Dados Pessoais* (LGPD), mostram claramente a preocupação com a privacidade dos dados pessoais dos cidadãos. Paralelamente assiste-se ao multiplicar de casos de uso inadequado de tecnologias, nomeadamente inteligência artificial, extração de dados, sistemas como Siri da empresa Apple ou Alexa da empresa Amazon, que acompanham a rotina dos indivíduos, criando perfis de consumo e possibilitando, com isso, um atendimento mais personalizado aos cidadãos. Contudo, o uso desses dados nem sempre é feito de forma lícita e diversas empresas não colocam limites, importunando, e chegando, às vezes, a vender dados dos cidadãos, que acabam por ser explorados por pessoas mal-intencionadas. Adiciona-se ainda a falta de preparação e a vulnerabilidade dos cidadãos e das organizações em lidar com a proteção das informações, muitas vezes consideradas pela lei como dados sensíveis que, em caso de violação, geram sanções ainda maiores aos infratores.

Uma pesquisa realizada pela Federação Brasileira de Bancos (Febraban, 2021) concluiu que o advento da pandemia mundial contribuiu de forma significativa para o aumento de casos de infração de uso indevido de dados. Esta pesquisa expõe o crescimento de ataques de engenharia social (somados com crescimento de 165%), que envolvem *phishing* (aumento de 26%), falsos estafetas (aumento de 271%), falsos *call center* e uso inadequado da aplicação WhatsApp (são

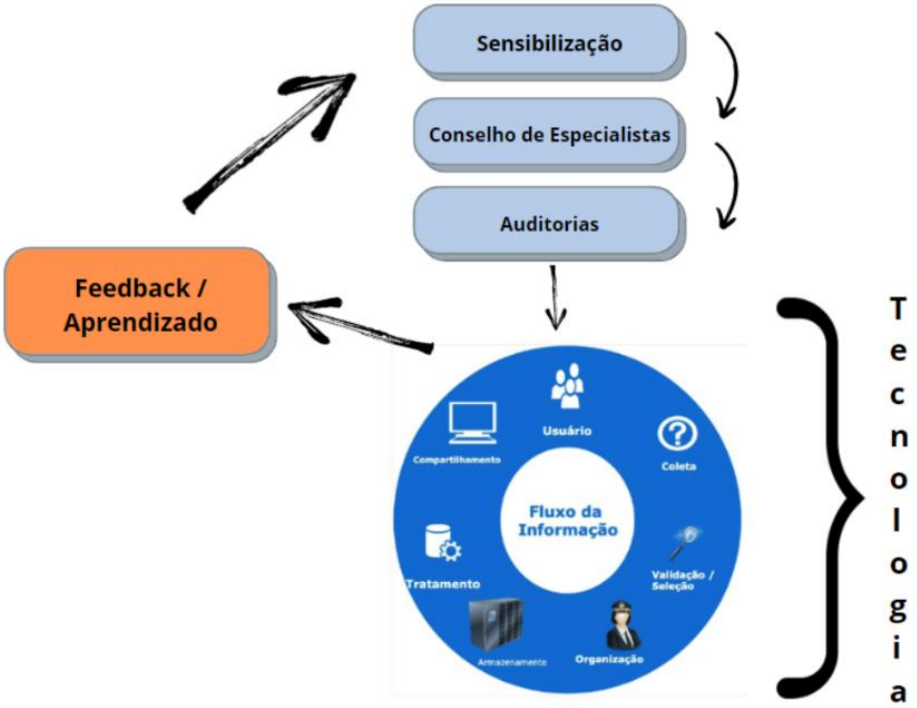
vários os exemplos de processos instaurados na justiça brasileira originados pelo envio através desta ferramenta de documentos com dados sensíveis, entre os quais atestados médicos). Uma outra pesquisa, realizada pelo portal Deep Legal Analytics (2022), realça que, apesar de as vulnerabilidades humanas serem responsáveis pela maioria das fraudes, em mais de 60% dos casos, na justiça, as empresas são responsabilizadas pelas fraudes, pagando pela sua falta de preparação no atendimento dos clientes. Tal evidencia claramente a necessidade de as empresas investirem na proteção das informações que são tratadas pelos seus colaboradores, independentemente dos cargos que ocupam (de níveis mais elevados e cujas informações são estratégicas para organização, ou ocupantes de funções de menor impacto, mas que podem contribuir consideravelmente para a fraude).

O aumento exponencial da informação recebida e gerada diariamente exige das organizações a criação de mecanismos de proteção que garantam a salvaguarda e a gestão do ciclo de vida dessa informação. Neste sentido, este artigo tem por objetivo demonstrar como a aplicação de um modelo de gestão de informação contribui para a proteção eficaz de informações e para a criação de uma cultura de proteção que promove o sucesso das organizações nesta empreitada.

2 A GESTÃO DA INFORMAÇÃO NA PROTEÇÃO E PRIVACIDADE DE DADOS: O MODELO MAGIC

Ao analisar os conceitos de gestão de informação e ao fazer um paralelo com os requisitos das normas de segurança da informação e privacidade de dados (em especial as normas ISO 27 001 e 27 701) e com a LGPD, percebe-se claramente a existência de aplicabilidade prática destes conceitos. Em especial no tocante à necessidade da análise profunda, por parte das organizações, dos processos envolvidos e no ciclo das informações inseridas nos mesmos.

Dentro desse contexto, o Modelo de alinhamento de Gestão de Informação e Conhecimento (MAGIC), desenvolvido por Pessoa (2016), pode ser utilizado no intuito de servir como guia para gestores de tecnologia da informação e comunicação (TIC), gestão de topo e profissionais de segurança da informação no sentido de alinhar estrategicamente as informações do negócio aos requisitos das normas de segurança e à lei (Figura 1).



Fonte: Pessoa (2016).

Figura 1. Modelo MAGIC.

O modelo MAGIC deixa evidente que, no início do trabalho, é extremamente importante a sensibilização da gestão de topo da organização. O seu envolvimento, e consequente assumir da responsabilidade e o exigir do gestor de segurança (Data Protection Officer — DPO, encarregado de proteção de dados pessoais, etc.) compromisso, é um fator crítico de sucesso para a implementação do Modelo. Neste primeiro momento, este envolvimento fomentará, também, a compreensão dos restantes profissionais da importância do projeto para a organização.

No segundo momento, é necessário criar nas organizações um conselho de especialistas (comité de segurança e proteção da informação), composto pelos líderes da organização, e contar (se possível) com um representante de cada área (Jurídica, Comercial, Financeira, Recursos Humanos, etc.). Deve ser coordenado pelo profissional responsável pela proteção e segurança das informações, uma vez que será ele quem irá fazer a análise dos processos e dos fluxos informacionais da empresa. O conhecimento destes processos e fluxos habilita-o, no momento oportuno, a distribuir as responsabilidade e tarefas na procura da conformidade com as leis e normas da área. Este profissional tem que conhecer os conceitos de gestão de informação (GI) e proteção de dados, sob pena de o projeto ficar prejudicado por ele não dominar algum aspeto da área e criar, com isso, vulnerabilidade e riscos adicionais ao processo. Ademais, é de fundamental importância que este profissional tenha habilidades e competências na área de gestão, em especial de gestão de pessoas, porque será o responsável por liderar a equipa de implementação e/ou manutenção do processo (não basta simplesmente implantar, porque o processo é cíclico e terá que ser verificado periodicamente).

O comité de segurança e proteção da informação terá como responsabilidade mapear e analisar todos os processos da organização. Este mapeamento deve identificar claramente: as pessoas envolvidas (de cada área), a conexão existente entre as áreas e/ou com pessoas externas à organização, as informações envolvidas e as ferramentas (tecnologias, suportes) utilizadas para suportar o processo. Neste momento é importante fazer uma análise que demonstre a todos os envolvidos a situação da empresa (o patamar em que esta se encontra no momento inicial ao projeto) em relação à gestão e proteção da informação. É importante a utilização das normas de segurança (em especial as normas ISO 27 001 e 27 701) e, no caso do Brasil, da LGPD. Isto permitirá, após a implementação, comparar a evolução e deixar a empresa em conformidade com as necessidades regionais para proteção, segurança e privacidade de dados.

Após análise dos processos, o líder do projeto (DPO, profissional de segurança) deve analisar o fluxo da informação dentro de cada processo mapeado, o qual engloba um conjunto de etapas:

- **Perceção**: inicia-se no momento em que o profissional sente a necessidade de ter informação que o apoie na execução do seu trabalho e na tomada de decisão. Compete ao comité de segurança identificar a informação necessária e como esta será procurada e obtida.
- **Recolha**: conhecidas as necessidades de informação, segue-se a análise das formas de a obter, ou seja, como a informação entrará na organização. Toda a informação tem que ser protegida e os cuidados a adotar deverão abarcar toda a informação, independentemente do seu suporte.
- **Validação/Seleção**: visa evitar a criação de um repositório de informações sem valor para o negócio da empresa e com riscos desnecessários (e que gere necessidade de investimentos de proteção pois, se foi obtida, deve ser protegida, em especial os dados pessoais). Outro fator da importância da validação reside na verificação de informações que foram obtidas de diversas formas (papel, email, folhas de cálculo, aplicações de telemóvel, etc.) e que serão posteriormente inseridas nos sistemas de informação organizacionais. Está implícito nas melhores práticas a necessidade de o comité de segurança nomear um profissional que terá como responsabilidade conferir periodicamente a veracidade e consistência dos sistemas em relação ao que foi obtido e inserido posteriormente. Só assim será possível confirmar a integridade da informação analisada.
- **Organização**: segundo Alvarenga (2003), devem-se observar três estágios na implementação de um sistema de GI eficaz:
- o estágio anterior à entrada de itens no sistema de informação; ii) o que corresponde à entrada do item no sistema; iii) o pós-inclusão do item no sistema. Estes três estágios visam tornar a recuperação eficaz, permitir que o profissional encontre a informação pertinente e a possa usar no momento oportuno. É fulcral que as informações sejam

analisadas segundo a sua importância para o negócio da organização. A partir daí, deve ser feita uma análise de riscos e, posteriormente, uma classificação das informações por níveis que permitirão aos gestores dos sistemas de informação e/ou gestores de arquivos físicos criar níveis de privilégio de acesso às informações armazenadas. Esta classificação ambiciona evitar possíveis acessos indevidos às informações e, consequentemente, eventuais incidentes de segurança da informação e/ou violação de dados pessoais.

- **Armazenamento**: momento que consiste em analisar as soluções que respondam melhor às necessidades do negócio. Frequentemente a informação encontra-se em diversos suportes e é essencial assegurar um sistema integral e sistémico de informação que apoie a aprendizagem organizacional e a gestão corrente e estratégica da organização. É importante, portanto, criar uma solução que consiga armazenar, de forma ativa e permanente, essas informações que devem ser protegidas da mesma forma por fazer parte do acervo (ativo) das organizações.
- **Disseminação/Manutenção**: no contexto da proteção da informação, a disseminação deve seguir as regras de classificação definidas previamente na fase de organização e ditará as regras de acesso nos sistemas de armazenamento escolhidos na fase anterior, ou seja, para que um profissional da empresa tenha acesso e privilégios de criar, editar e apagar uma informação, deve ser feito um estudo profundo que terá como base um conjunto de elementos, a saber: necessidade do uso, qual a informação a que deve aceder (princípio da minimização de dados - LGPD), e nível de acesso (somente leitura, edição, eliminação). Este estudo fará com que o uso seja seguro e eficaz para o negócio da organização.
- **Uso Efetivo/Tomada de Decisão**: o ciclo da informação terminará no momento em que os profissionais usam de facto a informação de forma eficaz e sem prejuízo para a organização, ou seja, sem gerar um eventual incidente de segurança e/ou uma violação de dados pessoais.
- ***Feedback*/Monitorização Estratégica**: o *feedback*, designado de valorização por Jamil (2014, p. 22), "destina-se a estudar e apreciar os métodos quantitativos aplicados e as tentativas de apropriar valores financeiros e de outras grandezas relacionadas a indicadores, como produtividade, custo de oferta, preços, etc." e a monitorização estratégica "se destina a perceber se a informação e conhecimento gerados poderiam ser aplicados para finalidades estratégicas, como tomadas de decisão e planejamento".

3 METODOLOGIA

A metodologia de múltiplos casos foi adotada para o presente trabalho, porque permite a obtenção de resultados consistentes, em função de comparação por critério único, de casos classificados como potencialmente semelhantes em termos de contexto para análise (Yin, 2010; Jamil, 2005; Jamil & Silva, 2016; Vergara, 2016). Este método traz, consigo, as perspetivas de resultados advindos dos estudos de caso, de larga adoção em diversos campos científicos. Porém, a ampliação para a análise de vários casos de forma padronizada, pode possibilitar, em virtude da consistência e robustez nas análises feitas nestes casos, o alcance de resultados potencialmente generalizáveis (Gustafsson, 2012; Jamil & Silva, 2016).

Segundo Gustafsson (2012) e Halkias (2022), os estudos de múltiplos casos são estudos qualitativos de bom aproveitamento para obter resultados como os esperados neste trabalho, sendo fatores críticos para sua adoção: 1) o conhecimento prévio de casos; 2) a possibilidade de classificação precisa dos casos selecionados; 3) o domínio da situação dos casos, que permita, entre outros fatores, a análise prevista pelos objetivos do estudo; e 4) condições semelhantes no que tange ao âmbito da pesquisa em curso (acesso às fontes de dados, entrevistados, exames *in loco*, entre outros fatores que caracterizam a aplicação da metodologia tradicional dos estudos de casos).

O modelo MAGIC foi aplicado em 5 empresas de diferentes dimensões e áreas de atuação no Brasil, como pode ser observado na tabela 1. No primeiro momento foi criado, em todas as empresas, o comité de segurança com o objetivo de conduzir a implementação do projeto, conforme descrito no modelo MAGIC. Realça-se que houve o cuidado de convidar os diretores

das cinco empresas para constituírem o comité de segurança e assim observar o requisito primeiro do modelo (sensibilização da gestão de topo). Constituído o comité de segurança, foi realizada uma análise, através da aplicação de um questionário em dois momentos: o primeiro, no início, com o objetivo de fazer a avaliação inicial e conhecer como se encontravam as empresas antes da aplicação do modelo MAGIC; o segundo, cerca de doze meses após a aplicação do modelo MAGIC, para avaliar os impactos nos requisitos de segurança da organização. As questões do inquérito abarcam todos os requisitos existentes nas normas ISO 27 001 e ISO 27 701, normas internacionais de segurança da informação e privacidade de dados pessoais, respetivamente. O questionário foi respondido por elementos do comité de segurança, com destaque para gestores da área de Tecnologia da Informação das organizações.

Tabela 1. Apresentação das empresas.

Empresas	Área	Dimensão	N.º Trabalhadores
1	Advocacia	Média	60
2	Publicidade	Média	60
3	Consultoria Extração Mineral	Pequena	11
4	Advocacia	Grande	1 600
5	Supermercados	Grande	26 000

Paralelamente à aplicação do questionário, todos as áreas das empresas elaboraram um relatório no qual é estudado o fluxo da informação de cada processo, de cada setor específico, tornando viável o estudo da análise de risco envolvido no tratamento das informações nas organizações. A partir destes dados são traçados planos de ação com o objetivo de dar resposta aos requisitos das normas e mitigar os riscos identificados nos processos analisados em conjunto com o comité de segurança. Dentro dos planos traçados para todas as empresas, é descrito um plano de formação de temas envolvidos da área de gestão, proteção e privacidade de dados, para que todos os elementos da organização estejam conscientes deles, conheçam os conceitos e saibam como aplicá-los no quotidiano empresarial.

4 RESULTADOS

Após a aplicação do questionário foram elaborados gráficos que servem de guia na procura da melhoria contínua do nível de segurança das empresas. Os valores dos gráficos foram gerados relativamente ao nível de exigência das normas (ou da regulamentação da Autoridade Nacional de Proteção de Dados) devido à dimensão e complexidade dos dados tratados pelas empresas. A tabela 2 apresenta o critério de avaliação para adequação aos requisitos das normas e respetiva pontuação atribuída que foram usados para fazer a avaliação em cada empresa.

Tabela 2. Critério de avaliação para adequação aos requisitos das normas.

Critério	Pontuação atribuída
Não existe nada implementado	0
Existe a documentação mas não está implementado	1
Existe implementado mas não tem documentação (evidências)	1
Existe implementado e documentado	2
Não se aplica	2

Foram definidos, de acordo com a pontuação obtida, quatro níveis de risco: Risco Alto, Risco Médio, Risco Baixo e Ideal (tabela 3).

Tabela 3. Critério de avaliação para adequação aos requisitos das normas.

Nível de risco	Pontuação
Risco Alto	inferior a 213 pontos
Risco Médio	entre 214 e 340
Risco Baixo	entre 341 e 404 pontos
Ideal	acima de 405 pontos

A figura 2 sintetiza os resultados das avaliações feitas no início e após doze meses da aplicação do modelo MAGIC nas cinco empresas objeto de estudo. A empresa 1 apresentou uma melhoria significativa nos requisitos de segurança da organização. Na avaliação inicial obteve 117 pontos, o que significa que apresentava um Risco Alto. Alcançou a classificação mais baixa de quatro níveis, o que corresponde a um nível de conformidade baixo. Porém, doze meses depois, e após a aplicação do modelo MAGIC, alcançou 382 pontos, situando-se no nível 3 da classificação, ou seja, Risco Baixo. Tais resultados evidenciam uma evolução importante a nível da gestão da informação e da segurança da informação nesta empresa.

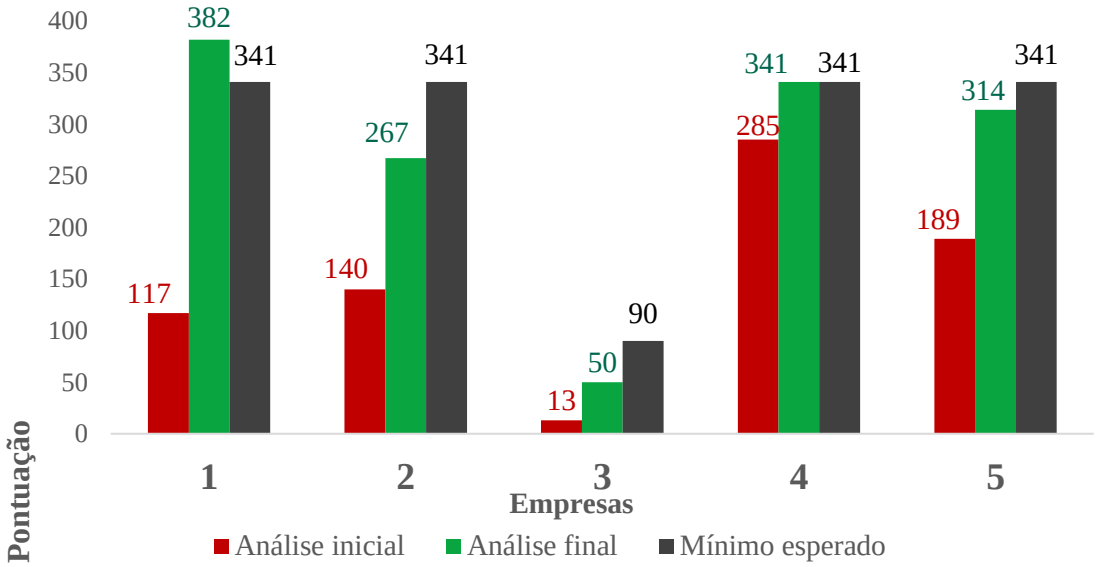


Figura 2. Resumo dos resultados obtidos na avaliação inicial e na final nas 5 empresas.

A empresa 2 teve uma ligeira melhoria, passando dos 140 pontos para 267, ou seja, passou do nível de Risco Alto para o de Risco Médio após a aplicação do modelo MAGIC. Por sua vez, a empresa 3 registou um incremento da proteção e segurança da informação da empresa uma vez que passou de 13 valores, na avaliação inicial, para 50 após 12 meses de trabalho de adequação (passou do nível de Risco Alto para o de Risco Médio). Importa salientar que, sendo uma empresa de pequena dimensão, os requisitos exigidos em relação aos parâmetros de segurança são em número menor. Perante estas características o inquérito foi diferente do aplicado às restantes empresas.

No caso da empresa 4 contata-se uma melhoria importante a nível de segurança da informação. Passou de uma nota inicial de 285 (Risco Médio, o segundo nível mais baixo) para 341 pontos, doze meses depois, situando-se no nível 3 da classificação, ou seja, Risco Baixo. Por fim, a empresa 5 apresentou uma ligeira melhoria na avaliação da segurança da informação. Na

avaliação inicial obteve uma nota de 189, ou seja, Risco Alto, e alcançou 314 pontos na avaliação final, situando-se no nível 2 da classificação, ou seja, Risco Médio.

Todas as empresas objeto de estudo registaram melhorias a nível de segurança da informação. Analisando a classificação obtida na análise final, constata-se que a empresa 4 alcançou o mínimo definido, a empresa 1 ultrapassou-o e as restantes (empresas 2, 3 e 5) não conseguiram atingir os níveis desejáveis de conformidade dentro do prazo estabelecido.

4.1 Análises da aplicação do modelo MAGIC

O impacto da aplicação do modelo teórico nas 5 empresas é evidente e demonstra, na prática, a sua eficácia na melhoria da gestão da informação e na busca da conformidade com as normas e leis da área de proteção e privacidade de dados. Globalmente, considera-se relevante destacar quatro pontos:

1) a necessidade do envolvimento da gestão de topo: ficou evidente ao longo do trabalho que, conforme demonstrado no modelo MAGIC, num primeiro momento, é necessário um envolvimento dos gestores das empresas para que o trabalho flua de forma natural na procura da conformidade. Nas empresas onde os gestores atuaram de forma eficaz (empresas 1 e 4) a melhoria do resultado é significativa. Verifica-se que o resultado não é condicionado pela dimensão da empresa, porque nas restantes empresas, cujos gestores não tiveram essa sensibilidade (mesmo na empresa 3 considerada de pequena dimensão), a melhoria não foi a esperada.

2) Envolvimento de toda a equipa: como seria expetável, o compromisso da equipa (em especial do comité de segurança) é essencial para o sucesso da implementação. Também se aplicará aqui a regra da necessidade de os gestores estarem alinhados com o comité de segurança, porque, nas empresas onde os gestores não participaram ativamente, os responsáveis das áreas que compõem o comité de segurança não sentiram a necessidade e a responsabilidade de fazer com o que a conformidade fosse atingida no tempo proposto. Houve, por parte da equipa de implementação, uma dificuldade em fazer os processos evoluírem como deveriam.

3) Melhoria dos resultados: todas as empresas, com exceção da empresa 4 (onde já existia um processo mais evoluído devido à sua dimensão e às exigências dos seus clientes para que a empresa acautelasse a segurança dos dados tratados), encontravam-se num nível de conformidade baixo. Os resultados melhoraram de forma considerável após a aplicação do modelo, constatando-se que, mesmo nas empresas que não atingiram o nível esperado no prazo definido para a implementação, se registou uma melhoria.

4) A dimensão da empresa não é o fator preponderante. Esta afirmação é sustentada em duas análises distintas: i) a empresa 1 é de média dimensão e registou um envolvimento grande dos gestores e, consequentemente, do comité de segurança. Inicialmente encontrava-se num nível de conformidade baixo, porém, dentre as empresas analisadas, foi a que teve a melhoria mais considerável, chegando inclusive aos níveis desejáveis de conformidade dentro do prazo estabelecido; ii) era esperado que a empresa 5, sendo de grande dimensão, tivesse um nível de conformidade inicial maior e houvesse maior envolvimento dos seus líderes, devido ao facto de estarem mais bem preparados em termos de gestão e conhecimento. Contudo, não conseguiu o resultado esperado. Os líderes demoraram a iniciar os mapas de processos, as análises necessárias e, consequentemente, a geração de um plano de ação para mitigar os riscos e aumentar o índice de conformidade. Esta situação impediu que atingisse o índice esperado.

5 CONCLUSÕES

Os resultados obtidos confirmam que a adoção de boas práticas de gestão de informação agrega valor à informação em todas as etapas do ciclo de vida e potencia o desenvolvimento de uma

cultura de proteção de informação. A aplicação do modelo MAGIC tem trazido bons resultados para as empresas, tendo demonstrado ser eficiente para apoiar e orientar os gestores na melhoria da gestão e proteção das suas informações.

Tal como evidenciado, a sensibilização da gestão de topo das organizações é um fator crítico e fundamental para o sucesso da sua implementação porque influencia diretamente o nível de compromisso dos líderes da empresa (comité de segurança) e, consequentemente, dos restantes profissionais envolvidos no processo de adequação. Os resultados apresentados demonstram que sem o envolvimento da equipa e, principalmente da gestão de topo, os objetivos não são atingidos dentro do prazo esperado.

Parece igualmente evidente que a dimensão da empresa não será o fator preponderante de sucesso. A complexidade das informações tratadas, bem como a preparação da equipa para fazer o levantamento e a análise de processos é fundamental. Esta situação cria a necessidade do uso de algum modelo (guia) que levará ao sucesso da implementação e, neste sentido, o modelo MAGIC revela-se eficaz porque alinha a gestão da organização, as informações envolvidas, as ferramentas e os métodos na procura dos resultados esperados. Se aplicado devidamente, conforme corroboram os resultados obtidos pelas empresas 1 e 4, projeta as organizações para os patamares desejados dentro do prazo pré-definido.

REFERÊNCIAS

Alvarenga, L. (2003). Representação do conhecimento na perspectiva da ciência da informação em tempo e espaço digitais. *Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação*, Florianópolis, v. 8, n. 15, p. 19-40.

Deep Legal. (2022, janeiro 26). Fraudes eletrônicas: estudo revela que 60% das empresas são responsabilizadas por golpes. https://www.deeplegal.com.br/blog/engenharia-social-fraudes-eletronicas

Febraban (2021, novembro 1). Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais. https://febraban.org.br/noticia/3704/pt-br/

Gustafsson, J. (2017, janeiro 12). S*ingle case studies vs. multiple case studies: A comparative study*. http://hh.diva-portal.org/smash/record.jsf?pid=diva2:1064378

Halkias, D., Neubert, M., Thurman, P. W., & Harkiolakis, N. (2022). T*he multiple case study design*. San Francisco: Ed. Routledge.

Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD). http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Jamil, G. L. (2005). *Gestão da Informação e do conhecimento em empresas brasileiras: Um estudo de múltiplos casos.* [Tese de Doutorado, Universidade Federal de Minas Gerais].

Jamil, G. L., & Silva, A. M. da (2016). *Inteligência de Mercado como um Processo de Gestão da Informação e do Conhecimento: Proposta de Oficinas de Capacitação Setoriais*. Porto: Editora Formalpress, Século XXI.

Pessoa, C. R. M. (2016). *Gestão da Informação e do Conhecimento no Alinhamento Estratégico em Empresas de Engenharia*. [Tese de Doutoramento, Universidade Federal de Minas Gerais, 2016]. https://bityli.com/YXSYWyrg

Regulamento Geral sobre a Proteção de Dados (GDPR). https://gdprinfo.eu/pt-pt

Vergara, S. (2016). *Projetos e Relatórios de Pesquisas em Administração*. São Paulo: Ed. Atlas.

Yin, R. K. (2010). *Estudo de caso: Planejamento e métodos.* Porto Alegre: Bookman.