DOI: 10.5748/19CONTECSI/PSE/LIS/7039

A GESTÃO DA INFORMAÇÃO APLICADA NA PROTEÇÃO E PRIVACIDADE DE DADOS

Claudio Roberto Magalhães Pessoa ; https://orcid.org/0000-0002-9439-0382
EMGE - Escola de Engenharia de Minas Gerais: Belo Horizonte

George Leal Jamil ; https://orcid.org/0000-0003-0989-6600
Infoaction

Sónia Catarina Lopes Estrela ; https://orcid.org/0000-0002-8932-7055
Universidade de Aveiro

A GESTÃO DA INFORMAÇÃO APLICADA NA PROTEÇÃO E PRIVACIDADE DE DADOS

INFORMATION MANAGEMENT APPLIED TO DATA PROTECTION AND PRIVACY

RESUMO

A informação é um ativo essencial e crítico na sociedade atual pelo que a adoção de boas práticas de gestão agrega valor 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. Assim, este trabalho tem como 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 que conduzirá ao sucesso nessa empreitada.

A metodologia de pesquisa utilizada é a de estudo de múltiplos casos, aplicada em organizações de diversos portes e áreas de atividade. Os resultados permitem constatar que as empresas que aplicaram o modelo de gestão de informação de forma integral tiveram seus indicadores de segurança modificados de forma significativa. Por outro lado, as empresas que não aplicaram o modelo, em especial aquelas onde não houve uma sensibilização dos gestores, 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.

ABSTRACT

Information is an essential and critical asset in today's society, so the adoption of good management practices adds value throughout its life cycle. This reality associated with technological development, which has greatly contributed to the increase in the production, circulation, processing, storage and use of information, led to the creation and application of laws to protect information (data) concerning citizens and prevent their improper use by third parties. Thus, this work has a main objective to demonstrate how the application of an information management model contributes to the effective protection of information and the creation of a protection culture that will lead to success in this endeavor.

The research methodology used is the study of multiple cases, applied in organizations of different sizes and activities. The results show that the companies that applied the information management model in an integral way had their security indicators significantly modified. On the other hand, companies that did not apply the model, especially those where there was no awareness among managers, had less satisfactory results and were unable to reach the desired levels within the predefined period.

Keyword:
Information Protection and Privacy; Information management; Strategic alignment.

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.

Essa preocupação acentua-se perante ainda mais perante o multiplicar de casos de uso inadequado de tecnologias, sobretudo tecnologias como inteligência artificial, mineração de dados, sistemas como Siri da empresa Apple ou Alexa da empresa Amazon, que claramente acompanham a rotina de seus proprietários, criando perfis de consumo e possibilitando, com isso, um atendimento mais personalizado aos cidadãos. Tudo isso seria muito interessante, pois permite às empresas se programarem para esse atendimento. Contudo, nem tudo é usado de forma lícita. Diversas empresas não colocam limites para tal, importunando e, às vezes, até vendendo dados dos cidadãos para serem explorados por pessoas má intencionadas.

Soma-se a isso o despreparo e vulnerabilidade dos cidadãos e das empresas em lidar com a proteção de informações, muitas vezes consideradas pela lei com dados sensíveis, dados esses que em caso de violação geram sanções ainda maiores aos infratores. Segundo pesquisa realizada pela Federação Brasileira de Bancos (Febraban, 2021), o advento da pandemia mundial contribui de forma significativa para esse cenário. A pesquisa mostra o crescimento de ataques de engenharia social (somados com crescimento de 165%), que envolvem *phishing* (aumento de 26%), falso motoboy (aumento de 271%), falsa central de atendimento, uso do aplicativo WhatsApp de forma equivocada. São vários os exemplos de ações na justiça brasileira[1], cuja origem dos processos residiu no envio de documentos com dados sensíveis (nomeadamente atestados médicos) pela ferramenta.

Uma outra pesquisa, realizada pelo portal Deep Legal Analytics (2022)[2], mostra que apesar das vulnerabilidades humanas serem responsáveis pela maioria das fraudes, em mais de 60% dos casos na justiça as empresas são responsabilizadas pelas fraudes, ou seja, pagarão pelo despreparado no atendimento de seus clientes. Isso demonstra claramente a necessidade das empresas investirem na proteção das informações que são tratadas por seus colaboradores, independentemente de ocuparem níveis mais elevados (cujas informações são estratégicas para organização), ou funções de menor impacto, mas que podem contribuir consideravelmente para a fraude.

O aumento exponencial da informação recebida e gerada diariamente nas organizações exige a criação de mecanismos de proteção de forma a garantir sua salvaguarda e gestão do seu ciclo de vida. 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, criando uma cultura de proteção que naturalmente levará ao sucesso das organizações nessa empreitada.

FUNDAMENTAÇÃO TEÓRICA

GESTÃO DE INFORMAÇÃO

A informação é um ativo essencial que as organizações precisam gerir de forma eficaz e eficiente para atuarem de forma mais rápida e eficaz, diminuindo o tempo e os recursos. Gerir

[1] Violações à LGPD disponível em https://anppd.org/violacoes, cons. 29 setembro 2022.
[2] Disponível em https://www.deeplegal.com.br/blog/engenharia-social-fraudes-eletronicas, cons. 29 setembro 2022.

informação consiste em "(…) lidar, administrar, encontrar soluções práticas desde a génese até ao efeito multiplicador do fluxo da informação" (Silva, 2006, pp. 148-9). Neste sentido, tal como defende Detlor (2010), gerir informação permite controlar a forma como esta é criada, adquirida, organizada, armazenada, distribuída e usada, visando a agilização do fluxo e a intensificação do uso da informação por pessoas e organizações.

A aquisição engloba a identificação das necessidades de informação, o que exige conhecer qual a informação que os usuários precisam. Essa informação pode ser de origem externa ou interna (produzida organicamente pela organização) e apoiará os usuários na realização das suas atividades. Contudo, nem sempre as organizações têm a preocupação de identificar as necessidades de informação, o que impossibilita a articulação entre a informação e os objetivos e estratégia organizacionais, conduzindo ao aumento de informação cuja utilidade e pertinência são questionáveis.

A informação adquirida/produzida deve ser tratada, atividade que consiste num conjunto de procedimentos associados à existência ou possibilidade de registo, com o objetivo de ser consultado sempre que necessário e evitar ser esquecido. A informação só é útil se estiver devidamente tratada e organizada de forma a estar acessível e ser usada (Estrela, 1016). O tratamento engloba a organização e o armazenamento, o que exige esquemas intelectuais físicos de estruturação e categorização dos dados que permitam que a informação seja guardada, acedida e usada. A organização da informação, alinhada com a estrutura de funcionamento, permitirá determinar os tipos de acesso e a informação a que cada usuário poderá acessar (nomeadamente a classificação da informação por níveis de acesso).

A distribuição da informação consiste em disponibilizar a informação pertinente, no momento oportuno, às pessoas certas. Por fim, o uso da informação é uma etapa fundamental que se interliga com todas as fases do ciclo de vida da informação. O uso da informação é um processo pessoal, que depende do sujeito que conhece, pensa e se emociona e é profundamente modelado pelas características de quem usa a informação e do contexto em que está inserido.

Uma gestão eficaz da informação permitirá identificar as necessidades de informação, direcionar o uso da informação à estratégia da organização, evitar situações de redundância e duplicação da informação, avaliar a informação, promover a integração das diferentes soluções tecnológicas usadas, reduzir os custos de manutenção, aplicar a normalização, alcançar os objetivos organizacionais e cumprir os imperativos legais e fiscais (Pinto & Silva, 2005).

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

Ao se analisar os conceitos de gestão de informação e 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), alta gestão e aos 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).

Figura 1 - Modelo MAGIC

Fonte: Pessoa (2016)

O modelo MAGIC deixa evidente que, no início do trabalho, é de suma importância a sensibilização da alta gestão da organização. Sem que a alta gestão perceba e assuma a responsabilidade de cobrança, junto ao gestor de segurança (Data Protection Officer - DPO, encarregado de dados pessoais, etc), os profissionais da empresa não entenderão a importância do projeto podendo, na maioria das vezes, fracassar na sua implantação.

No segundo momento, faz-se necessário criar nas organizações um conselho de especialistas (comitê de segurança e proteção da informação). Esse comitê deve ser composto pelos líderes da organização, onde deve (caso possível) ter um representante de cada setor da empresa (jurídico, comercial, financeiro, recursos humanos, etc.). Deve ser coordenado pelo profissional responsável pela proteção e segurança das informações, uma vez ser esse profissional que irá fazer toda análise dos processos e fluxos informacionais da empresa. Dessa forma, ele conseguirá, no momento oportuno, distribuir as responsabilidade e tarefas na busca da conformidade com as leis e norma da área. Faz-se evidente, nesse momento, a necessidade desse profissional conhecer os conceitos de gestão de informação e proteção de dados, sob pena do projeto ficar prejudicado por ele não perceber algum aspecto 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 gestão de pessoas, pois será ele também o responsável por liderar a equipe de implantação e/ou manutenção do processo, uma vez que não basta simplesmente implantar, o processo é cíclico e deve ser verificado periodicamente.

O comitê de segurança terá como responsabilidade mapear e analisar todos os processos da organização. Esse mapeamento deve deixar claro: as pessoas envolvidas (dentro de cada setor),

a conexão existente entre os setores e/ou com pessoas externas à organização, as informações envolvidas e as ferramentas (tecnologias, meio físico) utilizadas para suportar o processo. Nesse momento é importante a realização de uma análise que mostrará a todos os envolvidos como a empresa 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. Isso permitirá, após a implantação, 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 que se descrevem a seguir:

Percepção: inicia-se no momento em que o profissional que irá utilizar uma informação sente a necessidade de se embasar melhor para uma tomada de decisão (por exemplo), e buscará alternativas para sua necessidade. Cabe ao comitê de segurança entender qual a informação necessária e como será a busca dessa informação.

Coleta: conhecidas as necessidades de informação, deve-se analisar as formas de coleta da mesma, ou seja, como a informação entrará na organização. É importante salientar que as informações podem estar em diversas mídias como papel, eletrônica, vídeos, etc. As informações, independentemente da mídia, têm que ser protegidas, não se deve esquecer que as informações não estão 100% no mundo eletrônico e que os cuidados a adotar devem abarcar toda a informação.

Validação/Seleção: esse é um momento importante no processo visando evitar a criação de um repositório de informações (banco de dados, por exemplo) inútil e com riscos desnecessários, ou seja que contenha informações sem valia alguma para o negócio da organização e/ou que gere necessidade de investimentos de proteção pois, se foi coletada, deve ser protegida (em especial dados pessoais).

Outro fator da importância da validação está na conferência de informações que foram coletadas de diversas formas (papel, email, planilhas eletrônicas, aplicativos de celulares, etc.) e que serão posteriormente inseridas em sistemas da empresa. Está implícito nas melhores práticas a necessidade do comitê de segurança nomear um profissional que terá como responsabilidade conferir periodicamente a veracidade e consistência dos sistemas em relação ao que foi coletado e posteriormente inseridos. Somente assim poderá ser confirmada a integridade da informação analisada.

Organização: segundo Alvarenga (2003), na implantação de um sistema de gestão de informação (GI) eficaz deve-se observar três estágios: i) estágio anterior à entrada de itens no sistema de informação; ii) estágio que corresponde à entrada do item no sistema; iii) estágio pós-inclusão do item no sistema. Tudo isso tem o intuito de ter recuperação eficaz, que permita ao profissional encontrar e informação pertinente e usá-la no momento oportuno.

Quando tratamos do tema proteção de informação, é mister que as informações sejam analisadas segundo a sua importância para o negócio da organização. A partir dessa análise, deve ser feita uma análise de riscos e, posteriormente, uma classificação das informações por níveis que permitirão aos gestores dos sistemas eletrônicos e/ou gestores de arquivos físicos criar níveis de privilégio de acesso às informações ali armazenadas. Isso evita possíveis acessos indevidos às informações e, consequentemente, eventuais incidentes de segurança da informação e/ou violação de dados pessoais.

Armazenamento: nessa fase do projeto, devem ser analisadas as melhores soluções que atendam à demanda do negócio. A escolha da solução deve levar em conta o conceito do modelo Sistema de Informação, integral, Ativa e Permanente (SI-AP), de Silva e Ribeiro (2009), o qual ganha importância ao lembrar que "a noção estática e analógica de documento (conteúdo + qualquer suporte material) é subordinada à noção operatória da informação". Os autores afirmam que nem toda informação está no formato eletrônico, "como a panaceia da adoção entusiástica e ingênua de ferramentas de TIC fez crer que fosse". Muitas informações estão em papéis e até mesmo com as pessoas que as detêm. Isso não quer dizer que podem ser perdidas, substituídas, pois fazem parte de um histórico fundamental para o aprendizado organizacional. Devem ser protegidas da mesma forma por fazer parte do acervo (ativo) das organizações. É importante, portanto, criar uma solução que consiga armazenar, de forma ativa e permanente, essas informações.

Disseminação/Manutenção: a disseminação da informação é fundamental no processo de gestão e proteção das mesmas. Para Marchand, Kettinger, e Rollins (2001) e Capurro (2003), o conhecimento só será útil em uma empresa caso seja compartilhado. Segundo Moresi (2000, p. 19), conhecimento pode ser definido como "sendo informações que foram analisadas e avaliadas sobre a sua confiabilidade, sua relevância e sua importância". 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 informação realmente deve ser acessada (princípio da minimização de dados - LGPD), e nível de acesso (somente leitura, edição, eliminação). Esse estudo fará com que o uso seja seguro e eficaz para o negócio da organização.

Uso Efetivo/Tomada de Decisão: o fim do ciclo da informação terminará no momento em que os profissionais usam de fato 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*/Monitoramento Estratégico**: de acordo com Jamil (2014, p. 22), o *feedback*, chamado por ele de valorização, "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 o monitoramento estratégico "se destina a perceber se a informação e conhecimento gerados poderiam ser aplicados para finalidades estratégicas, como tomadas de decisão e planejamento".

O modelo MAGIC tem sido utilizado em diversos tipos de organizações, inclusive de portes diferentes, permitindo atingir a conformidade e proteção de informações necessárias e, consequentemente, resultados operacionais melhores, conforme será demonstrado adiante.

METODOLOGIA

Visando atingir o objetivo traçado para essa pesquisa, o modelo Magic foi aplicado em 5 empresas de diferentes portes e áreas de atuação num estudo de múltiplos casos. A decisão pela metodologia de múltiplos casos foi tomada para permitir a obtenção de resultados mais 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 perspectivas de resultados

advindos dos estudos de caso, de larga adoção em campos científicos diversos. Porém, a ampliação para a análise de vários casos em 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).

Como analisam Gustafsson (2012) e Halkias (2022) os estudos de múltiplos casos são estudos qualitativos de bom aproveitamento para obtenção de resultados como os esperados por esta pesquisa, 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 escopo 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.

A escolha de uma opção metodológica não ocorre sem controvérsias, lembrando, por exemplo, a discussão apresentada por Vertzman (2013) quando o autor argui a exatidão em comparar *"sujeitos"* de pesquisas e o tradicional dilema da perspectiva e interesse da generalização, amplamente discutido com relação aos estudos de casos únicos, como apresentado por Silva et al. (2009). É importante ressaltar que Vertzman (2013) refere-se a estudos em que pacientes em tratamento clínico são os casos a serem estudados, portanto caracterizando uma amostra expressivamente difícil de ser delimitada por critérios metodológicos simples e, neste estudo, adota-se uma postura de não se pretender a generalização potencial dos resultados encontrados, outrossim de permitir a continuidade das discussões em torno do infindável tema de segurança informacional. Importa realçar que mesmo os procedimentos regulatórios citados, para que se defina o desafio da generalização, ainda se encontram imersos nas dinâmicas de políticas nacionais, transnacionais e de mercado, configurando a dificuldade potencial de uma pretensa generalização, que incide em expectativa para novos estudos que possam decorrer do presente, reforçando a sua oportunidade.

Portanto, diante das questões levantadas, principalmente considerando que a amostra selecionada atende aos quatro quesitos apresentados, a decisão de uso de técnica metodológica de estudo de múltiplos casos tem fundamento e possibilitou a obtenção síncrona de resultados aos objetivos definidos.

No primeiro momento, em todas as empresas, montou-se um comitê de segurança (conselho de especialistas) com o objetivo de conduzir a implantação conforme descrito no modelo MAGIC. Importante salientar que em todas as empresas tomou-se o cuidado de convidar os diretores das mesmas para constituírem o comitê de modo a atender ao requisito primeiro do modelo (sensibilização da alta gestão).

Montado o comitê, foi realizada uma análise, através da aplicação de questionários (um de avaliação inicial e um segundo, cerca de doze meses após a aplicação do modelo e com o objetivo de avaliar os impactos), cujas questões contém todos os requisitos existentes nas normas ISO 27.001 e ISO 27.701, normas internacionais de segurança da informação e privacidade de dados pessoais, respectivamente. Essa etapa tem por finalidade conhecer como se encontravam as empresas no início do processo e, após a aplicação do modelo, o quanto houve de melhoria nos requisitos de segurança da organização. O questionário foi respondido pelo comitê de segurança, principalmente pelos gestores da área de TI das organizações.

Em paralelo à aplicação do questionário, todos os setores elaboram um relatório onde é estudado o fluxo da informação em cada processo, de cada setor específico. Desta forma torna-

se viável o estudo da análise de risco envolvido no tratamento das informações nas organizações.

De posse desses dados, são traçados planos de ação visando atender aos requisitos das normas e mitigar os riscos encontrados nos processos analisados em conjunto com o comitê de segurança. Dentro dos planos traçados para todas as organizações, é descrito um plano de treinamentos de temas envolvidos da área de gestão, proteção e privacidade de dados, para que todos os elementos da organização tenham consciência e conheçam os conceitos e saibam como aplicá-los no cotidiano empresarial.

Para uma melhor compreensão dos casos estudados, apresentam-se de forma sucinta as cinco empresas:

Empresa 1: Empresa da área de advocacia, considerada empresa de médio porte e tem aproximadamente 60 funcionários.

Empresa 2: Empresa da área de publicidade e propaganda, classificada de médio porte e conta com cerca de 60 funcionários.

Empresa 3: Empresa da área de consultoria para extração mineral de pequeno porte, com aproximadamente 11 funcionários.

Empresa 4: Empresa da área de advocacia, considerada de grande porte e que conta com cerca de 1600 funcionários.

Empresa 5: Empresa do ramo de supermercados, considerada empresa de grande porte e tem aproximadamente 26.000 funcionários.

RESULTADOS

Conforme descrito acima, após a aplicação dos questionários, foram elaborados gráficos que servem de guia na busca 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 ao porte e complexidade dos dados tratados pela empresa.

O questionário foi aplicado no início do trabalho de adequação e 12 meses depois, com o objetivo de avaliar a evolução e eficácia do método. Além disso, foi utilizado o critério de avaliação em cada empresa, onde foram analisados os requisitos necessários e atribuídas as notas conforme demonstrado no quadro 1.

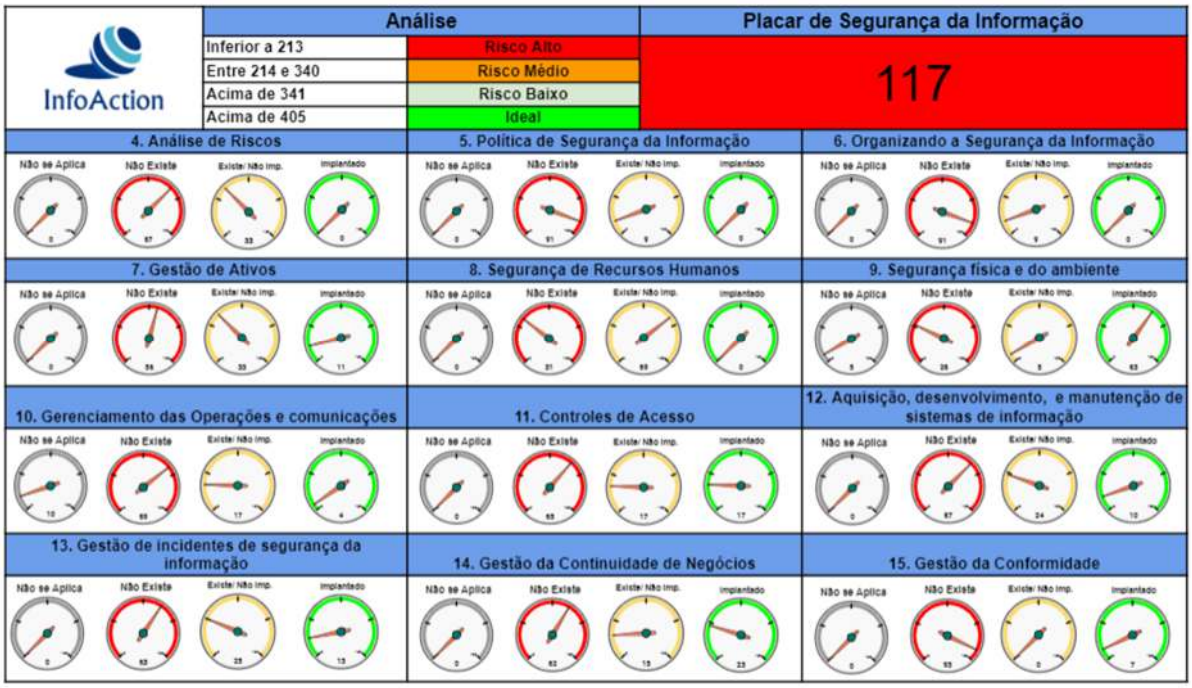
Quadro 1: Critério de avaliação para adequação aos requisitos das normas

Critério	Nota aplicada
Não existe nada implantado	0
Existe a documentação mas não está implantado	1
Existe implantado mas não tem documentação (evidências)	1
Existe implantado e documentado	2
Não se aplica	2

Seguidamente serão apresentados os resultados das avaliações - inicial e final - das cinco empresas objeto de análise no presente trabalho, com recurso a gráficos.

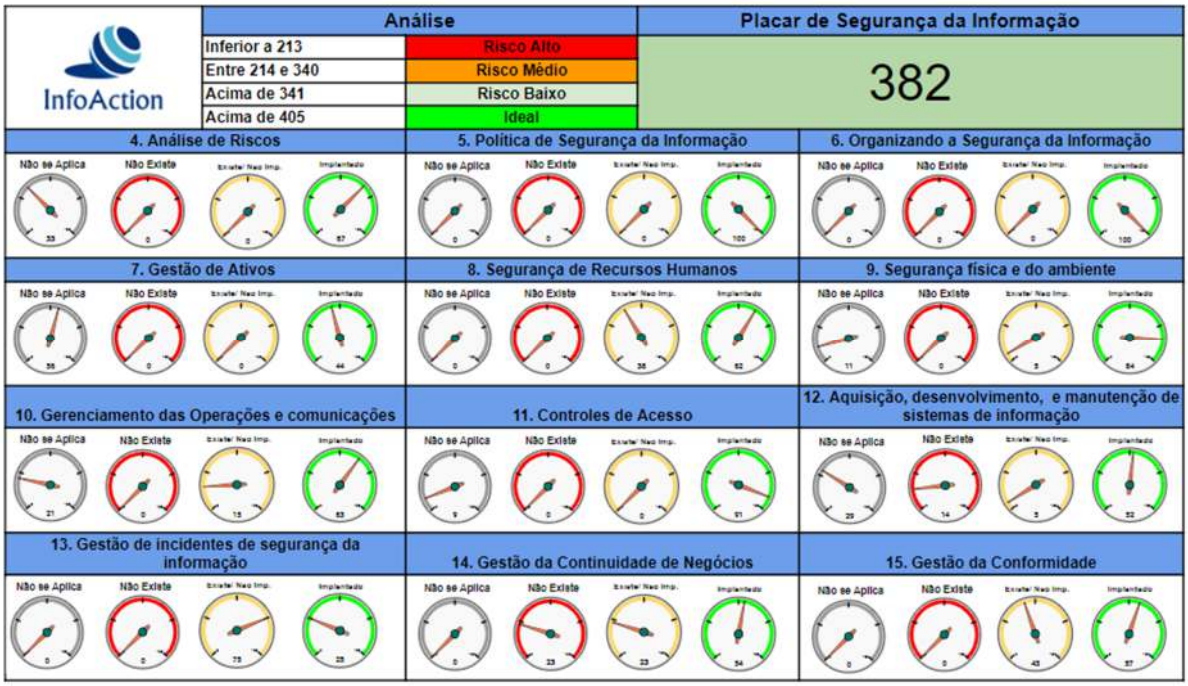
A empresa 1, como é possível verificar a partir da análise das figuras 2 e 3, apresentou uma melhoria significativa nos requisitos de segurança da organização. Na avaliação inicial obteve 117 pontos, o que significa que apresentava um risco alto (a classificação mais baixa de quatro níveis) e, consequentemente, 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: Avaliação inicial da empresa 1



Fonte: os autores

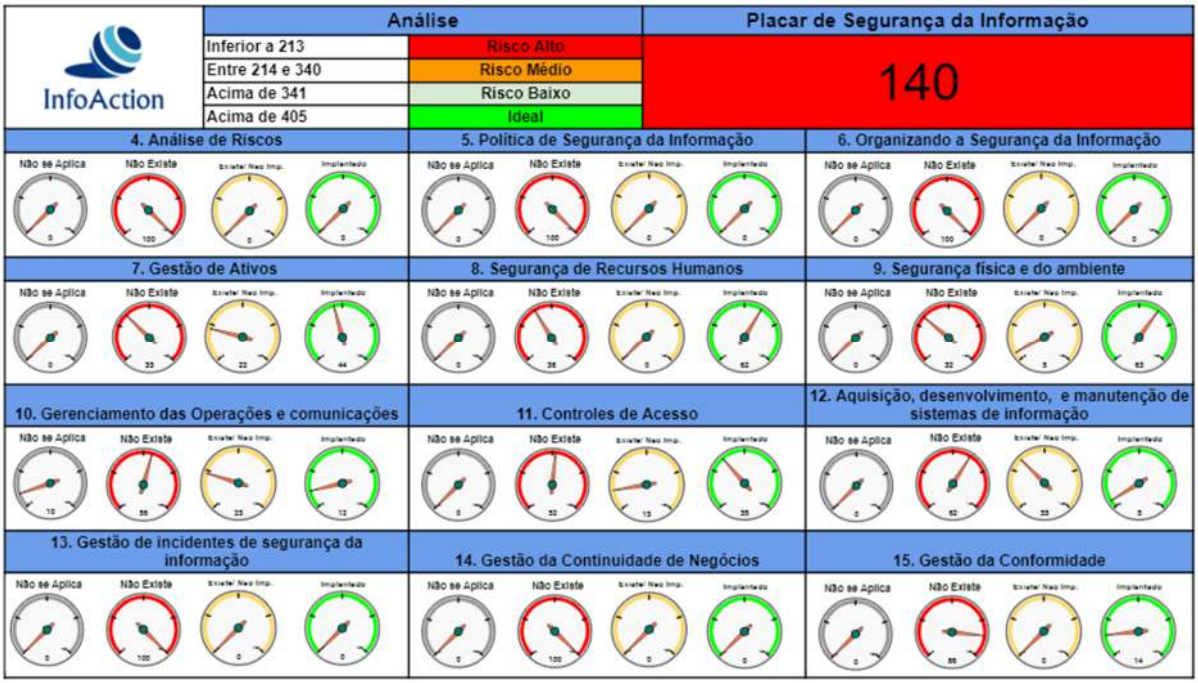
Figura 3: Avaliação Final da empresa 1



Fonte: os autores

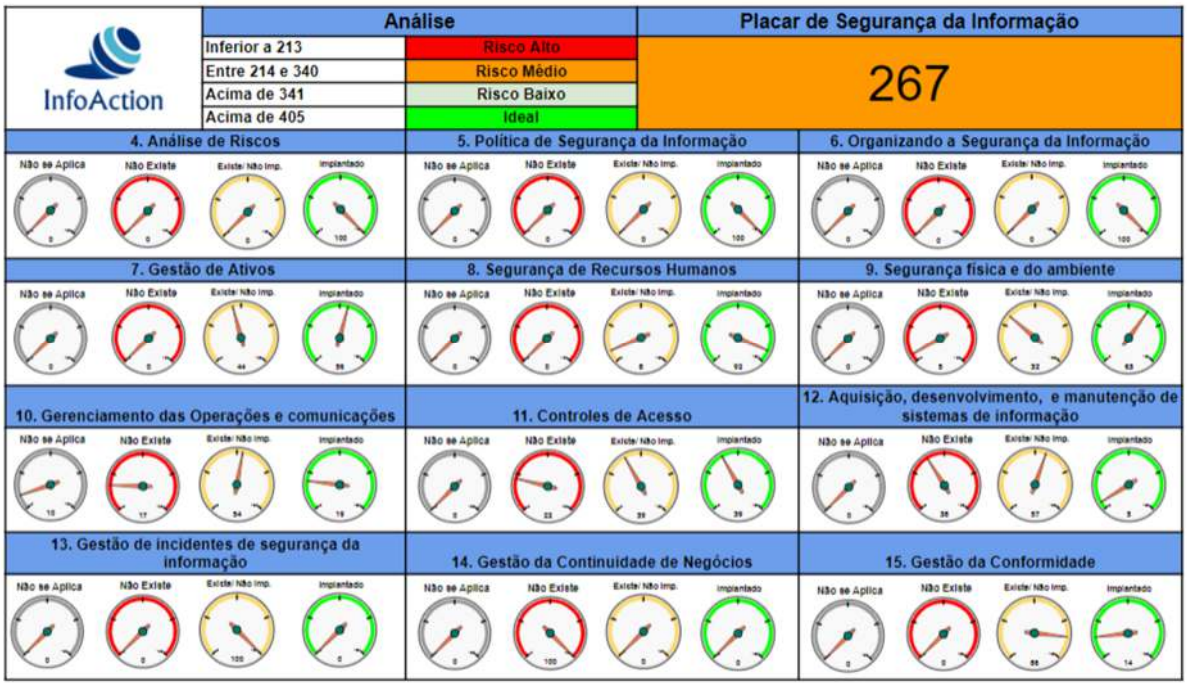
As figuras 4 e 5 permitem constatar uma ligeira melhoria na empresa 2, tendo passado dos 140 pontos para 267, ou seja, passou do nível de risco alto para o de risco médio após a aplicação do modelo MAGIC.

Figura 4: Avaliação inicial da empresa 2



Fonte: os autores

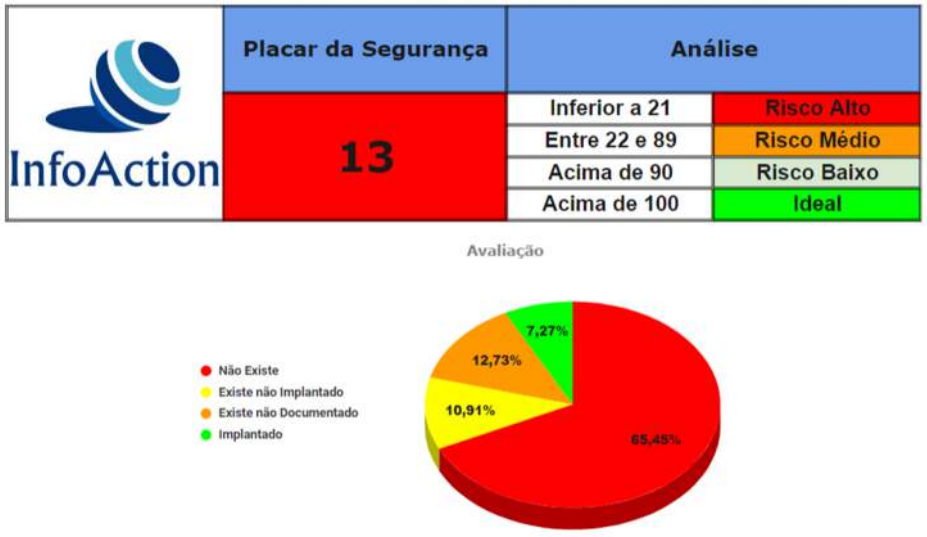
Figura 5: Avaliação Final da empresa 2



Fonte: os autores

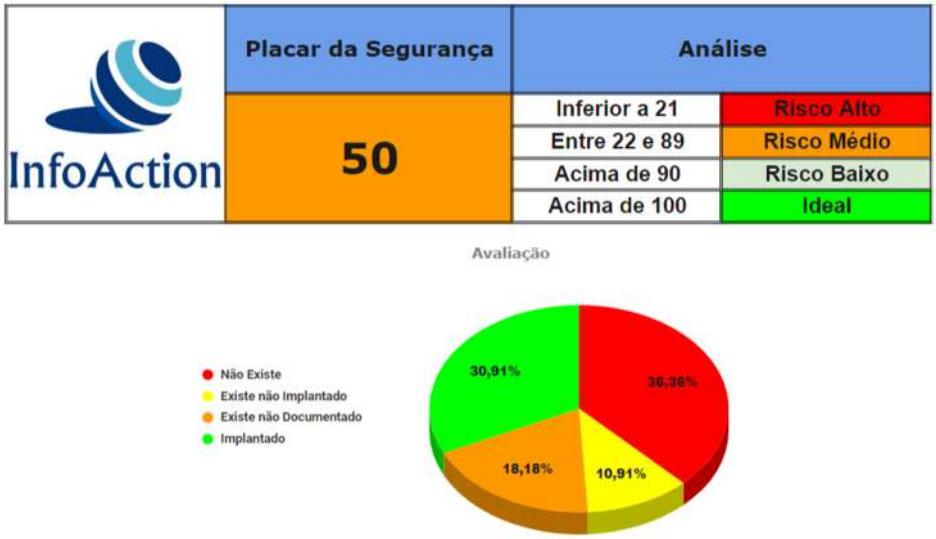
No que se refere à empresa 3, conclui-se a partir da observação das figuras 6 e 7, que se verificou um incremento da proteção e segurança da informação da empresa uma vez que passou de 13 valores, na avaliação inicial, para 50 após 12 meses de trabalho de adequação (passou do nível de risco alto para o de risco médio). Esta é a empresa de menor dimensão das cinco estudadas (trata-se de uma empresa de pequeno porte, que emprega 11 funcionários), e desenvolve atividades na área de consultoria para extração mineral. Importa salientar que, sendo uma empresa de pequeno porte, os requisitos exigidos em relação aos parâmetros de segurança são em número menor. Perante estas características o questionário administrado foi diferente do aplicado às restantes empresas.

Figura 6: Avaliação inicial da empresa 3



Fonte: os autores

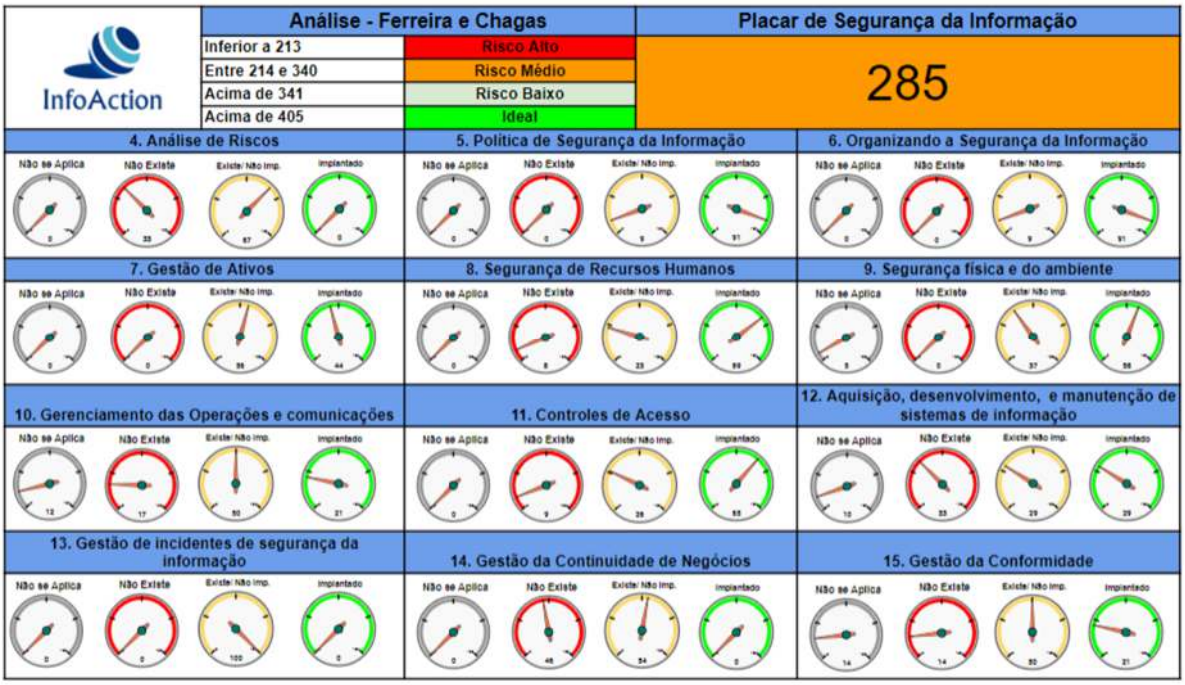
Figura 7: Avaliação Final da empresa 3



Fonte: os autores

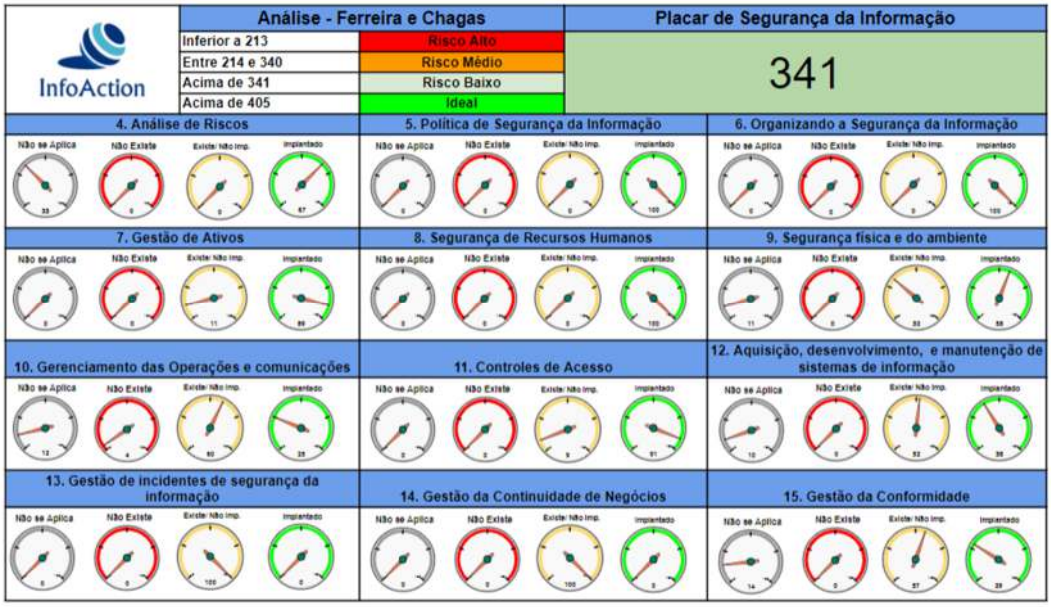
As figuras 8 e 9 demonstram que a empresa 4 apresentou uma melhoria importante a nível de segurança da informação. Passou de uma nota inicial de 285 (risco médio, o segundo nível mais baixa da escala de quatro níveis) para 341 pontos, doze meses depois, situando-se no nível 3 da classificação, ou seja, risco baixo.

Figura 8: Avaliação inicial da empresa 4



Fonte: os autores

Figura 9: Avaliação Final da empresa 4



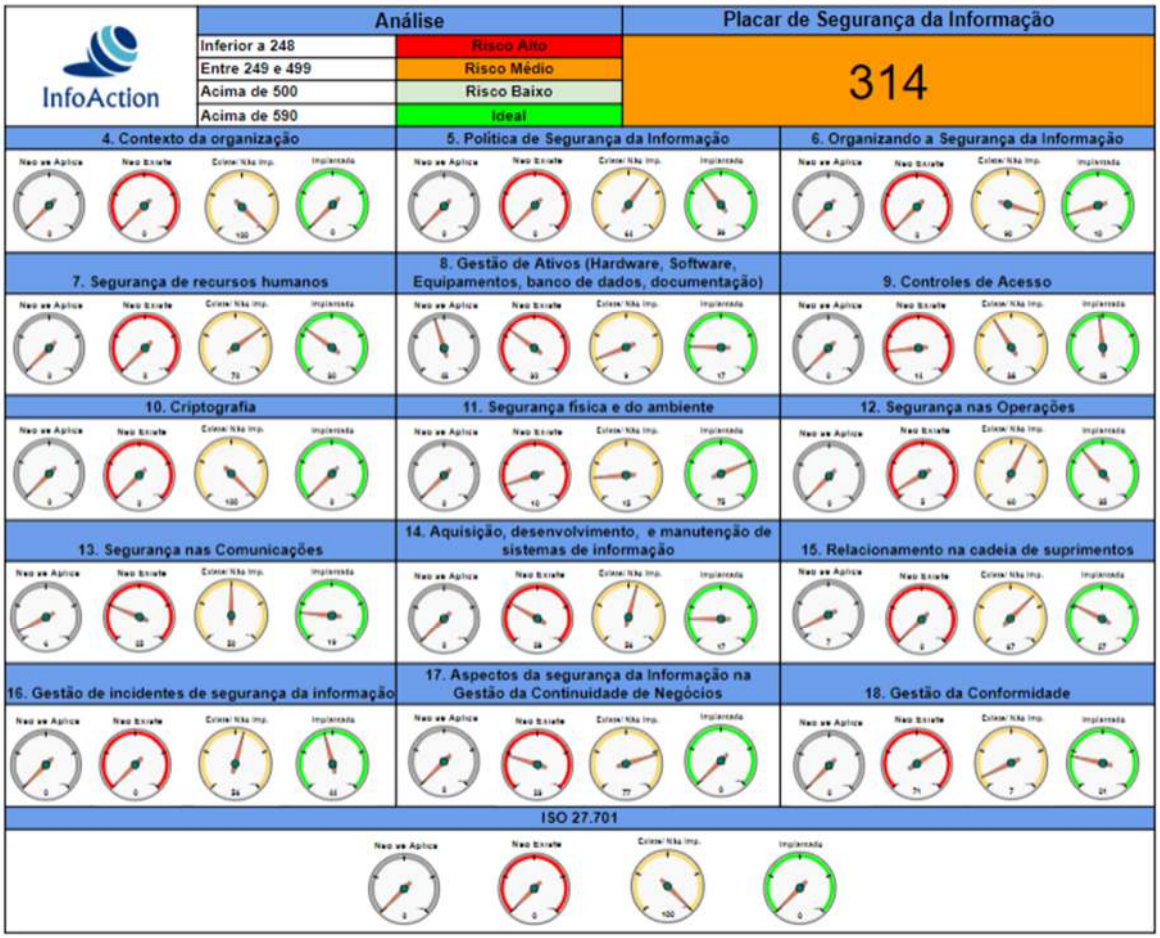
Fonte: os autores

A empresa 5 apresentou uma ligeira melhoria na avaliação da segurança da informação. Na avaliação inicial obteve uma nota de 189 (figura 10), ou seja, risco alto, e, na avaliação final alcançou 314 pontos (figura 11), situando-se no nível 2 da classificação, ou seja, risco médio.

Figura 10: Avaliação inicial da empresa 5

Fonte: os autores

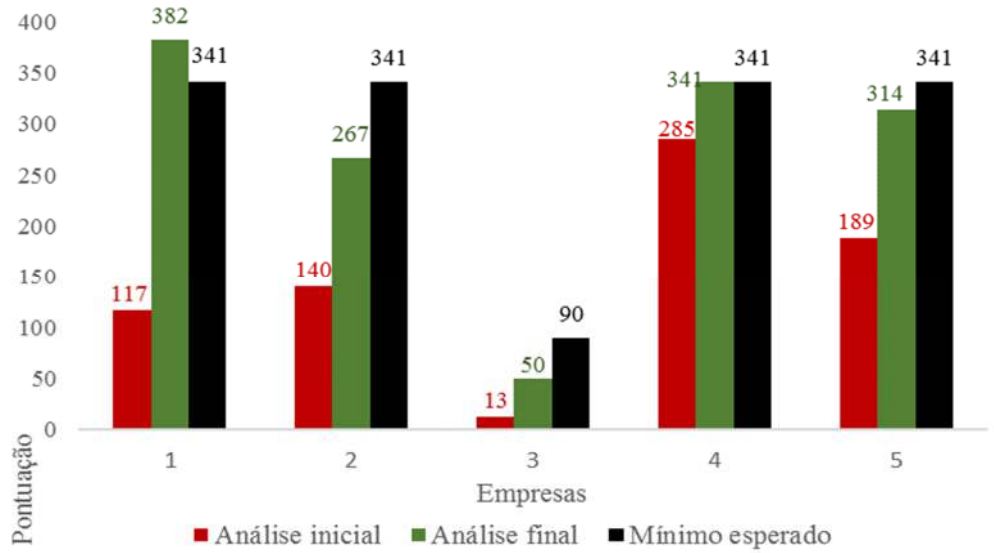
Figura 11: Avaliação Final da empresa 5



Fonte: os autores

Em suma, tal como evidenciado na figura 12, todas as empresas objeto de estudo registaram melhorias a nível de segurança da informação. Comparando o mínimo esperado definido e a classificação obtida na análise final, 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.

Figura 12: Resumo dos resultados obtidos



Fonte: os autores

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 engajamento da alta gestão: ficou evidente ao longo do trabalho que, conforme demonstrado no modelo MAGIC em seu primeiro momento, é necessário um engajamento dos gestores das organizações para que o trabalho flua de forma natural na busca da conformidade. Nas empresas onde os gestores atuaram de forma eficaz (empresas 1 e 4) a melhoria do resultado é significativa. E isso é independente do porte da empresa, pois vemos que as demais empresas, cujos gestores não tiveram essa sensibilidade (mesmo na empresa 3 considerada de pequeno porte) a melhoria não foi como esperado.

2) Engajamento de toda equipe: como era de se esperar, o engajamento da equipe (em especial do comitê de segurança) também é essencial na busca do sucesso da implantação. E também se aplicará aqui a regra da necessidade dos gestores estarem alinhados ao comitê de segurança, pois, nas mesmas empresas onde os gestores não participaram ativamente, os líderes dos setores que compõem o comitê de segurança não tiveram o mesmo senso de necessidade e responsabilidade para fazer com o que a conformidade fosse atingida no tempo proposto. Houve, por parte da equipe de implantação, uma dificuldade em fazer os processos evoluírem como deveriam.

3) Melhoria dos resultados: os resultados apresentados demonstram a eficácia da aplicação do modelo, independentemente dos problemas encontrados. Em todos os casos, com exceção da empresa 4 onde já existia um processo mais evoluído devido ao seu porte e exigências de seus clientes para a segurança dos dados tratados, as empresas se encontravam com um nível de conformidade baixo e, após aplicado o modelo, os resultados melhoraram de forma considerável. Mesmo naquelas empresas em que o resultado não chegou ao nível esperado pelo tempo de implantação se registou uma melhoria.

4) O tamanho da empresa não é o fator preponderante: é possível afirmar isso com base em duas análises distintas:

    a) A empresa 1 é uma empresa de porte médio, na qual houve um engajamento grande dos gestores e, consequentemente, do comitê de segurança. A empresa se encontrava em um nível de conformidade baixo, porém, dentre as empresas analisadas, foi a que teve uma melhoria considerável, chegando inclusive aos níveis desejáveis de conformidade dentro do prazo estabelecido.

    b) A empresa 5, empresa de grande porte, com isso era esperado um nível inicial maior de conformidade e um engajamento maior de seus líderes, devido ao fato de estarem melhores preparados em termos de gestão e conhecimento, não tiveram o resultado esperado. Houve uma demora significativa para que os líderes iniciassem os mapas de processos, as análises necessárias e consequentemente a geração de um plano de ação que é utilizado para mitigar os riscos e aumentar o índice de conformidade. Isso impediu que o resultado atingisse o índice esperado para tal empresa.

CONCLUSÃO

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. O modelo MAGIC tem vindo a ser aplicado com bons resultados em diversas empresas de portes e áreas diferentes com bons resultados, tendo demonstrado ser eficiente para orientar os gestores na busca da melhoria da gestão e proteção de suas informações.

Tal como evidenciado, na aplicação do modelo, a sensibilização da alta gestão das organizações é um fator crítico e fundamental para o sucesso da sua implantação porque influencia diretamente o nível de engajamento dos líderes da empresa (comitê de segurança) e, consequentemente, os demais profissionais envolvidos no processo de adequação. Os resultados apresentados demonstram que sem o engajamento da equipe e, principalmente da alta gestão, os resultados não são atingidos dentro do prazo esperado.

Parece igualmente evidente que o porte da empresa não será o fator preponderante de sucesso. A complexidade das informações tratadas, bem como o preparo da equipe para levantamento e análise de processos é fundamental para tal. Isso cria a necessidade do uso de algum modelo (guia) que levará ao sucesso da implantação. O modelo MAGIC se mostra eficaz nesse aspecto porque alinha a gestão da organização, as informações envolvidas, as ferramentas e os métodos na busca dos resultados esperados, e, caso aplicado devidamente, conforme pode ser observado especialmente nas empresas 1 e 4, os resultados atingem 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.

Capurro, R. (2003). Epistemologia y Ciencia de la Información. In: *Encontro Nacional de Pesquisa em Ciência da Informação: ENANCIB*, 5. Anais... Belo Horizonte: ECI/UFMG, 2003. Disponível em: http://www.capurro.de/enancib_p.htm . Acesso em: 17 abr. 2017.

Detlor, B. (2010). Information Management. *International Journal of Information Management*. v. 30, n. 2, p. 103-108. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0268401209001510. Acesso em 13 mar 2022.

Estrela, S. C. L. (2016). *Gestão da Informação na Tomada de Decisão: Estudo em PME da Região Centro.* Faro: Sílabas & Desafios.

Febraban (2021, novembro 1). Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais. https://febraban.org.br/noticia/3704/pt-br/, acessado em 14/09/2022.

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, com acesso em outubro de 2022.

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. (2014). Estruturação de Oficina de Inteligência de Mercado. In: Almeida, A. S. de A., Silva, A. M., Franco, M. J. B., & Freitas, C. C. de (Orgs.), *Coletânea Luso–Brasileira V: Gestão da Informação, Cooperação em redes e Competitividade*. Porto: Universidade do Porto.

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.

Marchand, D. A., Ketinger, W. J., & Rollins, J.D. (2001). *Information Orientation: The Link to Business Performance*. Oxford University Press.

Moresi, E. A. D. (2000). Delineando o valor do sistema de informação de uma organização.*Ci. Inf., Brasília, 29*(1), 14-24. https://doi.org/10.1590/S0100-19652000000100002

Pessoa, C. R. M. (2016). *Gestão da Informação e do Conhecimento no Alinhamento Estratégico em Empresas de Engenharia*. [Tese de Doutorado, Universidade Federal de Minas Gerais, 2016]. https://repositorio.ufmg.br/bitstream/1843/BUOS-AMXG58/1/tese_de_cl_udio_pessoa_.pdf

Pinto, M. M. A., Silva, A. M. da (2005). Um modelo sistémico e integral de gestão da informação nas organizações. *2º CONTECSI.* p. 1–24.

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

Silva, A. M. da. (2006). *A informação: Da compreensão do fenómeno e construção do objecto científico.* Porto: Afrontamento.

Silva, A. M. da., & Ribeiro, F. (2009). *A gestão da informação na Administração Pública. Interface, 50*(161), 32-39.

Silva, F. C. C., Silva, M. V. D., & Souza, R. S. (2009). O método de estudo de caso: O sim e o não, talvez. A controvérsia da utilização do método de estudo de caso nas pesquisas em contabilidade e administração. *Anais do XVI Congresso Brasileiro de Custos*. Fortaleza, novembro de 2009.

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

Verztman, J. S. (2013). Estudo psicanalítico de casos clínicos múltiplos. In A. M. Nicolaci-da-Costa, & D. R. Romão-Dias (Orgs.), *Qualidade faz diferença: Métodos qualitativos para a pesquisa em psicologia e áreas afins* (pp. 67-92). Rio de Janeiro: Loyola.

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