DOI: 10.5102/un.gti.v7i1.4192

Análise estratégica das políticas de segurança da informação no setor bancário*

Strategic analysis of information security policies in the banking sector

Mauricio Rocha Lyra[1]
Vitor Tormin Nishi [2]

Resumo

Este trabalho pretende apresentar uma análise, do ponto de vista estratégico, baseado em preceitos do CoBIT 5 for Information Security, das políticas de segurança da informação no setor bancário. Buscou-se, por meio de 12 princípios de governança propostos na publicação da ISACA, avaliar quão alinhados se encontram os aspectos estratégicos com os aspectos táticos/operacionais da segurança nas políticas de segurança da informação. Como esperado, o estudou mostrou um índice de aderência aos preceitos de governança inferior a 50% nas organizações e evidenciou que, mesmo entre elas, existe uma grande diferença entre os níveis de aderência quando comparadas uma a uma. O entendimento final do trabalho leva a acreditar que existe um desalinhamento entre o negócio e a segurança, que, ainda, é muito vinculada aos conceitos conservadores de segurança, ignorando a vantagem competitiva de mercado que a segurança pode prover e não se atentando que a segurança envolve o negócio como um todo e não, apenas, TI e que ferramentas são os meios e não os motivadores da segurança.

Palavras-chave: Política de Segurança da Informação. Cobit 5 for Information Security. Governança da Segurança da Informação.

Abstract

This paper intends to present a strategic analysis, based on the precepts of CoBIT 5 for Information Security, of information security policies in the banking sector. Through the 12 principles of governance proposed in the ISACA publication, it was sought to assess how aligned are the strategic aspects with the tactical / operational aspects of security in information security policies. As expected, the study showed an adherence index to governance precepts of less than 50% in organizations and showed that, even among them, there is a big difference between levels of adherence when compared one by one. The final understanding of the work leads one to believe that there is a misalignment between the business and security, which is also closely linked to the conservative concepts of security, ignoring the competitive market advantage that security can provide and not taking into account that security involves the business as a whole and not just IT and what tools are the means and not the motivators of security.

Keywords: Information Security Policy. Cobit 5 for Information Security. Governance of Information Security.

* Recebido em: 12/08/2016.
Aprovado em: 23/03/2017.

[1] Doutor em ciência da Informação pela UnB. Professor dos cursos de graduação e Pós-graduação do UniCEUB. Profissional da área de segurança da informação atuando tanto na área privada quanto pública.

[2] Aluno da Pós-graduação do UniCEUB.

1 Introdução

A informação é o ativo mais importante de uma corporação e a segurança dos dados, desde sua criação até seu fim, devem ser controlados, protegidos e geridos dentro da organização. A segurança da informação ganha cada vez mais importância, uma vez que os riscos relacionados à informação aumentam na medida que o potencial de extração de informação dos dados se torna mais contundentes.

Os aspectos de confidencialidade, integridade, e disponibilidade da informação são conceitos, globalmente, aceitos que devem ser considerados ao projetar uma estrutura de segurança da informação corporativa.

Dentro de uma visão apresentada no Cobit 5, a informação é um dos mecanismos-chave para habilitar a governança corporativa, sendo, por vezes, o principal produto de uma organização. Ela permeia todas as áreas corporativas e a sua segurança é intimamente ligada a temas como os riscos do negócio e geração de valor competitivo para organização.

Princípios, políticas e frameworks, também, segundo a visão do Cobit 5, são outros habilitadores da governança dentro de uma organização e são os veículos para disseminar na corporação o comportamento desejado pela alta direção.

A política de segurança da informação reflete os desejos do board relacionados à segurança e é o insumo primordial para iniciar e manter um sistema gerenciamento de segurança da informação corporativa. A política direciona como a estrutura de segurança será projetada, como ela deve se comportar e como será gerenciada.

As normas ISO 27001 e ISO 27002 são os padrões utilizados na construção de políticas da segurança da informação corporativas, porém, em 2010, um consórcio formado pelo ISACA, ISF e Internacional Information System Security Certification Consortium [(ISC)2], propôs 12 princípios de governança a serem utilizados na construção de políticas de segurança da informação em conjunto com as normas ISO.

Os 12 princípios de governança propostos têm um foco no alinhamento estratégico corporativo com a segurança da informação, visando à agregação de valor por meio da segurança e de refletir o desejo estratégico do board empresarial na corporação.

Dentre os pilares econômicos de uma sociedade, o setor bancário se mostra como um dos mais importantes, sendo sua saúde muitas vezes o indicativo de confiabilidade, segurança e integridade de um governo.

A segurança da informação no setor bancário, devido à importância do setor para um país, é regulada com rigor pelas instituições governamentais e deveria ser considerada como prioridade estratégica na organização, não só abordando os riscos que rodeiam a informação e a protegendo, mas, também, buscando gerar valor para corporação por meio de ganhos competitivos sobre seus concorrentes, provendo um maior alinhamento da estratégia e objetivo corporativos com as necessidades de segurança da informação que o negócio demanda.

Este estudo se propõe a avaliar as políticas de segurança da informação de instituições bancárias, determinando, por meio de uma escala, o nível de aderência das políticas de segurança da informação aos 12 princípios de governança propostos, assim, avaliando quão alinhado com a estratégia corporativa as políticas de segurança da informação das instituições estão e dando uma noção do nível de prioridade que a segurança da informação é tratada e vista dentro das corporações.

O objetivo da pesquisa é determinar, primariamente, qual o foco primário das políticas analisadas, ou seja, se estas estão ou não alinhadas com os objetivos estratégicos da organização, se o desejo transmitido é, apenas, garantir a segurança dos dados ou, também, de procurar alinhar essa garantia de segurança com as necessidades estratégicas da corporação.

Secundariamente, este estudo pretende identificar, por meio da escala de aderência das políticas aos 12 princípios de governança propostos, quais áreas, dentre as 3 áreas nas quais os princípios são divididos, as corporações focaram mais ou menos na construção de suas políticas, fornecendo insumos para uma avaliação de qual direção as organizações devem seguir no intuito de procurar um maior alinhamento estratégico com a segurança da informação.

2 Metodologia

O setor bancário é um dos setores mais legislados, regulados, fiscalizados e competitivos de uma economia.

A similaridade entre os serviços ofertados pelas instituições e os preços cobrados por estes, tende a obrigar, cada vez mais, corporações a buscar melhorias tecnológicas e processuais de forma garantir sua competitividade no mercado.

As estratégias corporativas dessas instituições têm um papel fundamental na competitividade do setor, tornando-se o diferencial na obtenção de lucros.

Excelência operacional, qualidade dos serviços e inovação tecnológica são alguns dos fatores que determinam os resultados financeiros positivos, mesmo em tempos de crise.

A governança da segurança da informação, também, deve, ou deveria ser, um foco da estratégia corporativa, mitigando riscos operacionais, garantido a proteção dos ativos informacionais da instituição, prevenindo fraudes e assegurando a entrega de informações integras e oportunas para a tomada de decisão estratégica do *board* diretivo bancário.

Buscando dentro do setor uma variedade de empresas públicas e privadas, foram selecionadas as políticas de segurança da informação das instituições, conforme Figura 1.

Figura 1 - Instituições Financeiras

CAIXA	Caixa Econômica Federal • Empresa Pública
BANCO DO BRASIL	Banco do Brasil • Sociedade de Economia Mista
Banco de Brasília BRB	Banco de Brasília • Sociedade de Economia Mista
Itaú	Itaú • Sociedade Anônima
Bradesco	Bradesco • Sociedade Anônima
Santander	Santander • Sociedade Anônima

Fonte - O Autor

A Caixa Econômica foi escolhida pelo fato de se manter, ainda, como uma empresa pública, diferentemente das outras 2 instituições financeiras públicas selecionadas, ou seja, todo controle acionário e capital pertence ao governo federal.

O Banco do Brasil foi escolhido, além do fato de ser uma Sociedade de Economia Mista, ou seja, o capital não é integralmente público e parte do controle acionário não pertence ao governo, também pesou o fato de ser uma das três maiores instituições financeiras do Brasil.

Seguindo a mesma linha, o Banco de Brasília foi escolhido por se tratar de uma Sociedade de Economia Mista, porém, com uma atuação mais modesta e regional que os outros dois bancos públicos escolhidos.

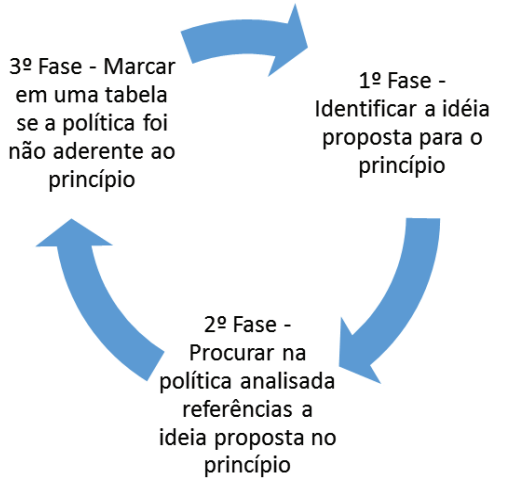
O Itaú e Bradesco foram escolhidos por se tratarem de dois dos maiores bancos privados do país e ambos vem travando uma batalha ao longo dos últimos anos pelo posto de maior instituição financeira do país.

O Santander foi escolhido por se tratar um banco privado com origem e controle estrangeiro. Escolhidas as instituições financeiras, as políticas foram adquiridas com pesquisa nos sites web das instituições financeiras privadas e as públicas o acesso foi conseguido através da Lei Federal nº 12.527/2011.

A Lei Federal nº 12.527/2011, conhecida como Lei de Acesso à Informação ou LAI é um dispositivo de transparência que permite que a população tenha acesso a informações de instituições públicas, desde que estás informações não sejam confidenciais ou de cunho estratégico. Todas as instituições públicas são obrigadas a manter, em seus sites, um link de acesso a ferramentas de requisição de informações daquela instituição.

As políticas foram analisadas de acordo com os princípios propostos pela ISACA (2012) e a análise foi conduzida da forma apresentada na Figura 2.

Figura 2 - Processo de Avaliação das Políticas



Fonte: O Autor.

Na primeira fase, cada um dos princípios foi analisado, individualmente, e sua ideia principal extraída conforme apresentado na Figura 3.

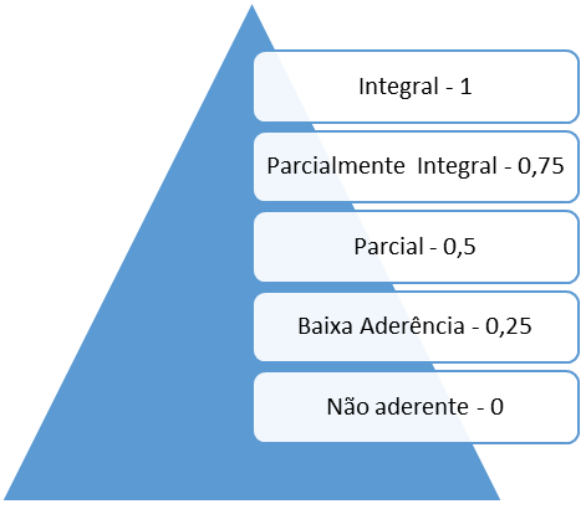
Figura 3 - Ideias dos Princípios

SN01 - Foco no Negócio	A política deve apresentar a ideia que a segurança deve ser um pilar de apoio dos processos de negócio e de gerenciamento de riscos, adotando uma postura de conselheira para suportar os objetivos de negócio, protegendo a informação e gerenciando o risco hoje e no futuro
SN02 - Entregar Valor e Qualidade as Partes Interessadas	A política deve engajar as partes interessadas na segurança através de uma comunicação regular que ajude a verificar se suas expectativas estão sendo atigindas. Promover os benefícios financeiros e não financeiros da Segurança da Informação ajuda a segurança no auxilio da tomada de decisão, o que pode aumentar o sucesso da visão de segurança na corporação
SN03 - Aderência aos requerimentos legais e regulatórios	Aderência aos requerimentos legais e regulatórios deve ser explita na política. As penalidades associadas a não aderência aos requerimentos deve ser claramemente apresentada e controles devem ser planejados prevendo mudanças nos requerimentos legais e regulatários
SN04 - Prover informações oportunas e precisas sobre a performance da segurança	Requerimentos de performance de segurança devem ser claramente definidas e suportadas por metricas precisas e objetivas, alinhadas com o negócio. A informação da performance deve ser buscada periodicamente, consistentemente e rigorosamente, buscando a precisão e atendendo os objetivos relevantes para os stakeholders
SN05 - Avaliar as ameaças atuais e futuras a informação	As ameaças devem ser categorizadas em um framework de fácil entedimento, cobrindo diversas fontes de ameaça, como ameaças políticas, legais, econômicas, técnicas e outras. Individuos devem dividir e construir seus conhecimentos sobre as ameças à informação, endereçando suas causas e não apenas os sintomas
SN06 - Promover a melhoria continua da segurança da informação	A segurança da informação deve estar em constante adaptação as mudanças organizacionais. O conhecimento deve ser melhorado constantemente com base nos incidentes de segurança e auditorias independentes
DN01 - Adotar uma abordagem baseada em riscos	As opções de endereçamento dos riscos devem ser revisadas constantemente para que as decisões de tratamento de riscos sejam propriamente tratadas
DN02 - Proteger informações confidenciais	A política deve trazer que a informação deve ser classificada e protegida de acordo com seu nível de confidencialidade, durante todo seu ciclo de vida e com todos os meios necessários para tal
DN03 - Concentrar nas aplicações críticas do negócio	A politica deve prever o impacto no negócio da perda ou disponibilidade de informações por suas aplicações e determinar quais aplicações devem ser priorizadas em sua proteção
DN04 - Desenvolver sistemas de forma segura	A política deve apresentar a ideia que a segurança de informação deve estar presente em todos os estágios do desenvolvimento de sistemas. Desde o desenho, construção e teste, sempre procurando estar embasado pela boas práticas de mercado
PC01 - Agir de forma ética e profissional	A política deve mostrar que a segurança da informação depende fortemente das habilidades dos profissionais em desempenhar suas responsabilidades e na sua integridade em proteger as informações que estes são responsáveis. Demostrando um comportamento ético em pró do negócio, em detrimento de necessidade pessoais e individuais
PC02 - Estimular uma cultura positiva da segurança da informação	O foco deve ser em promover a segurança da informação como uma parte fundamental do negócio, cultivando nos usuários o entendimento dos riscos que a informação sobre sua tutela esta submetida e fornecendo o conhecimento e poder necessário para eles protegerem as mesmas

Fonte: O Autor

Na segunda fase, as ideias dos princípios serão buscadas dentro das políticas, de forma integral ou parcial, sendo classificadas de acordo com a escala apresentada na Figura 4.

Figura 4 - Escala de Aderência



Fonte: O Autor

Os dados serão tabulados de acordo comas notas obtidas, em que serão atribuídas notas relativas ao desempenho de aderência aos princípios a cada política, assim obtendo um parâmetro quantitativo de comparação entra a aderência das políticas aos princípios.

Essa classificação, também, servirá para avaliar o desempenho da quantidade de princípios aderentes em relação ao tamanho da política para se ter uma dimensão da concisão e atomicidade das políticas.

Os resultados tabulados serão avaliados do ponto de vista da eficácia e eficiência das políticas na transmissão dos princípios de governança.

Para avaliação da eficácia das políticas, foi avaliado o desempenho obtido nos quesitos Total SN, Total DN, Total PC, Total Geral e Percentual Cobertura, comparando entre as políticas o desempenho obtido em cada um dos quesitos.

O Total SN equivale a soma dos pontos obtidos nos princípios do grupo Suporte ao Negócio, o Total DN equivale a soma pontos obtidos no grupo Defender o negócio, o Total PC equivale a soma dos pontos obtidos no Grupo Promover Comportamento, o Total Geral equivale à soma dos pontos obtidos no Total SN, Total DN e Total PC e por último o Percentual Cobertura equivale ao percentual do Total Geral dividido pelo número máximo de pontos possíveis, ou seja, pela fórmula:

$$\frac{Total\ Geral}{12} x100$$

Para avaliar a eficiência das políticas, foi considerado o indicador de quantidade de palavras dividido pelo percentual de cobertura, como apresentado na fórmula:

$$\frac{\text{Qtd Palavras}}{\text{Percentual Cobertura}}$$

Essa comparação irá prover os subsídios para extrapolar e inferir se os resultados estão de acordo com o esperado, quais motivos levaram ao desempenho alcançado em relação ao nível de aderências aos princípios de cada política e sugestões de como as instituições poderiam otimizar o desempenho das políticas em relação a aderência aos princípios.

3 Análise e Resultados

Seguindo os procedimentos propostos na metodologia, temos a Tabela 1, que mostra os resultados das análises realizadas nas políticas de segurança.

Tabela 1 - Resultados

	BB	Caixa	BRB	Itaú	Bradesco	Santander
SN01	0	0,5	0,5	0	0	0
SN02	0,25	0	0	0	0	0
SN03	1	0,75	0,25	0,75	0	0,75
SN04	0	0,5	0,5	0	0	0
SN05	0,25	0	1	1	0	0
SN06	0	0	0,5	0,5	0	0
Total SN	1,5	1,75	2,75	2,25	0	0,75
DN01	0	0	0,75	0	0	0
DN02	0,75	1	0	1	0	0
DN03	0,5	0,5	0,75	0	0	0
DN04	0	0	0	0	0	0
Total DN	1,25	1,5	1,5	1	0	0
PC01	0	0	0	0,5	0	0
PC02	0,25	0,75	1	1	0,5	0
Total PC	0,25	0,75	1	1,5	0,5	0
Total Geral	3	4	5,25	4,75	0,5	0,75
Qtd Palavras	445	1066	1174	1139	170	1975
Percentual de Cobertura	25%	33,33%	43,75%	39,58%	4,16%	6,25%

Fonte: O Autor

3.1 Análise de Eficácia

Nesta seção, iremos analisar a construção das políticas do ponto de vista da eficácia, ou seja, analisado os índices de cobertura dos princípios contidos nas políticas a fim de determinar quão eficientes elas são na transmissão dos princípios para os colaboradores.

Observando os resultados, o primeiro indicador que chama a atenção é o percentual de cobertura. Como pode ser visto, nenhuma instituição obteve 50% de aderência aos princípios de segurança propostos pela ISACA (2012), ou seja, do ponto de vista estratégico para o negócio, não existe um direcionamento explícito nas políticas que as leve para o caminho da entrega de valor.

De fato, como descrito por Von Solms (2005, p. 100), a expectativa ao analisar as políticas era de encontrar políticas mais acopladas as normas ISO 27001 e ISO 27002, ou seja, com foco no "como fazer", portanto, o desalinhamento em relação aos princípios de governança do COBIT era esperado, uma vez que o COBIT traz o foco no "porque fazer".

Porém, o fato de confirmar esse cenário é preocupante, corroborando, novamente, a ideia apresentada por Von Solms (2004, p. 372), uma vez que demonstra que as organizações, ainda, estão na contramão das vertentes de pensamento sobre a segurança da informação.

Tomando como exemplo o aspecto da construção da política, fica claro a tendência voltada aos processos do nível tático e operacional da tecnologia da informação e não a estratégia da instituição. Temas como tela limpa, uso de senhas e segurança de sistemas são mencionados com frequência. Porém, será que todos os colaboradores estão imersos em funções que tenham uma tela de computador? Utilizam senha de acesso? Ou fazem uso de sistemas baseados em software? Com certeza não, ou seja, a visão holística da segurança começa a se perder, focando estritamente na tecnologia da informação, com isso a segurança corporativa incorre no erro de delegar as áreas técnicas a responsabilidade pela definição da segurança, fato já mencionado por Von Solms (2004, p. 372) e na contramão do ideal proposto por Foina (2015).

Dentre as 3 instituições com melhores resultados, temos 2 organizações de capital majoritário público e 1 de capital majoritário privado e das 3 instituições com pior aderência temos 2 de capital majoritário privado e 1 de capital público, como podemos observar na Figura 5.

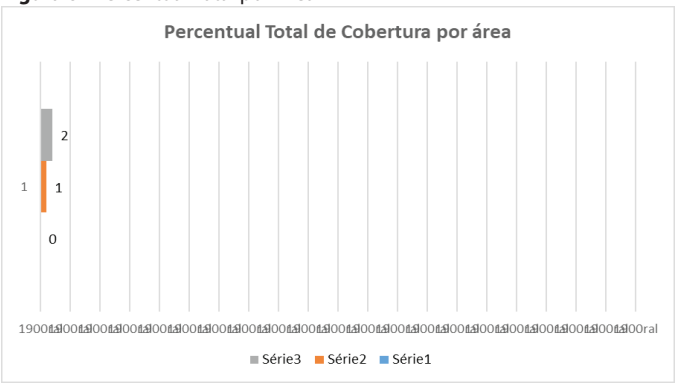
Figura 5 - Desempenho geral

Fonte: O Autor

Este resultado mostra que, diferentemente da cultura popular, as instituições públicas mostram uma preocupação maior com o alinhamento entre a segurança e o negócio, mesmo que ainda em fase insipiente.

Na Figura 6, temos uma visão geral, por área do desempenho de cada instituição.

Figura 6 - Percentual Total por Área



Fonte: O Autor

Analisando, de forma mais aprofundada cada área, temos a aderência das organizações dentro da área Suportar o Negócio, temos uma cobertura muito baixa dos princípios. O princípio 'SN2 - Entregar qualidade e valor para as partes interessadas para garantir que a segurança da informação agregue valor e atenda requisitos de negócios' não foi abordado por, apenas, uma das instituições e, mesmo assim, de forma quase nula.

Isto mostra, possivelmente, que a área segurança não é vista e não se vê como uma forma de entregar valor a organização e não existe uma preocupação em entender e atender as necessidades dos *stakeholders*. O que pode ser tomado como mais uma consequência do exposto por Von Solms (2004, p. 372), ou seja, a segurança, quando não planejada, juntamente à alta direção e sim pelas áreas tática e operacional, acaba por ter uma visão de sua função de forma estrita e não integrada com o propósito da organização.

Um reflexo da omissão desse princípio no direcionamento da segurança da instituição ocorre quando a área de segurança é vista pelos colaboradores de outras áreas como um setor incômodo, que só atrapalha o negócio e não agrega valor aos processos.

Outros princípios como o SN1, SN4 e SN6 também tiveram uma baixa aderência. Com no máximo 2 instituições abordando o tema e nenhuma delas abordando de forma completa.

O princípio 'SN1? Concentrar-se no negócio para garantir que a segurança da informação esteja integrada nas atividades essenciais de negócio' trata de um tema alinhado com o SN2 e como já discutido no princípio SN2, mostra que o alinhamento da segurança com o negócio, ainda, é insipiente nas instituições.

Já o princípio 'SN4 – Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação', também alinhado com o princípio SN2, reforça que a segurança da informação não se mostra propícia atender as necessidades das partes interessadas e apresentar resultados as partes interessadas de suas atividades, mostrando-se como um setor independente e autossuficiente da organização.

Analisando o princípio 'SN6 – Promover a melhoria contínua em segurança da informação para reduzir custos, melhorar a eficiência e efetividade, e promover uma cultura de melhoria contínua da segurança da informação', também, é, fortemente, ligada ao princípio SN2 e corrobora, mais uma vez, o desalinhamento da segurança com o negócio. Uma vez que a área de segurança tende a se ver de forma isolada da organização, é natural que exista uma dificuldade em perceber onde processos podem se tornar mais efetivos e eficazes. A ausência de feedbacks das partes interessadas tende a direcionar as áreas de segurança a uma falsa sensação de perfeição e onisciência.

Os princípios com um melhor desempenho foram o SN3 e SN5, naturalmente, devido ao alinhamento das políticas as normas ISO e recomendações regulatórias do Banco Central.

Dentro da área Defender o Negócio, temos, novamente, um desempenho abaixo do esperado pelas instituições, em especial no princípio 'DN4 - Desenvolver sistemas, de forma segura, para construir sistemas de qualidade, com relação custo/benefício aceitável, nos quais os gerentes de negócio possam confiar', onde nenhuma organização abordou o tema. Isto mostra, possivelmente, uma tendência reativa da área de segurança. Não mostrando a devida preocupação com a arquitetura de segurança dos sistemas desenvolvidos, incorrendo em prejuízos para o negócio para recuperar os prejuízos gerados. Novamente, a ideia do isolamento da segurança das demais áreas organizacionais pode ser uma fonte causadora da negligência desse princípio.

O princípio 'DN1 - Adotar uma abordagem baseada em risco para garantir que o risco é tratado de uma maneira consistente e efetiva' também teve uma baixa aderência, sendo abordado por apenas uma instituição. Podemos considerar a baixa adesão a esse princípio um reflexo direto da baixa adesão ao princípio SN5. Se temos uma ausência cultural basear a segurança em uma cultura de gestão de riscos corporativos, provavelmente, também, teremos uma defasagem em endereçar as ações de segurança de acordo com o mapeamento dos riscos corporativos.

Analisando a aderência ao princípio 'DN2 - Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas', tivemos um índice maior de aderência ao princípio, porém, uma situação curiosa foi que as 3 instituições que preconizaram totalmente ou parcialmente em sua política este princípio, nem o Banco do Brasil e o Itaú classificaram a política de segurança da informação. Isto pode indicar que a política da segurança da informação é mais um documento mantido por fatores de obrigação normativa do que realmente como direcionador da segurança corporativa.

Já no princípio 'DN3 - Concentrar-se em aplicações críticas de negócios para priorizar recursos escassos de segurança da informação, protegendo as aplicações de negócio nas quais um incidente de segurança teria o maior impacto nos negócios', assim como DN2 tivemos aderência ao menos parcial de 3 organizações, portanto, vemos que a preocupação com a continuidade do negócio não está presente em metade das instituições analisadas, o que reforça, mais uma vez, que a segurança se vê como um setor isolado de outros setores da corporação.

Observando a área Promover o comportamento responsável em segurança da informação vemos que o princípio 'PC1 - Agir de forma ética e profissional para garantir que as atividades relacionadas à segurança da informação sejam realizadas de uma forma confiável, responsável e efetiva' não foi abordado por nenhuma instituição, exceto por uma abordagem parcial na política do Itaú.

Na contramão do princípio PC1, o princípio 'PC2 - Estimular uma cultura positiva de segurança da informação para exercer uma influência positiva no comportamento dos usuários finais, reduzir a probabilidade de ocorrência de incidentes de segurança e limitar o seu potencial impacto nos negócios' teve uma aderência, mesmo que parcial, de quase todas as instituições, exceto pelo Santander.

Esses dois dados mostram que existe uma preocupação das áreas de segurança em treinar os colaboradores e divulgar os procedimentos de segurança na organização, porém, não atribuem ao usuário a devida importância de suas ações na garantia da segurança corporativa.

A ideia transmitida é que a garantida da segurança se dá mais por processos, tecnologias e controles e menos pelo comportamento, conhecimento e atitude das partes interessadas, ideologia que já se mostra insuficiente para atender o negócio, como citado por Cherdantseva (2015, p. 17).

Não basta um foco exclusivo em treinar e divulgar informações sobre a segurança, promover o entendimento do papel individual e conjunto de cada colaborador na segurança da informação é tão importante quanto sua capacitação.

3.2 Análise de Eficiência

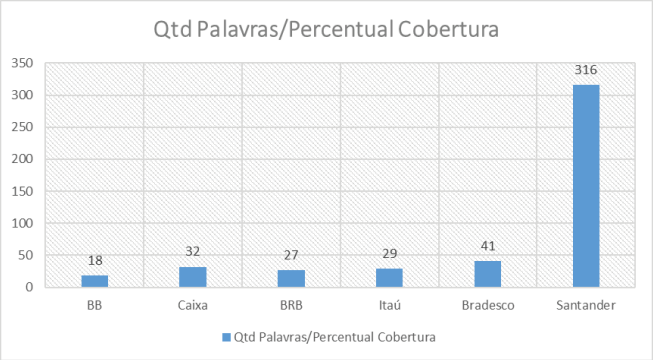
Os dados analisados até o momento nos dão uma noção da eficácia das políticas analisadas em perpetuar os termos propostos pela ISACA (2012) quando compreendidas, porém, a eficácia das políticas não pode ser avaliada pelos mesmos parâmetros.

A eficiência da política é outro fator de suma importância que devemos avaliar. Políticas muito extensas com diversas nuances técnicos tendem a não transmitir, eficientemente, ao leitor os pontos principais que a política deveria se propor a transmitir.

Para uma análise da eficiência das políticas, utilizaremos os parâmetros de quantidade de palavras com o percentual de cobertura. De forma intuitiva, podemos concluir que quão menor for a quantidade de palavras utilizadas e maior for o percentual coberto, mais eficaz em transmitir a mensagem a política será.

Nesse sentido temos a Figura 10, em que considerou-se a quantidade de palavras necessárias, em média, para cada ponto percentual de cobertura obtido pela política.

Figura 10- Qtd Palavras / Percentual Cobertura



Fonte - O Autor

O resultado da Figura 10 permite uma avaliação por outro aspecto. Diferentemente da análise por eficácia, em que 3 instituições na faixa entre 1000 e 1500 palavras tiveram o melhor desempenho, aqui temos que a melhor eficiência foi do Banco do Brasil com uma média de 18 palavras por ponto percentual, ou seja, uma política mais enxuta, com menos de 500 palavras, tende a ter uma eficiência maior em transmitir sua mensagem do que políticas mais extensas.

Essa análise nos permite inferir que as políticas da Caixa, BRB e Itaú, apesar de possuírem uma eficácia maior na cobertura dos aspectos propostos pela ISACA (2012), também contêm muitas informações extras não relacionadas aos princípios, como aspectos técnicos ou específicos que não deveriam ser abordados inicialmente política.

A Figura 10, também, permite fazer uma comparação entre as 2 políticas com a menor eficácia. Apesar de ambas possuírem uma baixa eficácia, a eficiência da política do Bradesco é 7 vezes superior à do Santander.

Esse fato mostra que a política do Bradesco, apesar da baixa aderência aos princípios, transmite a informação ali contida de forma concisa, portanto, de fácil entendimento para o usuário.

O mesmo não pode se dizer da política do Santander, esta se mostra, além da baixa aderência, complexa e maçante, tornando a transmissão da mensagem da política de baixa qualidade.

Foram observados do ponto de vista de eficiência os dados obtidos e, de forma geral, o desempenho das políticas, em especial na aderência aos princípios de governança da segurança propostos pelo ISACA (2012) foi o esperado, apesar de preocupante, pois, como já citado, expõe que as políticas, ainda, são vistas e construídas por áreas táticas e operacionais, visando à segurança do ponto de vista dela mesmo, sem considerar o negócio.

Do ponto de vista de eficiência, temos que as políticas trazem, ainda, um carregamento muito grande de aspectos técnicos e específicos que, muitas vezes, apenas, dificultam o entendimento desta para os colaboradores. Mais uma vez, o reflexo da visão individual que as áreas de segurança trazem.

4 Conclusão

A análise dos resultados obtidos constatou o desalinhamento entre o negócio e a segurança nas instituições avaliadas, nem uma corporação obteve ao menos um índice de aderência próximo de 50% aos princípios de governança propostos e o foco das políticas fica claro que é em "como fazer" e não "porque fazer" a segurança.

Ainda existe um apego forte aos critérios de confiabilidade, integridade e disponibilidade de forma restrita e direcionada às áreas de tecnologia da informação. Conceitos com uma visão holística de segurança, ainda, estão uma fase incipiente nas organizações e os reflexos dessa rigidez são encontrados nos entraves burocráticos impostos pela segurança, nos prejuízos financeiros gerados pela alta reatividade da segurança e pela dificuldade de planejar o time to Market das instituições.

Além da baixa eficiência em apresentar os princípios de governança, as organizações, também, mostram uma baixa eficácia na transmissão da ideologia da segurança, do ponto de vista do negócio.

As políticas se mostram, ainda, carregadas de informações técnicas e operacionais, pouco focadas em transmitir as ideias e princípios de segurança. De forma geral, o foco das políticas não é a comunicação e entendimento de qualquer colaborador e sim direcionada para áreas mais relacionadas com a tecnologia da informação.

A comprovação desse fato em um setor tão competitivo e com diversos controles legais e regulatórios mostram que as instituições, ainda, não compreendem a segurança da informação, estrategicamente, como uma força e não percebem o ganho de valor que a segurança pode proporcionar aos clientes, tanto externos como internos.

O setor bancário pode estar próximo de um ponto de ruptura de seu modelo tradicional de negócio. Produtos e serviços tendem a ser planejados com alta conectividade, facilidade, baixo custo e dinamismo, conforme demanda atual dos clientes. Isto muda os paradigmas de relacionamento entre as instituições e os Clientes colocando cada vez mais uma pressão na estrutura tradicional de agências físicas, tarifas, serviços, produtos e segurança oferecidos atualmente.

A segurança da informação pode ser o fiel da balança nesse período de transição por vir, auxiliando e provendo o dinamismo necessário para o negócio mudar e se adaptar à nova realidade ou sendo um entrave organizacional que limita a capacidade de adaptação e mudança da corporação.

As análises foram realizadas com base nas informações contidas nas políticas de segurança da informação e do ponto de vista da governança da segurança, as conclusões obtidas foram portanto com base nestes dados e não necessariamente se provam como verdade total ou parcial dentro das instituições avaliadas, porém são um forte indicativo da situação ambiental das corporações uma vez que a política de segurança da informação deve ser o documento principal de onde se derivam as demais políticas, procedimentos padrões, manuais, processos e outros relacionados à segurança da informação.

Referências

ABNT. *NBR ISO/IEC 27001*: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos. 2. ed. Rio de Janeiro: ABNT, 2013.

ABNT. *NBR ISO/IEC 27002*: Tecnologia da informação -Técnicas de segurança - Código de prática para controles de segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2013.

CHERDANTSEVA, Y.; HILTON, J. Information security and information assurance: the discussion about the meaning, scope and goals. In: ALMEIDA, F.; PORTELA, I. (Ed.). O*rganizational, legal, and technological dimensions of is administrator. igi global publishing*. September, 2014. Disponível em: <http://www.igi- global.com/chapter/information-security-and-information- assurance/80717>. Acesso em: 04 nov. 2015.

FOINA, P. R. *Estratégia e segurança de informação*. Governança da Segurança da Informação. 2015.

ISACA. *COBIT 5 for Information Security*. Rolling Meadows: ISACA, 2012.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. *Computer & Security*, v. 23, n. 5, p. 371-376, jul. 2004.

VON SOLMS, B.; VON SOLMS, R. Information Security Governance: Cobit or ISO17799 or both. *Computer & Security*, v. 24, n. 2, p. 99-104, mar. 2005.