Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

VITOR TORMIN NISHI

ANÁLISE ESTRATÉGICA DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO SETOR BANCÁRIO

Brasília
2016

ANÁLISE ESTRATÉGICA DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO SETOR BANCÁRIO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança de TI

Orientador: Prof. Dr. / Prof. Maurício Lyra

Brasília
2016

ANÁLISE ESTRATÉGICA DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO SETOR BANCÁRIO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança de TI

Orientador: Prof. Dr. / Prof. Maurício Lyra.

Brasília, 12 de Abril de 2016.

Banca Examinadora

_____

Prof. Dr. Gilson Ciarallo

_____

Prof. Dr. Paulo Foina

Dedico esta obra à minha família, amigos e professores que me deram o suporte necessário para esta jornada.

AGRADECIMENTO(S)

Agradeço a o apoio de todos que contribuíram direta ou indiretamente para a construção da obra.

“O problema não é se as máquinas pensam, mas se os homens fazem. ”
B.F. Skinner, autor e psicólogo, no livro Contingencies of Reinforcement, de 1969.

RESUMO

Este trabalho pretende apresentar uma análise, do ponto de vista estratégico, baseados em preceitos do *CoBIT 5 for Information Security*, das políticas de segurança da informação no setor bancário. Buscou-se, através 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 da Segurança da Informação. CoBIT 5 for Information Security. Governança da Segurança da Informação.

ABSTRACT

This work intends to present an analysis, from a strategic point of view, based on the precepts of CoBIT 5 for Information Security, for information security policies in the banking sector. It was intend, by 12 principles of governance proposed in the publication of ISACA, evaluate how are aligned the strategic aspects with the tactical / operational aspects of security in information security policies. As expected, the studies showed an adherence rate of governance precepts lower than 50% in organizations and showed that even among them, there is a big difference between the levels of grip compared one by one. The final understanding of the work leads us to believe that there is a misalignment between business and security, which is still very tied to conservative concepts of security, ignoring the competitive advantage to the business that security can provide and not paying attention that security involves the business as a whole and not just IT and tools are the means and not the security motivators.

Key words: Information Security Policy. CoBIT 5 for Information Security. Governance of Information Security.

SUMÁRIO

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 tornam 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 a agregação de valor através 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 por muitas vezes o indicativo de confiabilidade, segurança e integridade de um governo.

Casos recentes, como a crise Grega, mostram como o setor bancário reflete uma política adotada por um país e é um dos primeiros a entregar para a população as consequências dos atos 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 através 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, através 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 em 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 através 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.

Para conduzir a pesquisa, primeiro foi necessário determinar quais instituições financeiras seriam pesquisadas. Para isto as instituições foram divididas em 2 grupos, públicas e privadas.

Para as instituições privadas foi realizada uma pesquisa nos sites corporativos e para as instituições públicas foi utilizado os instrumentos providos na

lei de acesso a informação.

De posse das políticas foi determinada uma escala de aderência e os critérios de avaliação das políticas em relação aos princípios de governança.

Estes critérios foram aplicados as políticas e os resultados tabulados conforme o previsto na escala de aderência, gerando os resultados para análise posteriormente.

Os resultados foram analisados e as interpretações dos resultados extrapoladas na forma de gráficos, buscando expor os de forma mais clara o nível de aderência e o alinhamento das políticas com a estratégia da corporação.

No primeiro capítulo será apresentado o referencial teórico necessário para um completo entendimento da pesquisa, abordando os conceitos de segurança da informação e de política de segurança da informação, apresentando a importância das normas ISO para segurança da informação e da geração de valor através da governança e por fim o papel do Cobit 5 nessa abordagem.

Na sequência, no segundo capítulo, serão apresentados, de forma detalhada, os procedimentos metodológicos utilizados para conduzir a pesquisa.

No terceiro capítulo as políticas serão avaliadas e os resultados analisados com base na escala de maturidade e critérios de avaliação determinados no capítulo anterior.

Por fim, no quarto capítulo, será realizada a conclusão do trabalho, buscando um entendimento final dos objetivos propostos e os objetivos alcançados na monografia.

1 INTRODUÇÃO TEÓRICA

Informação é um ativo chave de qualquer organização no mundo atual, sua relevância na tomada de decisões estratégicas, táticas e operacionais é fundamental para existência da corporação. Conforme descrito por Freitas, Becker, Kladis e Hoppen (1997):

> Nas organizações, a informação já é considerada como um recurso básico e essencial, como são a mão -de- obra e a matéria-prima. A informação é vista como um elemento decisivo que pode determinar o êxito ou fracasso de um empreendimento

Evoluindo essa linha de pensamento, Sêmola (2014, p.23) afirma:

> [...] é inegável que todas as empresas, independentemente de seu segmento de mercado, de seu *core business* e porte, em todas essas fases de existência, sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, ganho de *market share*, aumento de agilidade, competitividade e apoio a tomada de decisão.

Portanto, em todo seu ciclo de vida, a informação deve ser armazenada, disponibilizada e acessada de forma adequada, quando necessária e para quem for autorizado, visando a melhor utilização da mesma nas tomadas de decisão.

A segurança da informação pode ser entendida, segundo (ISACA,2012a), como algo que garante que, dentro da organização, as informações são protegidas contra a divulgação para usuários não autorizados (confidencialidade), a modificação imprópria (integridade) e o bloqueio de acesso, quando necessário (disponibilidade).

Outro conceito, este apresentado pela na norma ISO 27000 (2014), nos diz:

> A segurança da Informação inclui 3 principais dimensões: Confidencialidade, Integridade e Disponibilidade.
> A segurança da informação envolve a aplicação e gestão das medidas de segurança adequadas que envolvem a consideração de uma ampla gama de ameaças, com o objetivo de garantir o sucesso sustentável do negócio e continuidade, e minimizando os impactos dos incidentes de segurança da informação

Em ambos conceitos, podemos notar a presença do tripé CID (Confidencialidade, Integridade e Disponibilidade) e um foco no que a segurança

deve fazer. Apesar de comum na literatura, este conceito não nos fornece uma definição holística do que é a segurança da informação, como descrito por Marciano e Marques (2006, p.94).

Porém antes de prosseguirmos, precisamos estabelecer uma definição do que é informação e na sequência de um entendimento do significado de segurança da informação.

1.1 Informação

O termo informação é uma palavra de comum uso no cotidiano, seu uso permeia todos os círculos, desde o meio acadêmico, passando pelo profissional e por fim no social.

Algumas das definições do termo, como no dicionário Michaelis Online, diz que informação é a transmissão de conhecimento, transmissão de notícias e instrução/ensinamento.

Em outra definição, Weaver (1978, p.28 apud PRIMO, 2003, p.139), na Teoria Matemática da Comunicação, no diz que:

> [...]a palavra informação não se refere tanto ao que você efetivamente *diz*, mas ao que *poderia* dizer. Isto é: informação é uma medida de sua liberdade de escolha quando seleciona uma mensagem

Campbell (1982, p.68 apud SERRA, 2008, p. 98), define que:

> [...]uma mensagem não transmite informação a não ser que exista alguma incerteza prévia na mente do receptor acerca do que a mensagem conterá. E quanto maior a incerteza, maior a quantidade de informação transmitida quando a incerteza é resolvida[...]

Portanto, nosso primeiro entendimento é que a informação se origina de uma mensagem, desde que seu receptor consiga contextualizar essa mensagem dentro alguma incerteza que ele tenha em seu subconsciente.

A mensagem pode ser armazenada e transmitida de várias maneiras, como afirma Capurro (2003, p.3 apud MATHEUS F, 2005, p.148), “uma mensagem pode ser codificada e transmitida através de diferentes meios ou mensageiros”.

Ou seja, todo e qualquer dado físico ou lógico, contém uma mensagem codificada que pode ou não ser interpretada por um receptor extraindo assim uma informação.

Podemos entender que a informação depende do contexto no qual o receptor daquela mensagem a insere, quanto maior a expectativa do receptor, acerca do conhecimento que pode transmitir aquela mensagem, maior o grau informação contida nele quando está for tratada.

Em seu livro *Sistemas de Informações Gerenciais*, Oliveira (1997), diz que:

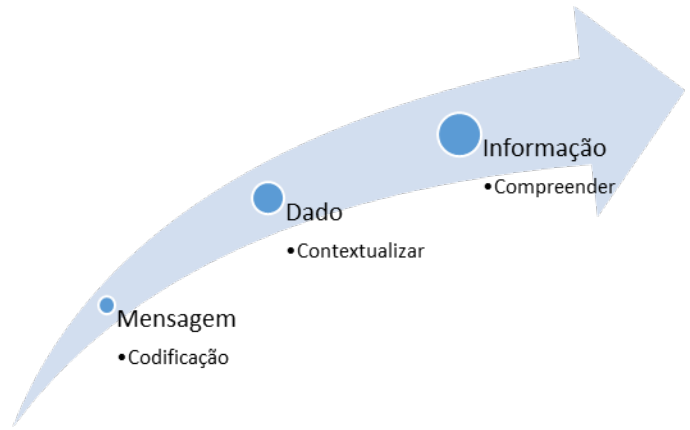
> Dado é qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação.
>
> Informação é o dado trabalhado que permite [...] tomar decisões

Hayes (1986) nos traz a definição:

> Informação é uma propriedade dos dados resultantes de ou produzida por um processo realizado sobre os dados (em cujo caso são aplicáveis a definição a medida utilizadas na teoria da comunicação); pode ser a seleção de dados; pode ser a organização de dados; pode ser a análise de dados

Com base nesses dois conceitos apresentados podemos entender, conforme a Figura 1, que uma informação é uma mensagem que pode estar codificada em um dado que passa por um processo de contextualização pelo receptor na busca de um conhecimento ao qual ele ainda possui uma incerteza e precisa compreender algo.

Figura 1 – Dado e Informação



Fonte - O Autor

Isso atribui a qualquer dado o potencial de possuir um certo grau de informação, de acordo com receptor que obtêm. Seja gravada em bit, bytes, em um papel, ou em uma foto, bem como em uma conversa interceptada no vento, toda mensagem pode ser contextualizada e usada pelo seu receptor, gerando assim a necessidade de garantir a segurança das informações geradas por uma corporação.

1.2 Segurança da Informação

Como vimos o conceito de informação não é vinculado apenas a dados computacionais, mas é aplicado a qualquer mensagem codificada, seja ela em papel, foto, som, bits, bytes e etc.

Garantir a segurança da informação de uma organização é fundamental para a existência da organização ou vez que o uso da informação de forma não segura pode gerar danos irreparáveis.

O conceito de segurança da informação, conforme Sêmola (2014, p.68) é:

> Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Dessa forma, estaríamos falando da definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

Este conceito segue a mesma linha teoria das definições de segurança da informação apresentadas anteriormente do ponto de vista da ISO e da ISACA.

Porém, como também citado anteriormente, estes conceitos não apresentam uma visão geral do que seria a segurança da informação, se concentrando no tripé CID e estão mais concentrados no fazer do que no porquê.

Uma definição mais abrangente do conceito de segurança da informação seria que a segurança da Informação é uma disciplina, cujo objetivo principal é manter o conhecimento, dados e seu significado livres de eventos indesejáveis, tais como roubo, espionagem, dano, ameaça e outro perigo. Segurança da Informação contempla todas as ações, tomadas com antecedência, para evitar eventos que indesejáveis aconteçam com o conhecimento, dados e seu significado para que estes sejam confiáveis, conforme apresentado por Cherdantseva (2015, p.5).

Está definição é mais abrangente que as apresentas anteriormente, pois conforme o próprio autor expões, esta não restringe o tipo de dados, inclui todas as ações possíveis para proteger a informação, a lista de eventos indesejáveis e ampla e aberta, os objetivos da segurança não se prendem a contemplar apenas os conceitos do tripé CID e traz uma preocupação em prevenir os incidentes e não apenas tratá-los quando já ocorreram.

Isso mostra uma mudança no paradigma do conceito de segurança da informação e se faz necessária pois uma definição restrita a um determinado conjunto de segurança objetivos (CID), impede que os especialistas em segurança tenham uma visão ampla e necessária da segurança da informação. Portanto, o foco

na realização de várias metas de segurança pré-definidas, em vez da realização de uma segurança adequada é uma abordagem falha e perigosa, uma vez que pode levar a um descuido de algumas ameaças (Cherdantseva, 2015, p.9).

Esta visão, desprendida do tripé CID, também foi explicitada por Marciano e Marques (2006, p.95) que apresentam o seguinte conceito de segurança da informação:

> Segurança da informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.

Portanto a segurança da informação seria um conceito mais amplo, complexo e mais abrangente que confidencialidade, integridade e disponibilidade, sendo mais um conceito multidisciplinar, com uma abordagem ampla e adaptativa ao ambiente, onde fatores tecnológicos, culturais, econômicos, sociais e outros devem ser considerados e capazes de interagir em harmonia.

Cherdantseva (2015, p.17) estabelece que atualmente está claro que apenas tecnologia não é suficiente para tratar os problemas complexos da segurança da informação. As necessidades do negócio, o fator humano, incentivos econômicos, cultura e aspectos organizacionais devem ser consideradas a fim de ser obter uma proteção adequada da informação.

Apesar deste entendimento atual que a segurança não é um fator tridimensional, focado em tecnologia e uma preocupação única dos níveis táticos e operacionais. As corporações ainda tendem a se prender a este conceito antigo, conforme descrito por Von Solms (2004, p.372), em muitos casos a direção executiva ainda entende que tecnologia é tudo que necessitam para segurança e delegam ou rebaixam a questão de segurança aos níveis técnicos e convenientemente esquecem do problema. Implantando tecnologia para gerenciar a segurança da informação, porém sem conseguir compreender e atender o problema como um todo, frequentemente desperdiçando recursos financeiros.

1.3 Família ISO 27000

A família ISO 27000 é um grupo de normas publicada pela ISO (the International Organization for Standardization) e a IEC (the International Electrotechnical Commission) que prove assistência para qualquer tipo de organização, não importando o tamanho e tipo, para implementar e manter um sistema de gerenciamento da segurança da informação (SGSI).

Como já informado anteriormente, a ISO 27000 (2014) nos define a segurança da informação com o aspecto tridimensional da CID, considerando a aplicação e gestão de medidas de segurança adequadas que envolvem a

consideração de uma gama ampla de ameaças, objetivando a sustentabilidade e continuidade do negócio, minimizando os impactos dos incidentes de segurança.

Dentre as normas da família ISO 27000 temos especificamente as normas:

- ISO 27000: Information technology — Security techniques — Information security management systems — Overview and vocabular: Prove um *overview* sobre o a família ISO 27000, uma introdução sobre o que um SGSI e apresenta os termos utilizados nas demais normas da família;

- ISO 27001: Information technology — Security techniques — Information security management systems — Requirements: Prove os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI dentro do contexto da organização;

- ISO 27002: Information technology — Security techniques — Code of practice for information security controls: Prove um guia para implementação do SGSI com as melhores práticas e controles de acordo com ambiente de risco da corporação.

As normas ISO 27001 e ISO 27002, são amplamente adotadas no estabelecimento da segurança da informação em corporações, principalmente pelo foco no “como fazer” segurança da informação que elas apresentam, como descrito por Von Solms (2005, p.100), o que é esperado, uma vez que papel complexo e estratégico da segurança ainda não é compreendido em sua totalidade nas organizações.

A facilidade na adoção de um gerenciamento de segurança, partindo das normas da família ISO 27000 também é destacado por Oliveira (2015):

> Considera-se a norma ISO/IEC 27001 como ponto de partida para a operação de um sistema de gerenciamento da segurança da informação, pois estabelece o ele mento principal para o mesmo, seus requisitos. Muitos tem atribuído inclusive à influência única da TI na norma. Isso não é bem verdade, mas podemos considerar que ela auxilia sobremaneira o planejamento de requisitos adequado para a construção e sustentação de sistemas informatizados que garantirão o Sistema de Gerenciamento de Segurança da Informação.

A ISO 27001 segue o modelo PDCA (Plan-Do-Check-Act), que pode ser visto na Figura 2 e conforme Santos (2012, p.15) podemos definir as fases da seguinte forma:

> PLAN (PLANEJAR) – Estabelecimento de políticas, objetivos, processos e procedimentos relevantes para a administração do risco e para a melhoria da Segurança da Informação. Planeia os resultados de acordo com a estratégia da organização.
>
> DO (FAZER/IMPLEMENTAR/OPERAR) – Implementação e

operacionalização das políticas de controlo, processos e procedimentos do Sistema.

CHECK (VERIFICAR/MONITORIZAR/REVER) – Inspeção da performance dos processos em comparação com as políticas e objetivos de um SGSI. Estes resultados devem ser reportados à gestão para análise.

ACT (AGIR/MANTER/OTIMIZAR) – Tomada de ações corretivas e preventivas, baseadas nos resultados das auditorias internas do SGSI e demais informações provenientes da gestão ou demais fontes relevantes.

Figura 2 - Modelo PDCA

Fonte SANTOS (2012, p14)

A norma ISO 27002 (2013), apresenta 35 objetivos de controle e 114 controles que devem ser implementados, de acordo com as necessidades das organizações em ordem obter os requisitos de segurança requeridos na ISO 27001 (2014), conforme apresentado pela norma:

> A ordem em que se encontram as seções não implica nem significa o seu grau de importância. Dependendo das circunstâncias, os controles de segurança da informação de uma de quaisquer das seções podem ser importantes; assim, convém que cada organização implemente esta Norma identificando quais controles são aplicáveis, quão importantes eles são e qual a aplicação para os processos individuais do negócio. A relação dos controles, portanto, não está em ordem de prioridade.

A ideia da flexibilização dos controles, de acordo com as necessidades corporativas é reforçada na ISO 27002 (2013) que diz:

> Nem todos os controles e diretrizes contidos neste código de prática podem ser aplicados. Além disto, controles adicionais e recomendações não incluídas nesta Norma, podem ser necessários. Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma referência cruzada com as seções desta Norma, onde aplicável, para facilitar a verificação da conformidade por auditores e parceiros de negócio.

A norma também recomenda que a decisão de quais controles devem, ou não ser implementados seja baseado em uma avaliação de riscos do ambiente corporativo e regulatório como um todo, conforme descrito:

> Os recursos empregados na implementação dos controles precisam ser balanceados com base na probabilidade de danos ao negócio, resultado dos problemas de segurança pela ausência desses controles. Os resultados de uma avaliação de risco ajudarão a orientar e determinar as ações de gestão apropriadas e as prioridades para gerenciar os riscos de segurança da informação e a implementação dos controles selecionados para proteger contra estes riscos. (ISO 27002, 2013)

A implementação da norma 27002 garante aderência a norma 27001, a utilização das melhores práticas reconhecidas de mercado na área de segurança da informação e torna o SGSI capaz de receber uma auditoria externa reconhecida pela ISO, conforme descrito por Calder (2009, p.11).

Mas não é apenas do ponto de vista da certificação de segurança por uma entidade de auditoria externa que a adoção das normas oferece as organizações um benefício, do ponto de vista regulatório a adoção das normas também traz benefícios as corporações.

Novamente, Calder (2009, p. 5) nos diz que leis e regulamentos costumam ser mal escritos, frequentemente contraditórios entre suas jurisdições e dificilmente fornecem um guia para implementação da segurança nas entidades. Tornando difícil para as organizações identificar métodos específicos para atender leis individualmente, com isso a implementação de melhores práticas de segurança se torna a forma mais eficiente para proteger o negócio da organização em um tribunal e atender a maioria das necessidades legais possíveis.

No Brasil, o Banco Central do Brasil (BACEN) regulamente as entidades financeiras e o mesmo recomenda o uso da norma, conforme recomendado pelo BACEN (2013) no Manual de Segurança da RSFN, “As Instituições, visando a melhoria da segurança, devem seguir a norma NBR ISO/IEC 27002:2005 editada pela ABNT”.

O escopo de outras resoluções do BACEN, apesar de não citar diretamente as normas ISO da família 27000, fazem referências a requisitos que são implementados pelas normas como, por exemplo, na RESOLUÇÃO N° 2.554/1998 que determina a segregação de funções dentro do artigo 1 e na norma ISO27002(2013), no item 6.1.2, é descrito o controle e as diretrizes de implementação da segregação de funções dentro de uma organização.

Porém não é escopo deste trabalho fazer o mapeamento das normas ISO 27000 e a regulamentação bancária no Brasil, ficando o tema como sugestão para um trabalho futuro.

1.4 Governança da Segurança da Informação

No item anterior vimos que as normas ISO da família 27000 tem um papel importante na segurança das organizações e seu uso é incentivado por diversos motivos como necessidades regulamentárias e facilidade do uso, uma vez que como descrito por Von Solms (2005, p.100) e já citado anteriormente, o foco das normas é mais em como fazer/implementar a segurança da informação em uma corporação. Porém, muitas vezes a família ISO 27000 é adotada mais por forças externas, como imposições regulatórias, do que por um entendimento da alta direção que a segurança é uma necessidade estratégica e importante.

Renegar a segurança da informação as áreas táticas e técnicas da entidade acabam por remeter a empresa ao problema citado por Von Solms (2004, p.372), onde a direção executiva delega ou rebaixa as questões de segurança aos níveis técnicos que implantam a tecnologia para gerenciar a segurança da informação, porém sem conseguir compreender e atender o problema como um todo, frequentemente desperdiçando recursos financeiros.

Porém devemos entender que o papel da alta direção é do ponto de vista estratégico do negócio, ou seja, a direção executiva faz uma análise do ponto de vista das necessidades do negócio e dos stakeholders, não faz parte do seu escopo questões de nível técnico e tecnológico, estes devem ser apenas os meios para atender o que o negócio demanda, como descrito por Foina (2015):

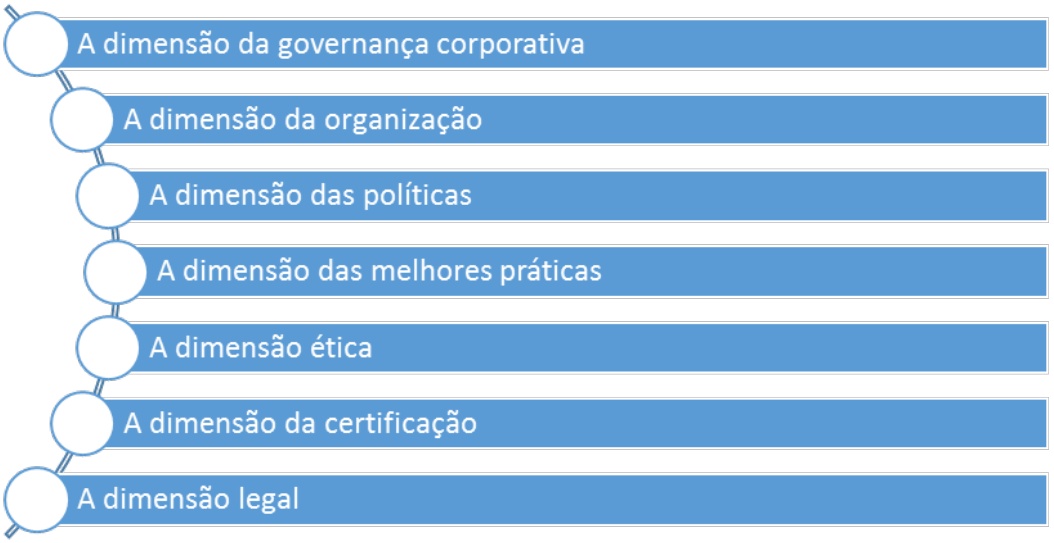
> Ao trazer a discussão sobre segurança da informação para o nível estratégico da organização, colocamos a questão em termos de danos potenciais e do eventual prejuízo financeiro que ele trará, se não for adequadamente tratado. Ao mesmo tempo, envolvemos toda a alta direção nessa questão facilitando a implantação de procedimentos e normas de controle e gestão de informação. Notem que em nenhum momento da discussão com a alta direção, são abordadas as ferramentas e tecnologias envolvidas, mas sim as questões financeiras envolvidas numa potencial invasão dos sistemas de informação.

Outro problema, que a omissão da alta direção nas questões da segurança gera dentro de uma organização, também é citada por Von Solms (2004, p.372), é que apesar da governança corporativa reconhecer cada vez mais vez o papel essencial e integrado da governança da segurança da informação dentro corporação em decorrência de uma série de medidas legais que atribuem a alta direção a responsabilidade da segurança da informação nas entidades, esse fator ainda pode ser ignorado, gerando uma série de implicações legais podem recair sob alta direção em decorrência de sua negligência.

Uma outra falha citada por Von Solms (2004, p.373) é não perceber que, a segurança da informação é uma disciplina multidimensional e que todas as dimensões devem ser consideradas na implantação da segurança, entre algumas

das dimensões que podem ser listadas, temos as apresentadas na Figura 3.

Figura 3 - Dimensões da Segurança



Fonte - O Autor

Nesse sentido a ISACA, na última atualização do *framework* do COBIT, apresentou uma evolução e segundo a definição da ISACA (2012a):

> O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI. Em termos simples, O COBIT 5 ajuda as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. O COBIT 5 permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI. O COBIT 5 é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

Ele nos apresenta uma estrutura baseada em cinco princípios, como visto na Figura 4.

Figura 4 - Princípios do COBIT 5

Fonte 1 - O Autor

E descreve 7 habilitadores que dão o suporte necessário para o pleno funcionamento da governança dentro da organização, como apresentado na Figura 5.

Figura 1.5 – Habilitadores

Fonte - O Autor

Princípios, políticas e frameworks, possuem um papel fundamental dentro do COBIT, conforme descrito este habilitador traduz o comportamento desejado pela alta direção que deve ser seguido pela corporação (ISACA, 2012a).

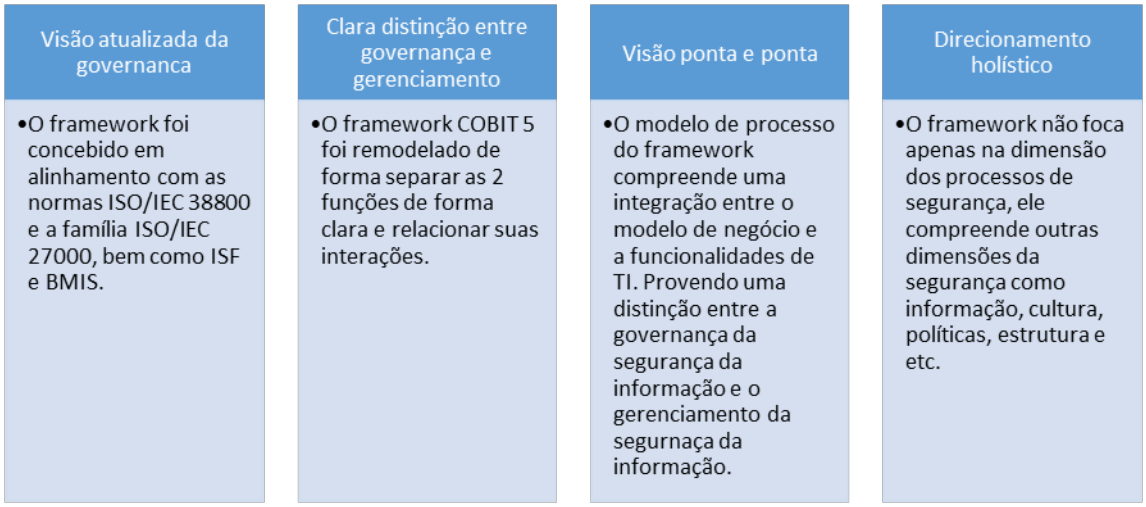
O habilitador informação também é de extrema importância no funcionamento do framework, conforme definição da ISACA (2012a), a informação é:

> **Informação:** permeia qualquer organização e inclui todas as informações produzidas e usadas pela organização. A informação é necessária para manter a organização em funcionamento e bem governada, mas no nível operacional, a informação por si só é muitas vezes o principal produto da organização.

Sua importância levou a ISACA a publicar um guia profissional nomeado Cobit 5 for Information Security. Onde o COBIT 5 é revisto dentro de uma perspectiva voltada para governança da segurança da informação.

Este guia nos prove as capacidades descritas na Figura 6 e iremos discutir mais sobre ele no próximo tópico.

Figura 6 - Capacidades do Cobit 5 for Information Security



Fonte 2 - O Autor

1.5 Políticas

Políticas, como destacado dentro do COBIT 5, é um dos pilares mais importantes dentre os habilitadores trabalhados dentro do framework. Elas traduzem para organização o direcionamento estratégico desejado pela alta direção. Segundo Von Solms (2004, p.374), as políticas de segurança da informação são destacadas por todas boas práticas de segurança da informação, como o coração e base de qualquer plano bem-sucedido de segurança da informação e que a política de segurança da informação são o ponto de partida e referência que todas subpolíticas, procedimentos e padrões devem ser baseados.

O autor Sêmola (2014, p.129) afirma ainda que:

> Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à Constituição federal para um país.

A ISACA (2012b) nos diz que políticas, princípios e *frameworks* são os veículos para traduzir o comportamento desejado, a respeitos da segurança da informação, para os membros da corporação de uma maneira formal, mas ainda prática nas práticas do dia a dia.

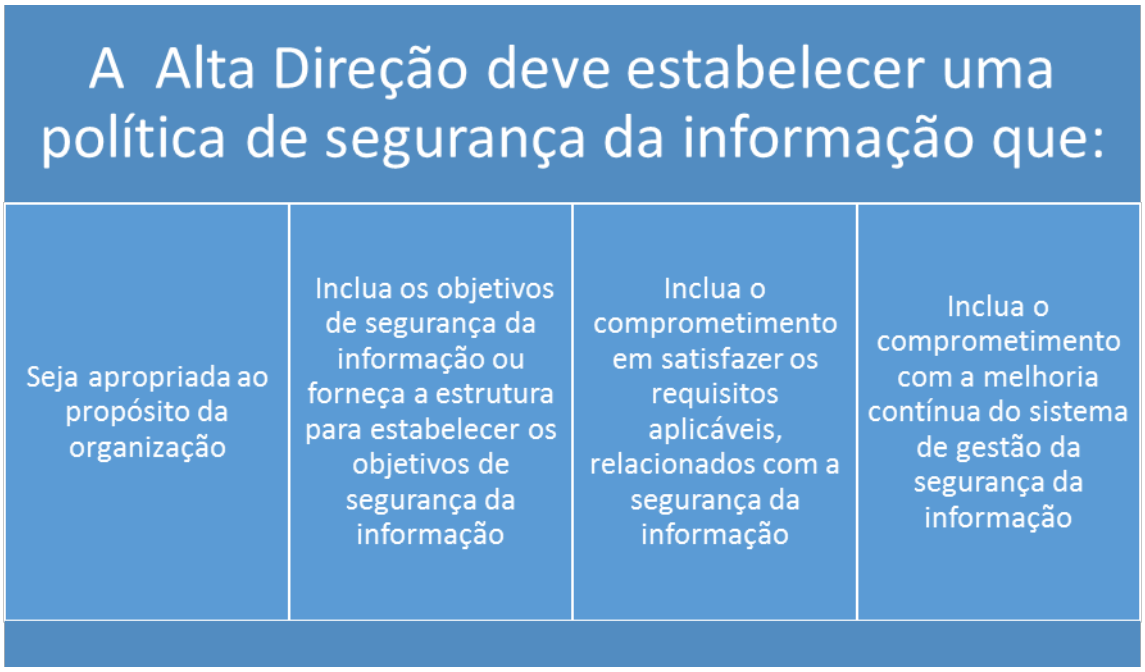
A norma ISO27001 (2013) estabelece que a política da segurança da informação é um dos requisitos previstos e diz que a política e os objetivos de segurança da informação devem ser explícitos e compatíveis com o direcionamento estratégico da corporação.

Portanto é um consenso entre autores e boas práticas de mercado que as políticas de segurança da informação são instrumentos importantes, do ponto de vista estratégico e a base de toda segurança da informação corporativa. Seu conteúdo deve alinhado com a estratégica corporativa que deve deixar de forma

clara seu apoio e comprometimento com a segurança da informação.

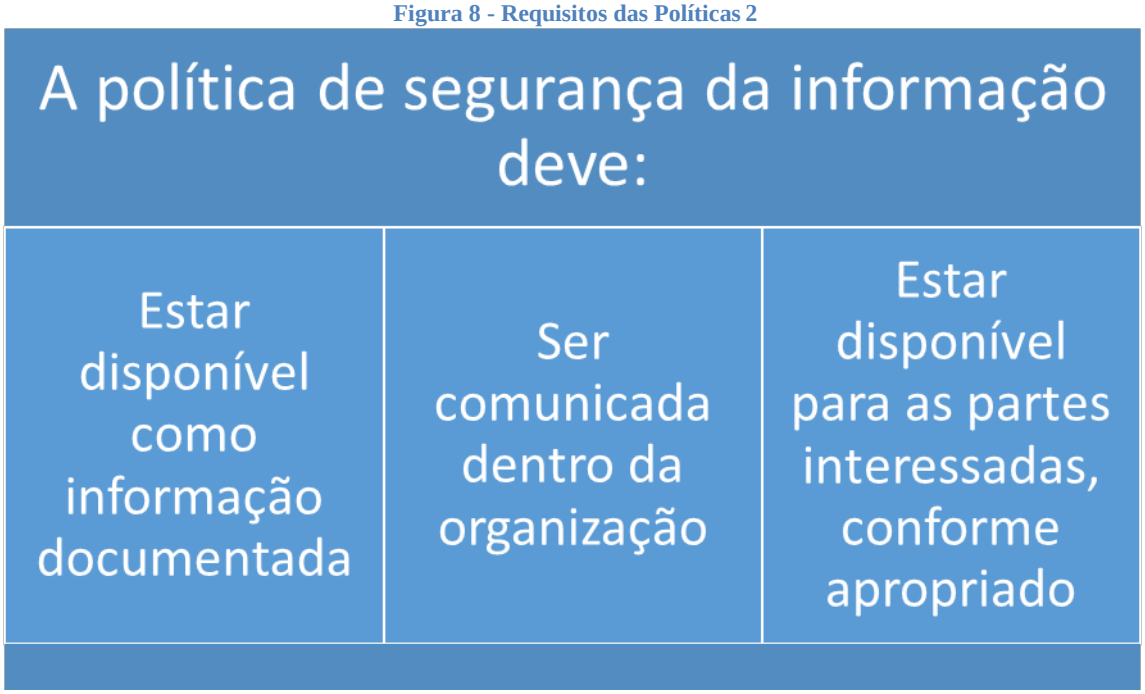
A norma ISO 27001 (2013) apresenta os requisitos de segurança, relativos a políticas, de acordo com as Figuras 7 e 8.

Figura 7 - Requisitos das Políticas 1



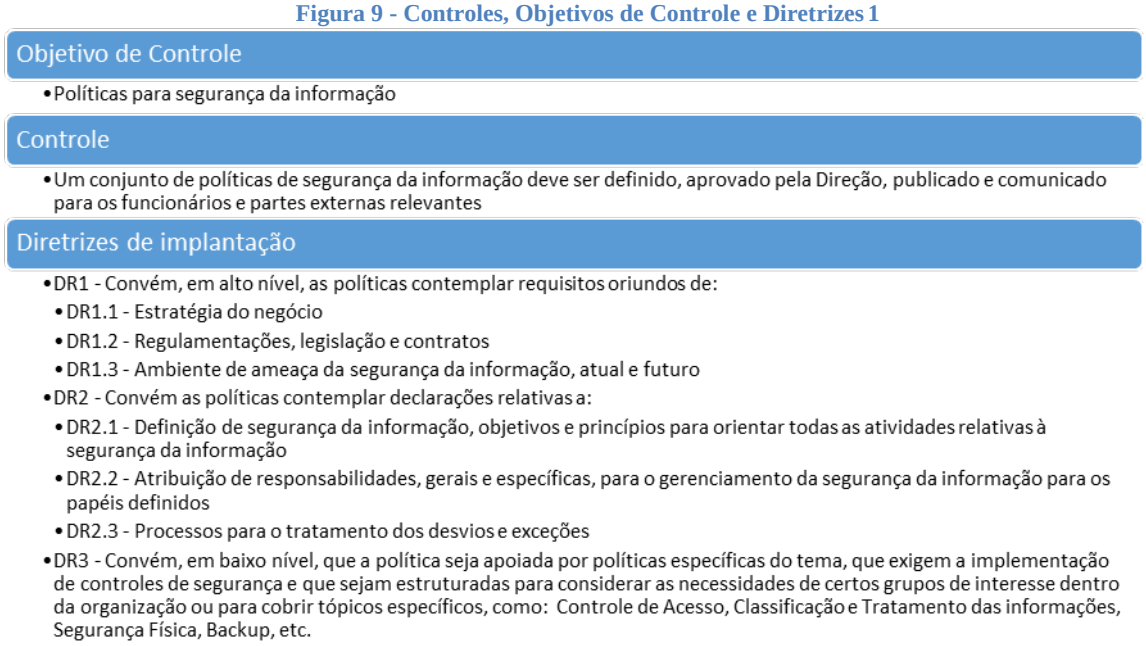
Fonte 3 - O Autor

Figura 8 - Requisitos das Políticas 2



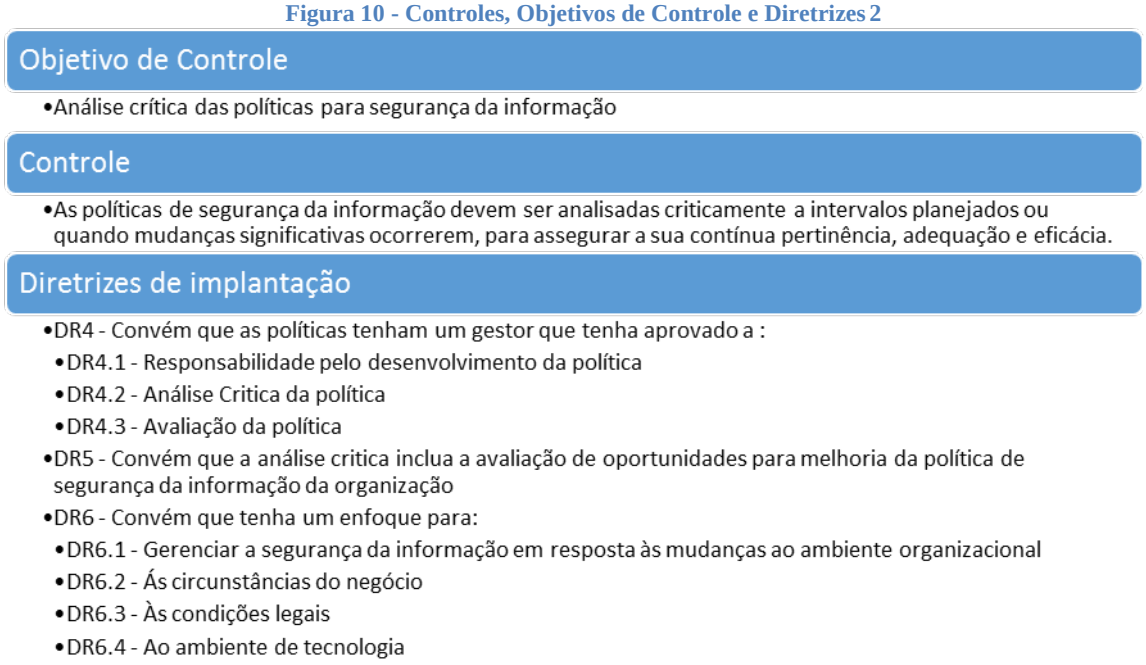
Os controles e diretrizes de implantação são apresentados conforme Figuras 9 e 10.

Figura 9 - Controles, Objetivos de Controle e Diretrizes 1



Fonte - O Autor

Figura 10 - Controles, Objetivos de Controle e Diretrizes 2

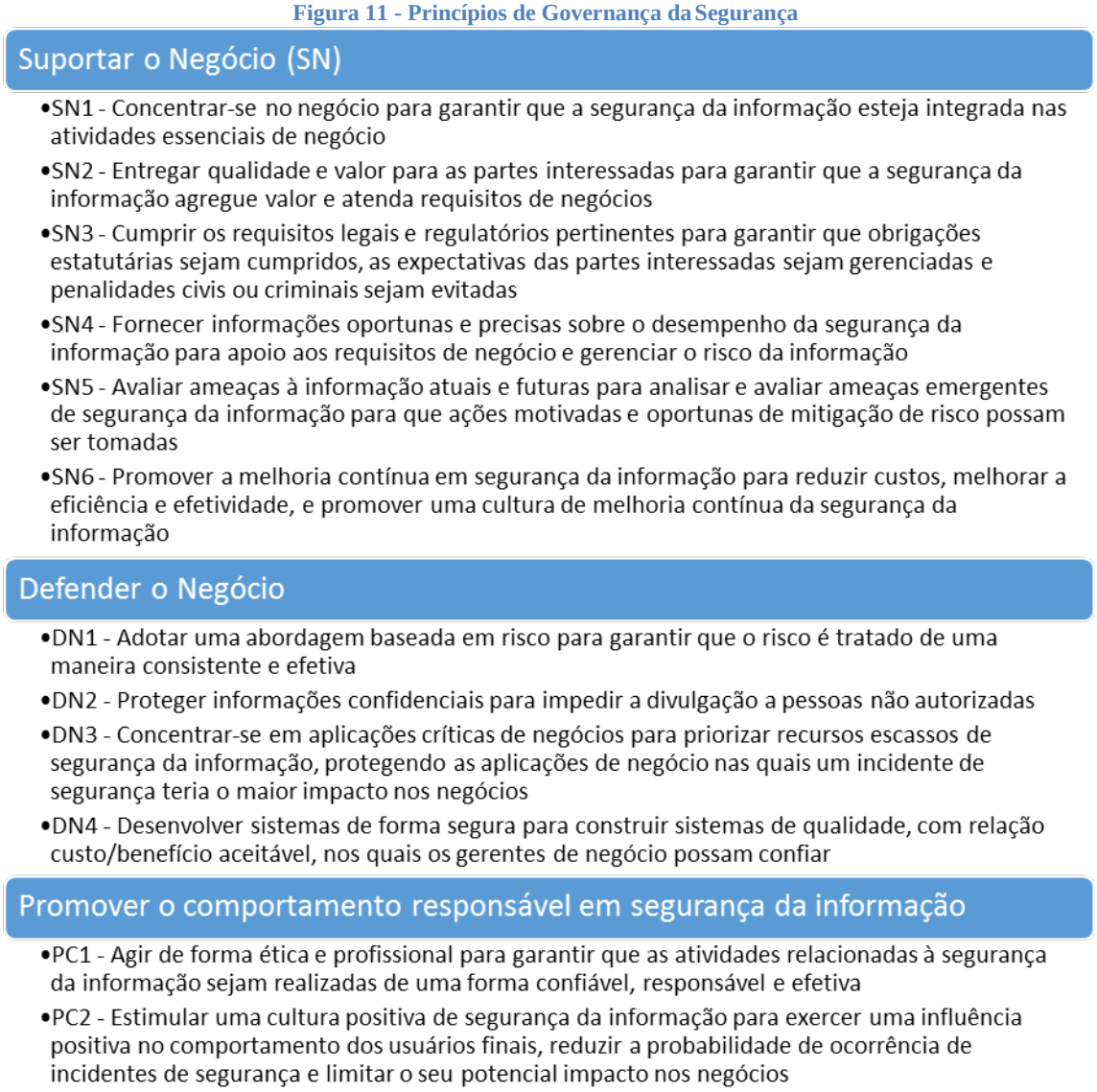


Fonte - O Autor

A ISACA (2012b) apresentou, dentro do *Cobit 5 for Information Security,* um conjunto de princípios, definidos por três líderes globais em boas práticas de segurança da informação – ISACA, ISF e International Information System Security Certification Consortium [(ISC)2] – com o intuito de alinhar dentro das políticas de segurança conceitos que ajudem a área de segurança a agregar valor ao negócio, apoiando com sucesso o negócio e promovendo boas práticas dentro da corporação.

Os princípios propostos pela ISACA (2012b) são divididos em 3 áreas conforme tradução de Neto (2012) e apresentado na Figura 11.

Figura 11 - Princípios de Governança da Segurança



Fonte - O Autor

Ao analisarmos as diretrizes de implantação, previstos na norma ISO 27002, em conjunto com os 12 princípios mencionados anteriormente, podemos identificar o grau de cobertura dos princípios que a implantação de uma política de segurança da informação, baseada apenas nas normas ISO 27001 e ISO 27002, entregaria a uma corporação, do ponto de vista da governança da segurança da informação.

Dentro das diretrizes da norma ISO 27002, temos algumas determinações explícitas, como por exemplo o princípio SN3 que diz: “Cumprir os requisitos legais e regulatórios pertinentes para garantir que obrigações estatutárias sejam cumpridas, as expectativas das partes interessadas sejam gerenciadas e penalidades civis ou criminais sejam evitadas”. Este é previsto na norma ISO 27002 (2013) como “Convém que as políticas de segurança da informação contemplem requisitos oriundos de regulamentações, legislação e contratos”.

Outros princípios, no entanto, não foram previstos pelas normas da família

e é de se esperar que não sejam identificados em políticas baseadas estritamente na norma, como por exemplo o princípio SN2, que diz: “Entregar qualidade e valor para as partes interessadas para garantir que a segurança da informação agregue valor e atenda requisitos de negócios”. Este princípio não possui uma diretriz de implantação, na norma ISO 27002, que faça referência de forma objetiva a entregar valor aos *stakeholders*, apesar de existir uma previsão de atender os requisitos de negócio, este princípio não é compreendido de forma plena pela norma.

Podemos verificar o mapeamento completo das diretrizes da norma ISSO 27002 (2013) e os 12 princípios da ISACA (2012b) na Tabela 1.

Tabela 1 – Mapeamento ISO 27002 vs Princípios de Governança da Segurança

	SN1	**SN2**	**SN3**	**SN4**	**SN5**	**SN6**	**DN1**	**DN2**	**DN3**	**DN4**	**PC1**	**PC2**
Diretrizes												
DR1	P	P	P	×	P	×	×	×	×	×	×	×
DR2	×	×	×	×	×	×	×	×	×	×	×	×
DR3	×	×	×	×	×	×	×	×	×	×	×	×
DR4	×	×	×	×	×	P	×	×	×	×	×	×
DR5	×	×	×	×	×	P	×	×	×	×	×	×
DR6	×	×	×	×	✓	×	×	×	×	×	×	×

Legenda: ✓ - Atende ao princípio / P – Atende parcialmente ao princípio / × - Não atende ao princípio
Fonte – O Autor

É possível observar que nem todos os princípios são cobertos pela norma e da mesma forma nem todas as diretrizes da norma possuem uma referência nos princípios de governança da segurança, como as diretrizes DR2 e DR3 que não tem referências dentro dos princípios e os princípios S4, DN1, DN2, DN3, DN4, PC1 e PC2 que não tem nenhuma diretriz que faça referência a eles.

A diretriz DR3 pode vir a ser uma espécie de coringa, pois ela pode trazer para dentro da política de segurança da informação elementos de princípios não cobertos diretamente pela norma, como por exemplo, fazer menção a uma política de desenvolvimento seguro de software, seguindo o recomendado pela DR03 faria com que aquela política de segurança da informação cobrisse o princípio DN4.

Vemos também que algumas diretrizes cobrem de forma parcial a um princípio, isso ocorre pois, de forma objetiva, aquela diretriz não atende de forma plena os requisitos do princípio.

Como forma de avaliar o conteúdo de uma política da segurança da informação, a ISACA (2012b) no apresentou dentro do Cobit 5 for Information Security uma descrição detalhada do conteúdo esperado em cada um dos

princípios, conforme pode ser visto no apêndice A deste trabalho.

2 METODOLOGIA

Neste capítulo será apresentada a metodologia utilizada na avaliação das políticas de segurança e será apresentado a seguir, de forma resumida, os assuntos que serão abordados neste capítulo.

O primeiro passo foi definir qual setor seria avaliado e escolher um *pool* de empresas que representasse de forma diversificada o segmento de mercado. Partindo deste ponto, foi feita uma pesquisa na internet em busca das políticas, para as instituições privadas e para as instituições públicas recorreu-se a Lei Federal nº 12.527/2011, popularmente conhecida como Lei de Acesso a Informação.

De posse das políticas, o próximo passo foi utilizar a tabela apresentada no Anexo I para identificar a quais dos princípios propostos as políticas das instituições são aderentes ou não.

Com estes dados serão feitos cruzamentos e comparações das informações obtidas de forma extrapolar conclusões e inferir sobre os motivos que levaram as políticas corporativas aos modelos atuais.

2.1 Segmento de Mercado e Instituições

Para este trabalho o segmento de mercado escolhido para análise foi o financeiro, em especial o setor bancário.

Esta escolha foi motivada devido à alta competitividade no setor, as várias regulamentações e legislações impostas e ao momento que o setor vive nos últimos anos e suas tendências para o futuro.

É um fato conhecido que o setor bancário é extremamente competitivo, as instituições bancarias estão sujeitas as mesmas regulamentações e legislações do governo e órgãos reguladores, oferecem uma carteira de serviços similares entre si a preços muito próximos e apesar dos lucros apresentados nos últimos anos pelo setor, tendências tecnológicas, como bancos virtualizados, por exemplo o Nubank, podem vir a comprometer o status quo destas instituições.

As estratégias corporativas destas 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 12.

Figura 12 - Instituições Financeiras

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 Itáu 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.

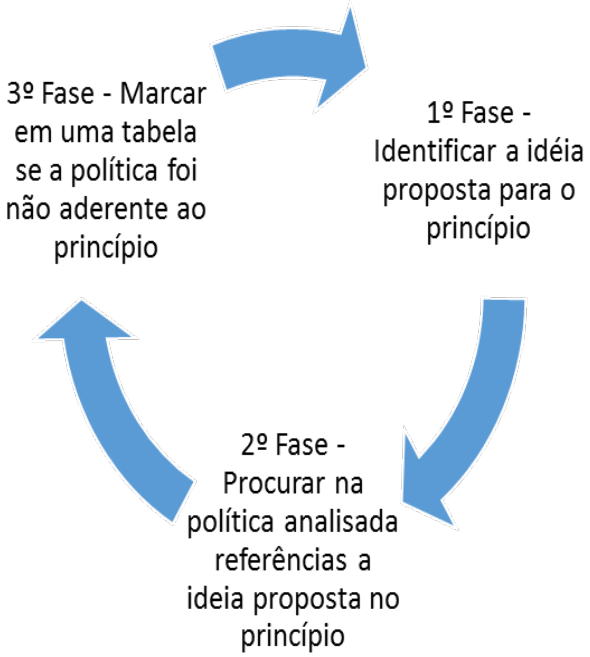
2.2 Análise das Políticas

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 a Informação ou LAI é um dispositivo de transparência que permite acesso a população 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 (2012b) e a análise foi conduzida da forma apresentada na Figura 13.

Figura 13 - Processo de Avaliação das Políticas



Fonte - O Autor

Onde na primeira fase, cada um dos princípios foi analisado individualmente e sua ideia principal extraída conforme apresentado na Figura 14.

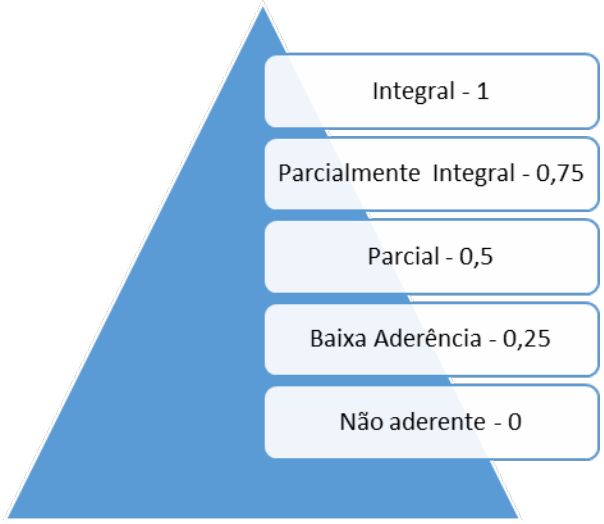
Figura 14 - Ideias dos Princípios

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 pessoaise 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 15.

Figura 15 - Escala de Aderência



Fonte - O Autor

A classificação será condensada na Tabela 2, onde será atribuída 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.

Esta 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.

Tabela 2.1 - Tabela de Aderência

	BB	Caixa	BRB	Itaú	Bradesco	Santander
SN01						
SN02						
SN03						
SN04						
SN05						
SN06						
Total SN						
DN01						
DN02						
DN03						
DN04						
Total DN						
PC01						
PC02						
Total PC						
Total Geral						
Qtd Palavras						
Percentual de Cobertura						

Fonte - O Autor

2.3 Análise dos Resultados

Os resultados condensados na Tabela 2 serão avaliados do ponto de vista do 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 a 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:

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

Esta 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 ANÁLISES E RESULTADOS

Seguindo os procedimentos propostos na metodologia, temos a Tabela 3, que mostra os resultados das análises realizadas nas políticas de segurança. No Apêndice A, podemos encontrar o detalhamento dos trechos de cada política que atribuíram as notas apresentadas na Tabela 3.

Tabela 3 - 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

Neste primeiro momento iremos analisar a construção das políticas do ponto de vista da eficácia, ou seja, analisado os índices de cobertura dos princípios contidos nas políticas afim 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 (2012b), 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 este cenário é preocupante, corroborando novamente a ideia apresentada por Von Solms (2004, p.372), uma vez que demonstra que a 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 16.

Figura 16 - 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.

Analisando a aderência das organizações dentro da área Suportar o Negócio, temos uma cobertura muito baixa nos 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 junto a 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.

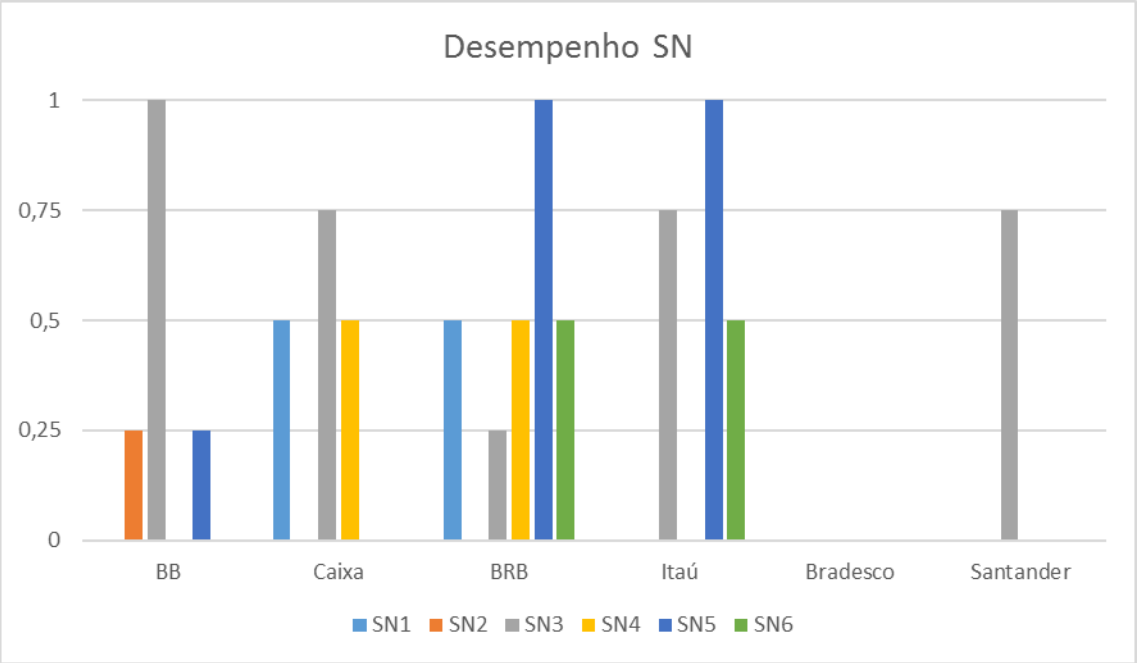
Já o princípio ‘SN4 - Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação’, também alinhado com o princípio SN2, reforça que a segurança da informação não se mostra propícia atender as necessidades 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 o alinhamento das políticas as normas ISO e recomendações regulatórias do Banco Central.

Uma consolidação do desempenho das instituições na área de Suportar o Negócio pode ser vista na Figura 17.

Figura 17 - Desempenho SN



Fonte - O Autor

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 deste 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.

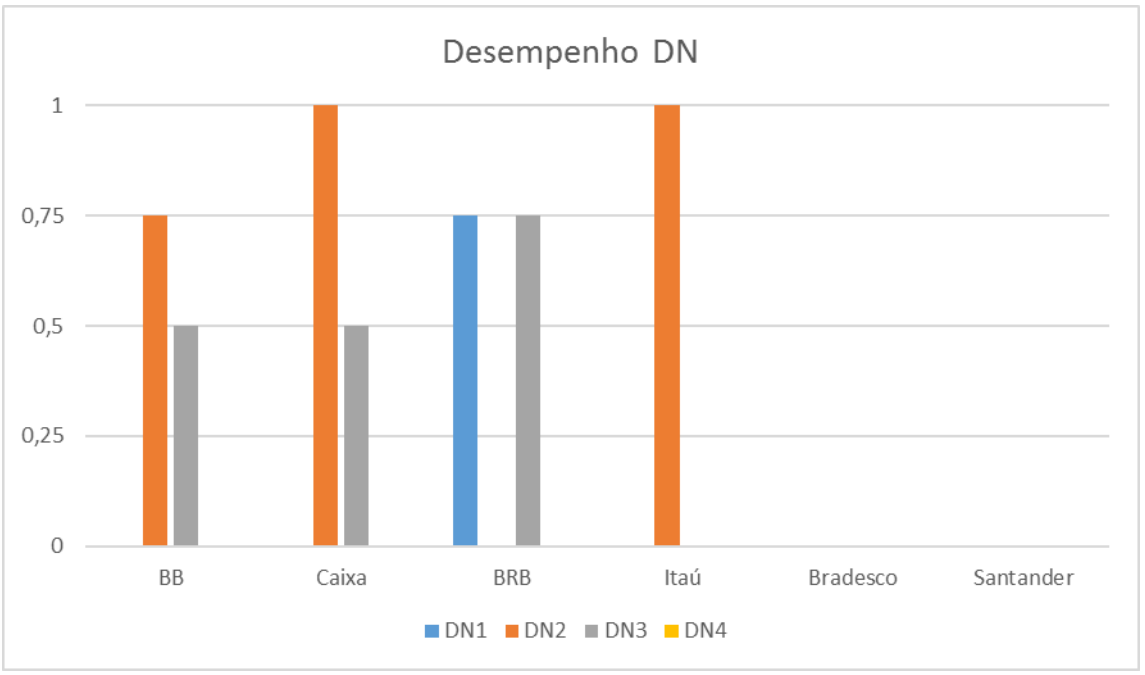
Analisando a aderência ao princípio 'DN2 - Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas', tivemos um índice maior de aderência ao princípio, porém uma situação curiosa foi que das 3 instituições que preconizaram totalmente ou parcialmente em sua política este

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.

Temos uma compilação dos resultados da área Defender o Negócio na Figura 18.

Figura 18 - Desempenho DN



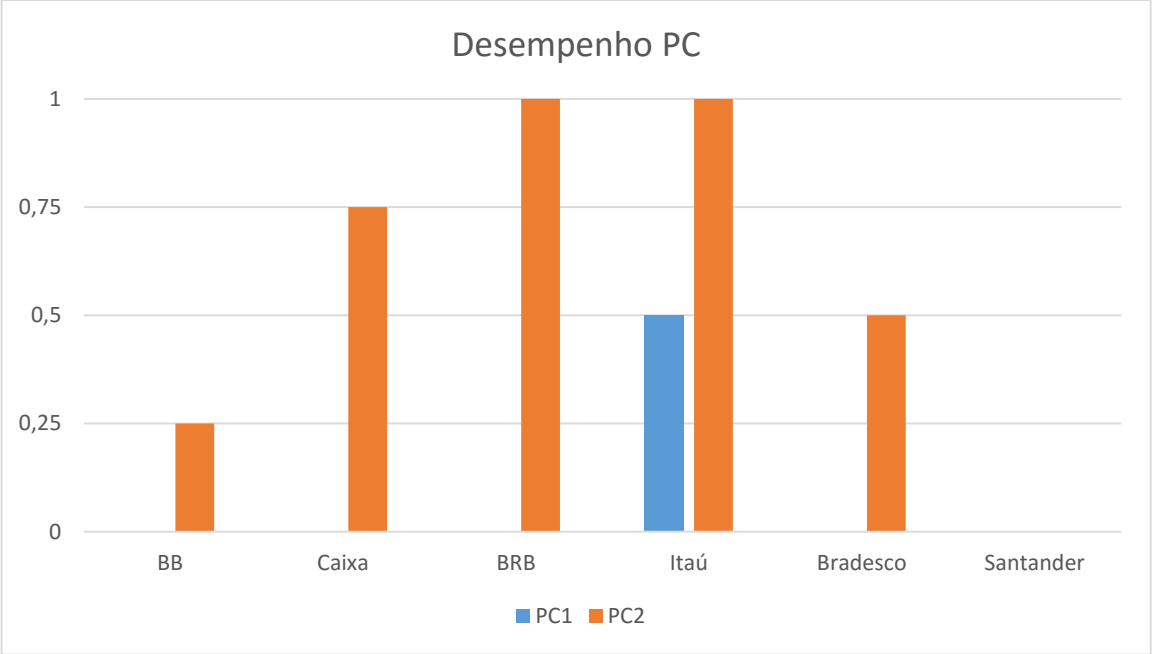
Fonte - O Autor

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, como observado na Figura 19.

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, com podemos ver na Figura 19.

Figura 19 - Desempenho PC



Fonte - O Autor

Estes 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 esta 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

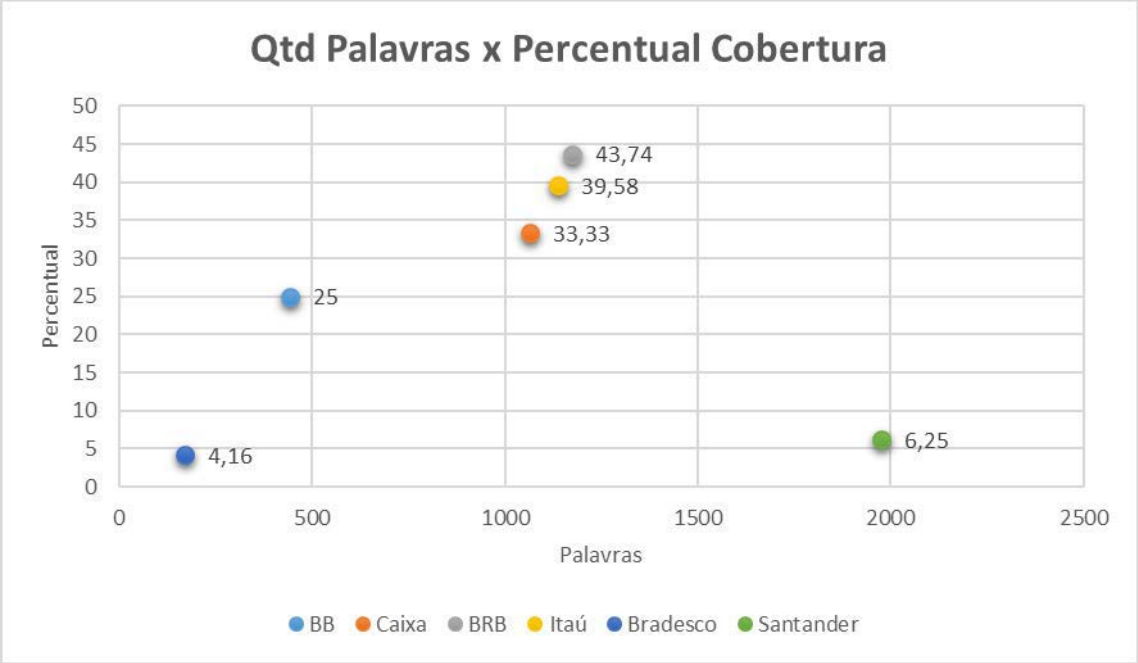
Os dados analisados até o momento nos dão uma noção da eficácia das políticas analisadas em perpetuar os termos propostos pela ISACA (2012b) quando compreendidas, porém a eficácia das políticas não pode ser avaliada pelos mesmos parâmetros.

A eficiência da política é outro fator de suma importância que devemos avaliar. Políticas muito extensas com diversos 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 e Percentual de cobertura.

A conjectura da quantidade de palavras com o percentual de cobertura nos fornece, de forma intuitiva, que quão menor for a quantidade de palavras Utilizadas e maior for o percentual coberto, mais eficaz em transmitir a mensagem a política será. Dentro desta linha de pensamento temos a Figura 20.

Figura 20- Qtd Palavras x Percentual Cobertura

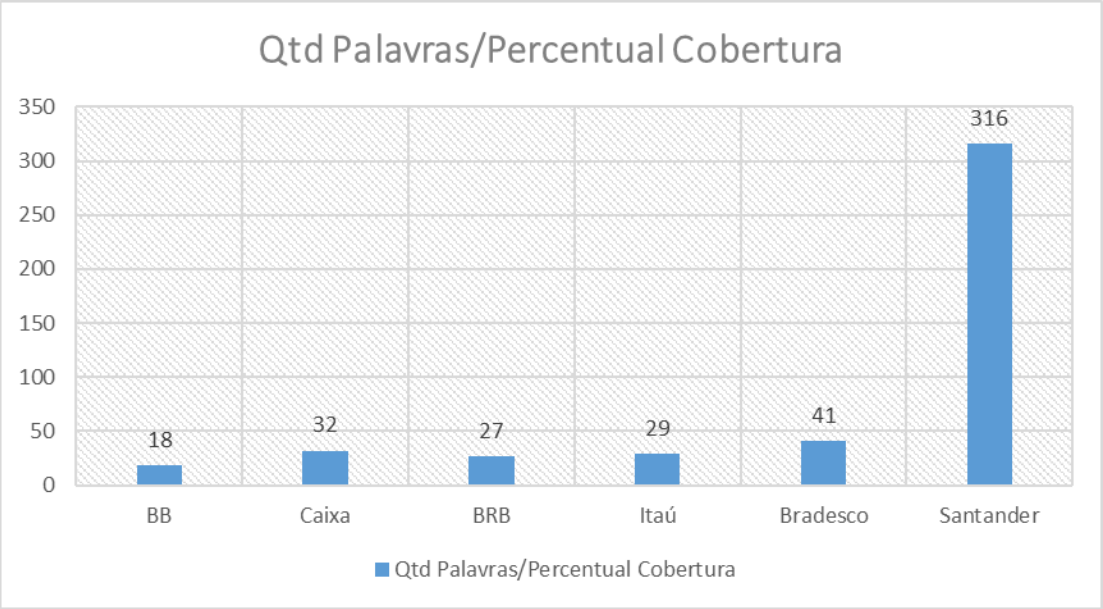


Fonte - O Autor

Na Figura 20 podemos observar que as 3 políticas com o melhor desempenho tiveram entre 1000 e 1500 palavras, enquanto que as políticas com o pior desempenho tiveram menos de 200 palavras ou mais de 1900 palavras.

Mas apenas os dados observados na Figura 20 não suficientes para inferir com mais objetividade a eficiência de cada política, para isso iremos dividir a quantidade de palavras pelo percentual de cobertura e agrupar os resultados na Figura 21.

Figura 21- Qtd Palavras / Percentual Cobertura



Fonte - O Autor

O resultado da Figura 21, permite uma avaliação mais profunda dos resultados apresentados na Figura 20. Na figura 20, temos que as 3 políticas com a melhor eficiência fizeram o uso entre 1000 e 1500 palavras, o que nos levaria assumir que a faixa de 1000 a 1500 palavras poderia ter o uso mais eficiente também, porém a Figura 21 nos mostra que a melhor eficiência foi do Banco do Brasil com uma média de 18 palavras por ponto percentual.

Está 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 (2012b), também contém muitas informações extras não relacionadas aos princípios, como aspectos técnicos ou específicos que não deveriam ser abordados inicialmente política.

A Figura 21 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.

Este 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, está 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 (2012b) 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 a 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 da mesma para os colaboradores, mais uma vez o reflexo da visão individual que as áreas de segurança trazem.

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 desta 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 deste fato em um setor tão competitivo e com diversos controles legais e regulatórios mostram que as instituições ainda não veem 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 neste 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.

BACEN, Banco Central do Brasil. **Manual de Segurança da RSFN**. 2013. Disponível em:
< http://www.bcb.gov.br/sfn/ced/manualdeseguran%C3%A7adarsfn-v32.pdf>
Acesso em: 04 nov. 2015.

CALDER A. **Implementing Information Security based on ISO 27001/ISO 27002**: A Management Guide. Nederlands: Van Haren Publishing, 2009.

CHERDANTSEVA Y. HILTON J. ***Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals***, In: F. ALMEIDA, and I. PORTELA (eds.), Organizational, 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, ed. 1. p. 1-7. 2015.

FREITAS H, BECKER J.L., HOPPEN N., KLADIS C. M. **Informação e decisão**: Sistemas de apoio e seu impacto. Porto Alegre: Ortiz, 1997.

HAYES, R. M. **Information Science Education**. Em:ALA World Encyclopedia of Library and Information Sciences. 2º edition. Chicago. American Library Association, 1986. P. 358-360.

ISACA. **COBIT 5**. Rolling Meadows: ISACA, 2012a.

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

ISO. **ISO/IEC 27000** - Information technology - Security techniques - Information security management systems - Overview and vocabular. 3. ed. Switzerland: ISO. 2014.

MARCIANO, J. L. P, MARQUES, M. L. **O Enfoque Social da Segurança da Informação**. Revista Ciência da Informação, v.35, n.3, p.89-98, set/dez 2006.

MATHEUS R. C. **Rafael Capurro e a filosofia da informação**: abordagens, conceitos e metodologias de pesquisa para a Ciência da Informação. Perspect. ciênc. inf., Belo Horizonte, v.10 n.2, p.140-165, jul/dez. 2005.

MICHAELLIS ONLINE. **Informação**. Disponível em: <

http://michaelis.uol.com.br/moderno/portugues/definicao/informacao%20_983588.html >. Acesso em: 04 nov. 2015.

OLIVEIRA, D. P. R. **Sistemas de informações gerenciais**: estratégicas, táticas, operacionais. 4º ed. São Paulo, Atlas, 1997, pg.34.

OLIVEIRA, F.M. **ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA PRODUÇÃO DE SOFTWARES**. Governança da Segurança da Informação, ed. 1. p. 145-158. 2015.

PRIMO A. F. T. **INTERAÇÃO MEDIADA POR COMPUTADOR:** a comunicação e a educação a distância segundo uma perspectiva sistêmico-relacional. Tese de Doutorado. Apresentada ao Programa de Pós- Graduação em Informática na Educação em março de 2003.

SANTOS D. L. R., SILVA R. M. S. **Segurança da Informação**: a Norma ISO/IEC 27000 e ISO/IEC. 2012. Trabalho de Segurança de Informação do MCI 2012/2013. Mestrado em Ciência da Informação. Faculdade de Engenharia da Universidade do Porto.

SÊMOLA, MARCOS. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SERRA J. P. **Manual de Teoria da Comunicação**. Covilhã: Livros Labcom, 2007. Disponível em: < http://www.livroslabcom.ubi.pt/pdfs/20110824-serra_paulo_manual_teoria_comunicacao.pdf >. Acesso em: 04 nov. 2015.

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.

APÊNDICE A – Detalhamento das notas atribuídas

Análise Banco do Brasil

Item: SN01 - Foco no Negócio
Nota: 0
Detalhamento: A política não passa nenhuma ideia da importância da segurança para o negócio. Ela não preza pelo aspecto conselheiro, sendo as proposições apresentadas de forma imperativas. O foco da política é tático e operacional, não tendo o enfoque estratégico. Uma frase da política que demonstra bem essas características é “...considerando proibido tudo aquilo que não for explicitamente permitido...”.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0.25
Detalhamento: A política não tem foco na entrega de valor para as partes interessadas. A nota não foi considerada 0 pois ao menos é previsto na política a ideia de comunicação regular que o princípio demanda, como visto no trecho “Disseminamos questões sobre segurança da informação por meio de programas permanentes de conscientização, de abrangência geral...”.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 1
Detalhamento: A política aborda as 3 questões que este princípio estipula. Ela impõe a aderência aos princípios legais e regulatórios, conforme o trecho “Espera-se que as empresas Controladas, Coligadas e Participações definam seus direcionamentos a partir dessas orientações, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.”. Ela informa as implicações legais do não cumprimento, como descrito no trecho “Analisamos as ocorrências de subtração, violação ou divulgação indevida de informações, sob os aspectos legal e disciplinar, imputando responsabilização...”. E por último ela prevê mecanismos para atualizar a política em casos de alterações, como no trecho “Periodicidade de revisão: no mínimo anualmente, ou extraordinariamente, a qualquer tempo.”.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0
Detalhamento: A política não tem nenhum foco em avaliar se a segurança entrega valor para as partes interessadas, portanto menções a métricas e medições de desempenho não aparecem no texto.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 0.25
Detalhamento: A política não tem foco na gestão do risco. O texto passa mais a ideia de tratar as consequências do que gerenciar o risco em si, conforme trecho “Identificamos e corrigimos as vulnerabilidades, as ameaças, os riscos e os impactos nocivos que envolvam os ativos de informação do Banco, por meio de procedimentos de teste e de avaliação periódicos, a intervalos regulares.”.

Item: SN06 - Promover a melhoria continua da segurança da informação
Nota: 0
Detalhamento: A política não aborda melhoria continua da segurança. Não existem menções a quaisquer avaliações dos processos de segurança.

Item: DN01 - Adotar uma abordagem baseada em riscos
Nota: 0
Detalhamento: A política não aborda faz uma abordagem baseada em riscos. Sem qualquer menção ao endereçamento de riscos

Item: DN02 - Proteger informações confidenciais
Nota: 0.75
Detalhamento: A política não aborda diretamente a classificação da informação, porém ela aborda que a informação deve ser protegida níveis de confidencialidade, como no trecho “Aplicamos proteção aos ativos de informação de forma compatível com seu impacto no Banco, alcançando todos os processos, informatizados ou não.”. O aspecto de garantir a confidencialidade da informação também é mencionado, conforme visto no trecho “Garantimos a disponibilidade, integridade e confidencialidade da informação, nos processos de coleta, armazenamento, processamento, distribuição e descarte.”.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0.5
Detalhamento: A política informa que existe outra política voltada para o assunto continuidade do negócio, como apresentado no trecho “Desenvolvemos Planos de Gestão da Continuidade de Negócios de acordo com Política Específica. ”, porém não menciona se dentro dessa política são abordados temas como sistemas prioritários e impactos na perda ou indisponibilidade de informações.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC01 - Agir de forma ética e profissional
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 0.25
Detalhamento: O foco da política não é em promover a segurança como parte fundamental do negócio, porém ela menciona que os usuários devem receber o conhecimento necessário para suas funções, conforme o trecho “Disseminamos questões sobre segurança da informação por meio de programas permanentes de conscientização, de abrangência geral, ou cursos de capacitação técnica para os usuários diretamente envolvidos na utilização de recursos.”.

Análise Caixa

Item: SN01 - Foco no Negócio
Nota: 0.5
Detalhamento: O foco da política não é apresentar a segurança como um pilar fundamental do negócio e gestão de risco, porém ela aborda que a segurança tem responsabilidades com o negócio, conforme o trecho “Segurança da informação – proteção da informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.”.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0
Detalhamento: A política não tem foco na entrega de valor para as partes interessadas. Não existe menção de promoção dos benefícios da segurança e de planos de comunicação com as partes interessadas.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 0.75
Detalhamento: A política não adere de forma explícita aos princípios legais e regulatórios necessários, como visto no trecho “Acompanham o cumprimento das regras estabelecidas para proteção das informações. ”, e também não apresenta as implicações legais envolvidas na não aderência a legislação, exceto para terceiros, como podemos ver no trecho “Os contratos que impliquem manuseio de informações da CAIXA ou por ela custodiadas possuem cláusula de confidencialidade, com intuito de garantir a observância da Política de Segurança da Informação e a responsabilização da empresa contratada.”. A reavaliação periódica e quando necessária da política foi prevista, conforme o trecho “Esta Política será revisada, sempre que se fizer necessário, não excedendo o período máximo de 03 anos.”.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0.5
Detalhamento: A política traz indicadores de efetividade, como pode ser visto nos trechos “Assinatura do Termo de Responsabilidade de Segurança da Informação pelos empregados. ” e “Empregados sensibilizados em Segurança da Informação. ”, porém não existe menção de buscar opinião das partes interessadas e os índices não apresentam a precisão necessária para o negócio ou não é um critério objetivo.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 0
Detalhamento: A política não tem foco na gestão do risco. Não é feita sequer menção a palavra risco dentro do texto da política.

Item: SN06 - Promover a melhoria continua da segurança da informação
Nota: 0
Detalhamento: A política não aborda melhoria continua da segurança. Apesar de mencionar a existência de controles e notificação de incidentes de segurança, a política não indica qual deve o uso desses indicadores.

Item: DN01 - Adotar uma abordagem baseada em riscos

Nota: 0
Detalhamento: A política não aborda faz uma abordagem baseada em riscos. Sem qualquer menção ao endereçamento de riscos

Item: DN02 - Proteger informações confidenciais
Nota: 1
Detalhamento: A política aborda de forma clara que toda informação deve ser catalogada e protegida de acordo com sua classificação, como podemos ver nos trechos “As informações, ativos essenciais para a CAIXA, são protegidas contra alteração, destruição, divulgação, cópia e impressão não autorizadas, acidentais ou intencionais. ”, “As informações são classificadas conforme seu grau de sigilo, observados os critérios estabelecidos pela CAIXA. ” e “O acesso à informação é condizente com a necessidade do usuário para o desempenho de suas atribuições na Instituição. ”.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0.5
Detalhamento: A política traz apenas a preocupação com a informação e não aborda as aplicações críticas, conforme o trecho “A recuperação da informação é assegurada como uma das formas de resguardar a continuidade dos negócios da CAIXA.”.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC01 - Agir de forma ética e profissional
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 0.75
Detalhamento: A política traz que a segurança da informação deve ser promovida dentro da organização, como observado nos trechos “Os clientes e todos os usuários são sensibilizados quanto à importância da Segurança da Informação. ” e “ Os empregados conhecem as suas responsabilidades com referência à Segurança da Informação. ”. Ela também aborda que o usuário tem o poder de proteger os ativos da organização, como visto no trecho “Comunicam imediatamente qualquer incidente de Segurança da Informação à área competente. ”. Porém não aborda a questão de prover o conhecimento necessário.

Análise BRB

Item: SN01 - Foco no Negócio
Nota: 0.5
Detalhamento: O foco da política não é apresentar a segurança como um pilar fundamental do negócio e gestão de risco, porém ela aborda que a segurança tem responsabilidades com o negócio, conforme o trecho “Adotamos procedimentos padronizados e medidas para preservar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade no tratamento das informações, possuídas ou custodiadas, que possam promover impactos na continuidade e na competitividade do negócio do conglomerado BRB”.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0
Detalhamento: A política não tem foco na entrega de valor para as partes interessadas. Não existe menção de promoção dos benefícios da segurança e de planos de comunicação com as partes interessadas.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 0.25
Detalhamento: A política não adere de forma explícita aos princípios legais e regulatórios necessários, como visto no trecho “Dispomos de acordos de confidencialidade e de não divulgação de informações confidenciais, ou sigilosas, que visam a proteção das informações do Banco... ”, e também não apresenta as implicações legais envolvidas na não aderência a legislação. A reavaliação periódica e quando necessária da política não foi prevista, sendo necessário aguardar o tempo de 2 anos para uma reavaliação, conforme trecho “Esta política possui validade de dois anos, a contar do dia útil seguinte à sua publicação...”.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0.5
Detalhamento: A política apresenta vários indicadores de performance de segurança, conforme os trechos “Buscamos implementar mecanismo que permita registrar os incidentes de segurança, tão logo sejam detectados, a fim de tratá-los adequadamente evitando sua replicação...”, “gerenciamento efetivo de incidentes para a garantia de resposta rápida, efetiva e ordenada, por meio da implementação de controles visando a manutenção do negócio” e “Registramos, periodicamente, em relatório específico, os resultados das atividades de verificação e avaliação do gerenciamento de segurança da informação...”. Porém o aspecto de garantir os objetivos das partes interessadas não é considerado.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 1
Detalhamento: A política traz a preocupação com a gestão de riscos conforme o trecho “Realizamos análises críticas periódicas dos riscos de segurança e dos controles implementados quando houver mudanças nos requisitos de negócio e suas prioridades, nas novas ameaças e vulnerabilidades, e para confirmar que os controles permanecem eficientes e adequados. ”.

Item: SN06 - Promover a melhoria continua da segurança da informação

Nota: 0.5
Detalhamento: É considerado o uso de uma base de incidentes na busca da construção de uma base de conhecimento, porém a melhoria continua da segurança não é abordada de forma clara, conforme podemos ver no trecho “Buscamos implementar mecanismo que permita registrar os incidentes de segurança, tão logo sejam detectados, a fim de tratá-los adequadamente evitando sua replicação”.

Item: DN01 - Adotar uma abordagem baseada em riscos
Nota: 0.75
Detalhamento: A política faz a abordagem do tema, porém não de forma explícita, conforme no trecho “Valemo-nos de mecanismos de controle para verificação dos fatores de risco para o negócio, custo e valor agregado em relação à tecnologia, para garantir a segurança da informação”.

Item: DN02 - Proteger informações confidenciais
Nota: 0
Detalhamento: Não a menção na política de processos de classificação da informação.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0.75
Detalhamento: A política se preocupa com a continuidade dos negócios e mudanças nos sistemas, porém não determina que os sistemas críticos devem ter prioridade, como podemos ver nos trechos “Adotamos controles rigorosos durante a implantação de mudanças, a fim de minimizar os riscos de alteração dos sistemas de informação, impondo o cumprimento de procedimentos formais;” e “Tratamos a administração da continuidade dos negócios do Grupo BRB como um processo crítico que deve envolver todos os níveis da organização”.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC01 - Agir de forma ética e profissional
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 1
Detalhamento: A política aborda os requisitos do princípio como visto no trecho “Treinamos todos os usuários das instalações, sistemas, equipamentos, documentos, informações, bens e materiais do Grupo BRB, de forma a certificá-los sobre as ameaças e preocupações quanto à segurança da informação e possibilitar o uso correto desses ativos, minimizando possíveis riscos de segurança”.

Análise Itaú

Item: SN01 - Foco no Negócio
Nota: 0
Detalhamento: Tema não abordado dentro da política.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0
Detalhamento: A política não tem foco na entrega de valor para as partes interessadas. Não existe menção de promoção dos benefícios da segurança e de planos de comunicação com as partes interessadas.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 0.75
Detalhamento: A política aborda a adesão aos requerimentos legais e as penalidades implicadas, conforme nos trechos “Os Colaboradores e Prestadores de Serviços diretamente contratados pela Instituição devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação” e “As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas das empresas da Instituição e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.”. Porém não aborda a revisão da política em detrimento de mudanças.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0
Detalhamento: Tema não abordado.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 1
Detalhamento: A política traz a preocupação com a gestão de riscos conforme o trecho “Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Instituição, para que sejam recomendadas as proteções adequadas.”.

Item: SN06 - Promover a melhoria continua da segurança da informação
Nota: 0.5
Detalhamento: A política aborda apenas a melhoria dela mesmo e não da segurança como um todo, conforme o trecho “A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de auditoria.”.

Item: DN01 - Adotar uma abordagem baseada em riscos
Nota: 0
Detalhamento: A política prevê o uso de uma gestão de risco, porém este princípio considera o endereçamento de processos de revisão e melhoria constante dos processos de risco, algo que não é citado na política.

Item: DN02 - Proteger informações confidenciais
Nota: 1
Detalhamento: Tema abordado como podemos ver no trecho “As informações

devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.”.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0
Detalhamento: A continuidade do negócio e os sistemas críticos não são temas abordados na política.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Não existe nenhuma abordagem do tema dentro da política.

Item: PC01 - Agir de forma ética e profissional
Nota: 0.5
Detalhamento: O comportamento ético é estimulado, porém não coloca a segurança como dependente das habilidades e responsabilidades das partes interessadas, conforme podemos ver no trecho “As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.”.

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 1
Detalhamento: A política aborda os requisitos do princípio como visto no trecho “A Instituição promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.”.

Análise Bradesco

Item: SN01 - Foco no Negócio
Nota: 0
Detalhamento: Tema não abordado.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0
Detalhamento: Tema não abordado.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 0
Detalhamento: Tema não abordado.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0
Detalhamento: Tema não abordado.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 0
Detalhamento: Tema não abordado.

Item: SN06 - Promover a melhoria continua da segurança da informação
Nota: 0.
Detalhamento: Tema não abordado

Item: DN01 - Adotar uma abordagem baseada em riscos
Nota: 0
Detalhamento: Tema não abordado.

Item: DN02 - Proteger informações confidenciais
Nota: 0
Detalhamento: Tema não abordado.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0
Detalhamento: Tema não abordado.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Tema não abordado.

Item: PC01 - Agir de forma ética e profissional
Nota: 0
Detalhamento: Tema não abordado

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 0.5
Detalhamento: Princípio abordado parcialmente no trecho “assegurar a participação dos colaboradores no Programa Corporativo de Conscientização e Educação em Segurança da Informação”

Análise Santander

Item: SN01 - Foco no Negócio
Nota: 0
Detalhamento: Tema não abordado.

Item: SN02 - Entregar Valor e Qualidade as Partes Interessadas
Nota: 0
Detalhamento: Tema não abordado.

Item: SN03 - Aderência aos requerimentos legais e regulatórios
Nota: 0.75
Detalhamento: A política aborda a aderência e penalidades envolvidas no não cumprimento dos requerimentos legais e regulatório, como apresentado nos trechos “Todas as atividades executadas pelo Correspondente, por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação. ” e “A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os Correspondentes às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.”. No entanto a política não prevê adaptações em caso de mudanças.

Item: SN04 - Prover informações oportunas e precisas sobre a performance da segurança
Nota: 0
Detalhamento: Tema não abordado.

Item: SN05 - Avaliar as ameaças atuais e futuras a informação
Nota: 0
Detalhamento: Tema não abordado.

Item: SN06 - Promover a melhoria continua da segurança da informação
Nota: 0.
Detalhamento: Tema não abordado

Item: DN01 - Adotar uma abordagem baseada em riscos
Nota: 0
Detalhamento: Tema não abordado.

Item: DN02 - Proteger informações confidenciais
Nota: 0
Detalhamento: Tema não abordado.

Item: DN03 - Concentrar nas aplicações críticas do negócio
Nota: 0
Detalhamento: Tema não abordado.

Item: DN04 - Desenvolver sistemas de forma segura
Nota: 0
Detalhamento: Tema não abordado.

Item: PC01 - Agir de forma ética e profissional
Nota: 0
Detalhamento: Tema não abordado

Item: PC02 - Estimular uma cultura positiva da segurança da informação
Nota: 0
Detalhamento: Tema não abordado

ANEXO A – PSI Banco do Brasil

Política Específica de Segurança da Informação

Área responsável pelo assunto: Diretoria de Gestão da Segurança (Diges).

Abrangência: Esta Política orienta o comportamento do Banco do Brasil. Espera-se que as empresas Controladas, Coligadas e Participações definam seus direcionamentos a partir dessas orientações, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

Regulamentação: Resolução 3.380/2006, do Conselho Monetário Nacional.

Periodicidade de revisão: no mínimo anualmente, ou extraordinariamente, a qualquer tempo.

Introdução: Esta Política orienta o Banco no gerenciamento da segurança da informação, demonstrando o compromisso da empresa com a proteção das informações corporativas e demais ativos de informação. Ela compõe a relação de políticas associadas ao gerenciamento do risco operacional do Banco do Brasil.

Tratamos a informação, na gestão empresarial, como ativo.

Garantimos a disponibilidade, integridade e confidencialidade da informação, nos processos de coleta, armazenamento, processamento, distribuição e descarte.

Aplicamos proteção aos ativos de informação de forma compatível com seu impacto no Banco, alcançando todos os processos, informatizados ou não.

Concedemos acesso para o funcionário do Banco somente às informações necessárias ao desempenho de suas funções e atribuições ou por determinação legal.

Adotamos mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens e roubo, quando do tratamento (coleta, acesso, manuseio, guarda, divulgação, transporte e descarte) das informações geradas ou utilizadas pelo Banco.

Preservamos a confidencialidade, integridade, disponibilidade, autenticidade e conformidade, na gestão, custódia e uso das informações, considerando proibido tudo aquilo que não for explicitamente permitido.

Procedemos à identificação e definição de, pelo menos, um gestor na administração da informação (busca, gerenciamento, controle, acompanhamento e identificação de ameaças à segurança).

Obedecemos ao princípio de segregação das funções de desenvolvimento de recursos, uso de recursos, administração da segurança e auditoria, na gestão da informação.

Desenvolvemos Planos de Gestão da Continuidade de Negócios de acordo com Política Específica.

Disseminamos questões sobre segurança da informação por meio de programas permanentes de conscientização, de abrangência geral, ou cursos de capacitação técnica para os usuários diretamente envolvidos na utilização de recursos.

Identificamos, nos sistemas de controle de acesso, cada usuário individualmente, responsabilizando-o, juntamente com o administrador que lhe concedeu o acesso, pelas atividades realizadas sob seu código de identificação.

Preservamos os mesmos quesitos de segurança adotados pelo Banco, na contratação de serviços ou de pessoas e no relacionamento com colaboradores, parceiros, contratados e estagiários.

Analisamos as ocorrências de subtração, violação ou divulgação indevida de informações, sob os aspectos legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades.

Identificamos e corrigimos as vulnerabilidades, as ameaças, os riscos e os impactos nocivos que envolvam os ativos de informação do Banco, por meio de procedimentos de teste e de avaliação periódicos, a intervalos regulares.

ANEXO B – PSI Caixa

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA CAIXA

SUMÁRIO DA NORMA

PREFÁCIO

TÍTULO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA CAIXA

UNIDADE GESTORA

GEROP - GN RISCO OPERACIONAL

UNIDADE(S) CORRESPONSÁVEL(IS)

Não se aplica.

CLASSIFICAÇÃO

Normativo de Políticas de Atuação CAIXA

PÚBLICO ALVO

Todas as Unidades da CAIXA.

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

Alterações:

Atualização do grau de sigilo em consonância com o OR016.

Relação com Outros Normativos – exclusão dos normativos listados em consonância com o OR002.

Regulamentação Utilizada – exclusão do Decreto 3.505, de 13.06.2000 e do Decreto 4.553, de 27.12.2002, e inclusão da Resolução do Conselho de Administração nº 15 – Ata nº 288, de 26.03.2013 e da Resolução do Conselho Diretor nº 2292, de 22.01.2013.

RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica.

REGULAMENTAÇÃO UTILIZADA

Resolução do Conselho de Administração – Ata n° 251, de 10.08.2011.

Resolução do Conselho de Administração nº 15 – Ata nº 288, de 26.03.2013.

Resolução do Conselho Diretor n° 5.428, de 02.08.2011.

Resolução do Conselho Diretor nº 2292, de 22.01.2013.

DOCUMENTAÇÃO UTILIZADA

Não se aplica

ROTEIRO PADRÃO

Não se aplica

ATENDIMENTO DE DÚVIDAS

GEROP - GN RISCO OPERACIONAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA CAIXA

1 OBJETIVO

1.1 Estabelecer princípios e diretrizes para proteção e disciplina do uso dos ativos de informação da CAIXA ou sob sua custódia, assegurando a confidencialidade, integridade, autenticidade e disponibilidade.

2 DEFINIÇÕES

- Ativo – bem tangível e intangível que tem valor para a organização;
- Incidente de segurança – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança pessoal, patrimonial e de tecnologia da informação e comunicação, tais como tentativas de ganhar acesso não autorizado a instalações, sistemas ou dados, ataques de negação de serviço, desrespeito à Política de Segurança da Instituição e sequestro de dignitários;
- Mesa Limpa e Tela Limpa – adoção de procedimentos adequados, especialmente fora do horário normal de trabalho, para o tratamento de papéis e mídias que devem ser guardados em locais seguros, e de computadores pessoais e impressoras que não devem ser deixados ligados quando não estiverem em uso e devem ser protegidos por senhas ou outros controles, na ausência do usuário;
- Segurança da informação – proteção da informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. Preservar a autenticidade, confidencialidade, integridade e disponibilidade da informação, garantir o não-repúdio, assegurar que o acesso seja obtido somente por pessoas autorizadas, garantir a exatidão e completeza da informação, a manutenção dos métodos de processamento e que os usuários autorizados obtenham acesso à informação e aos correspondentes sempre que necessário;
- Trilha de auditoria – constitui-se de um *log* de eventos históricos predefinidos, para apuração de ocorrências, de forma a identificar quem realizou a ação, quando, onde e o que foi realizado;
- Usuário – empregado, prestador de serviço, usuário fábrica ou estagiário autorizados a terem acesso a informações, dados, materiais ou documentos da CAIXA para desempenho de suas atribuições, respeitando a classificação que lhes foi atribuída.

3 NORMAS

3.1 PRINCÍPIOS E DIRETRIZES

3.1.1 PRINCÍPIOS

3.1.1.1 DISPONIBILIDADE

3.1.1.1.1 Propriedade da informação de estar acessível e utilizável sob demanda por uma entidade autorizada.

3.1.1.2 INTEGRIDADE

3.1.1.2.1 Propriedade de salvaguarda da exatidão e completeza da informação.

3.1.1.3 CONFIDENCIALIDADE

3.1.1.3.1 Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

3.1.1.4 AUTENTICIDADE

3.1.1.4.1 Propriedade de que a informação é verdadeira e fidedigna tanto na origem quanto no destino.

3.1.2 DIRETRIZES

3.1.2.1 As informações, ativos essenciais para a CAIXA, são protegidas contra alteração, destruição, divulgação, cópia e impressão não autorizadas, acidentais ou intencionais.

3.1.2.2 A recuperação da informação é assegurada como uma das formas de resguardar a continuidade dos negócios da CAIXA.

3.1.2.3 As senhas, ou outros mecanismos utilizados no controle de acesso aos sistemas da CAIXA, são pessoais e intransferíveis e não são compartilhadas.

3.1.2.4 As informações são classificadas conforme seu grau de sigilo, observados os critérios estabelecidos pela CAIXA.

3.1.2.5 O acesso à informação é condizente com a necessidade do usuário para o desempenho de suas atribuições na Instituição.

3.1.2.6 Os ambientes onde são tratados dados e informações são segregados, conforme a sua classificação e tipo de uso (desenvolvimento, homologação, rede, suporte e produção de sistemas corporativos).

3.1.2.7 Os sistemas da CAIXA possuem trilha de auditoria em razão do grau de sigilo da informação ou por exigência legal.

3.1.2.8 A prática de “Mesa Limpa e Tela Limpa” é adotada por todos os usuários.

3.1.2.9 Os clientes e todos os usuários são sensibilizados quanto à importância da Segurança da Informação.

3.1.2.10 Os empregados conhecem as suas responsabilidades com referência à Segurança da Informação.

3.1.2.11 As informações e recursos disponibilizados pela CAIXA são de uso exclusivo para fins relacionados ao trabalho.

3.1.2.12 Os contratos que impliquem manuseio de informações da CAIXA ou por ela custodiadas possuem cláusula de confidencialidade, com intuito de garantir a observância da Política de Segurança da Informação e a responsabilização da empresa contratada.

3.1.2.13 Esta Política será revisada, sempre que se fizer necessário, não excedendo o período máximo de 03 anos.

3.2 INDICADORES DE EFETIVIDADE

3.2.1 TERMO DE RESPONSABILIDADE DE SEGURANÇA DA INFORMAÇÃO

3.2.1.1 Assinatura do Termo de Responsabilidade de Segurança da Informação pelos empregados.

3.2.2 CULTURA CORPORATIVA EM SEGURANÇA DA INFORMAÇÃO

3.2.2.1 Empregados sensibilizados em Segurança da Informação.

3.3 RESPONSABILIDADES

3.3.1 UNIDADE RESPONSÁVEL PELA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

3.3.1.1 Promover a disseminação do conhecimento em Segurança da Informação.

3.3.1.2 Definir os critérios e procedimentos para a classificação da informação e para sua proteção.

3.3.2 UNIDADES DA CAIXA

3.3.2.1 Adotam mecanismos que garantam, em conjunto com as unidades responsáveis pela segurança tecnológica, eletrônica e física, as formas de proteção das informações sob sua gestão contra alteração, destruição, divulgação e cópia não autorizadas, acidentais ou intencionais.

3.3.2.2 Acompanham o cumprimento das regras estabelecidas para proteção das informações.

3.3.2.3 Conhecem e executam os procedimentos relativos à Segurança da Informação que lhe digam respeito.

3.3.2.4 Comunicam imediatamente qualquer incidente de Segurança da Informação à área competente.

4 PROCEDIMENTOS

Não se aplica.

5 ARQUIVAMENTO DE DOCUMENTOS

Não se aplica.

6 ANEXOS

Não se aplica.

ANEXO C – PSI BRB

Índice - clique aqui

#10

BRB BANCO DE BRASÍLIA	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Código	A.GOV.1.016/0005
		Responsável	SUSEM/GESEI
		Vigência	3/11/2014 – 2/11/2016
		Página	1/5

TÍTULO: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

CLASSIFICAÇÃO: NORMA ESTRATÉGICA

FINALIDADE: Estabelecer e disciplinar as diretrizes e definições da estrutura de segurança da informação para o conglomerado BRB.

ELABORAÇÃO: Superintendência de Segurança da Informação/Gerência de Segurança da Informação – Susem/Gesei.

APROVAÇÃO: Aprovada em Ata da 558ª Reunião do Conselho de Administração – CONSAD, em 31/10/2014, nos termos da Nota Executiva VIFIP/DIRCO – 2014/011, de 16/10/2014.

INÍCIO DE VIGÊNCIA: 3 de novembro de 2014.

NORMAS EXTERNAS RELACIONADAS:
Lei nº 7.232, de 29 de outubro de 1984.
Lei nº 9.296, de 24 de julho de 1996.
Lei Complementar 105, de 10 de janeiro de 2001.
Decreto Distrital nº 34.276, de 11 de abril de 2013.
Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.
ABNT NBR ISO IEC 17799:2005.
ABNT NBR ISO/IEC 27001:2005.
ABNT NBR ISO/IEC 27004:2010.

NORMAS INTERNAS RELACIONADAS:
Manual de Segurança da Informação e Comunicações – Susem/Gesei.
Manual de Classificação de Informação – Susem/Gesei.
Manual do Correio Eletrônico – Susem/Gesei.

NORMAS REVOGADAS: Política de Segurança da Informação, 4ª versão, aprovada em ata da 2.910ª reunião de Diretoria, de 26/10/2010.

HISTÓRICO:
1ª versão - Aprovada na 416ª Reunião de Diretoria, em 16/12/2003.
2ª versão - Aprovada na 2.509ª Reunião de Diretoria, em 20/03/2007.
3ª versão - Aprovada na 2.853ª Reunião de Diretoria, em 18/02/2010.
4ª versão - Aprovada na 2.910ª Reunião de Diretoria, em 26/10/2010.

BRB BANCO DE BRASÍLIA	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Código	A.GOV.1.016/0005
		Responsável	SUSEM/GESEI
		Vigência	3/11/2014 – 2/11/2016
		Página	2/5

ÍNDICE

TÍTULO I – DISPOSIÇÕES GERAIS
CAPÍTULO I – PRINCÍPIOS

Art. 1º. Os seguintes princípios norteiam a gestão da segurança da informação na Instituição:

I - Adotamos procedimentos padronizados e medidas para preservar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade no tratamento das informações, possuídas ou custodiadas, que possam promover impactos na continuidade e na competitividade do negócio do conglomerado BRB;

II - Utilizamos medidas de proteção das informações contra acesso, modificação, destruição ou divulgação não autorizada, garantindo sua confidencialidade, disponibilidade, integridade e não repúdio;

III - Buscamos garantir a segurança dos ativos que custodiam informações do Grupo BRB e fiscalizamos os processos que lhes são afetos;

IV - Valemo-nos de mecanismos de controle para verificação dos fatores de risco para o negócio, custo e valor agregado em relação à tecnologia, para garantir a segurança da informação;

V - Dispomos de acordos de confidencialidade e de não divulgação de informações confidenciais, ou sigilosas, que visam a proteção das informações do Banco, e informam aos signatários das suas responsabilidades, para proteger, usar ou divulgar a informação de maneira responsável e autorizada;

VI - Valemo-nos de requisitos e controles de segurança quando da necessidade de acesso aos recursos de processamento da informação, ou a informação do Banco por partes externas ou clientes;

VII - Treinamos todos os usuários das instalações, sistemas, equipamentos, documentos, informações, bens e materiais do Grupo BRB, de forma a certificá-los sobre as ameaças e preocupações quanto à segurança da informação e possibilitar o uso correto desses ativos, minimizando possíveis riscos de segurança;

VIII - Dispomos de canal interno para denúncias, garantido o anonimato do denunciante e assegurada a investigação, pois não toleramos fraudes ou atos ilícitos por parte de empregados ou colaboradores do Banco;

IX - Dispomos de sistema de segurança física para proteção dos acessos aos ambientes, do transporte de equipamentos e de documentação, com perímetro estabelecido de acordo com a criticidade dos locais, atividades e informações do conglomerado BRB;

X - Mantemos em segurança e protegidos por barreiras, eletrônicas ou não, todos os recursos e instalações de processamento de informações críticas ou sensíveis do negócio, inclusive equipamentos para contingência e mídia de backup, de acordo com a avaliação dos riscos e procedimentos claramente definidos;

XI - Buscamos a adoção de modelo de gestão das operações dos ativos de processamento de informações do Grupo BRB, visando o uso seguro e correto destes recursos, abrangendo a definição de procedimentos operacionais apropriados;

XII - Buscamos a segregação de funções e áreas para reduzir as oportunidades de modificação ou uso indevido, não autorizado ou não intencional, dos ativos da organização; e também a segregação dos ambientes de recursos de desenvolvimento, teste e produção, para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais;

XIII - Buscamos utilizar procedimentos e diretrizes de backups que permitam, em quaisquer situações, a recuperação de softwares, sistemas, dados, jobs e documentação, guardados em meio magnético, e que devem ser verificados e testados regularmente, para garantir sua efetividade;

XIV - Realizamos análises críticas periódicas dos riscos de segurança e dos controles implementados quando houver mudanças nos requisitos de negócio e suas prioridades, nas novas ameaças e vulnerabilidades, e para confirmar que os controles permanecem eficientes e adequados;

XV - Adotamos controles rigorosos durante a implantação de mudanças, a fim de minimizar os riscos de alteração dos sistemas de informação, impondo o cumprimento de procedimentos formais;

XVI - Dispomos, para os casos de terceirização do desenvolvimento de software, de acordos de licença, propriedade de código e de Direitos de Propriedade Intelectual e evolução do Sistema e cobramos requisitos contratuais com respeito à qualidade do código e à existência de garantias;

XVII - Buscamos implementar mecanismo que permita registrar os incidentes de segurança, tão logo sejam detectados, a fim de tratá-los adequadamente evitando sua replicação;

XVIII - Tratamos a administração da continuidade dos negócios do Grupo BRB como um processo crítico que deve envolver todos os níveis da organização;

XIX - Mantemos um gerenciamento efetivo de incidentes para a garantia de resposta rápida, efetiva e ordenada, por meio da implementação de controles visando a manutenção do negócio;

XX - Registramos, periodicamente, em relatório específico, os resultados das atividades de verificação e avaliação do gerenciamento de segurança da informação, para conhecimento da área avaliada e, se necessário, a instância superior.

TÍTULO I – DISPOSIÇÕES GERAIS
CAPÍTULO II – ÂMBITO E VALIDADE

Art. 2º. Esta política possui validade de dois anos, a contar do dia útil seguinte à sua publicação, e deverá ser cumprida por todos os empregados, parceiros, consultores, especialistas ou pessoas contratadas em regime temporário, estagiários, menores aprendizes e pessoas integrantes do quadro de pessoal de empresas contratadas.

Art. 3º. As diretrizes estabelecidas neste documento devem ser observadas pelo Banco e pelas demais empresas que compõem o Conglomerado BRB e aplica-se também a todos os ativos, equipamentos, software básico e aplicativos de propriedade do BRB ou de entidade parceira, assim como aqueles contratados em qualquer regime e integrantes da infraestrutura de Tecnologia da Informação do Banco.

Parágrafo único. As subsidiárias integrais do Banco, BRB DTVM e Financeira BRB, deverão aderir a esta norma mediante formalização de Termo de Adesão, enquanto que as demais empresas Controladas confeccionarão suas próprias normas à luz dos princípios aqui elencados.

ANEXO D – PSI Itaú

Política Corporativa de Segurança da Informação

1. OBJETIVO

A informação é um dos principais bens de qualquer organização. Assim, a Instituição estabelece a presente Política Corporativa de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações da organização, dos clientes e do público em geral.

2. PÚBLICO-ALVO

Esta política destina-se a todos os colaboradores e órgãos usuários de informações do Itaú Unibanco Holding S.A., suas empresas controladas no Brasil e exterior.

Para os fins do disposto nesta política “Itaú Unibanco Holding S.A." passa a ser substituído pelo termo “Instituição” no restante do texto, “Itaú Unibanco Brasil” passa a ser substituído por “Matriz” e o termo “Colaboradores” abrange todos os empregados, menores aprendizes, estagiários e administradores da Instituição.

3. RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionados pelo Comitê Corporativo de Segurança da Informação, coordenado pela Diretoria de Segurança Corporativa e composto por representantes das áreas de Riscos e Controles Internos, Auditoria, Tecnologia e Negócios da Instituição.

4. REGRAS

4.1 Regra Geral

As políticas de segurança da informação precisam estar disponíveis em local de acesso dos Colaboradores e protegida contra alterações.

A nomenclatura e o código das políticas de segurança da informação precisam ser mantidos com a mesma identificação da Matriz.

As políticas de segurança da informação são revisadas anualmente pela Matriz, encaminhadas para as unidades onde forem aplicáveis e sua revisão e publicação é de responsabilidade da unidade local após aprovação da Matriz.

4.2 Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da Instituição, clientes e público em geral está fundamentado nos seguintes princípios:

- confidencialidade - Garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

- disponibilidade - Garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;

- integridade - Garantimos a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

4.3 Diretrizes de Segurança da Informação

A Segurança da Informação na Instituição estabelece os principais controles, denominados diretrizes:

a) As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

c) Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um Colaborador ou equipe de Colaboradores.

d) O acesso às informações e recursos só deve ser feito se devidamente autorizado.

e) A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

f) A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

h) Os riscos às informações da Instituição devem ser reportados à área de Segurança da Informação.

i) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

4.4 Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

4.5 Gestão da Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Instituição adota os seguintes processos:

a) Gestão de Ativos da Informação

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Instituição.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

d) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Instituição, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

e) Tratamento de Incidentes de Segurança da Informação

Os incidentes de Segurança da Informação da Instituição devem ser reportados à Diretoria de Segurança Corporativa.

f) Conscientização em Segurança da Informação

A Instituição promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

g) Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de auditoria.

4.6 Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à Instituição não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

4.7 Declaração de Responsabilidade

Os Colaboradores e Prestadores de Serviços diretamente contratados pela Instituição devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos da Instituição devem possuir cláusula que assegure a confidencialidade das informações.

4.8 Medidas Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas das empresas da Instituição e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.

5. DOCUMENTOS RELACIONADOS

Esta Política Corporativa de Segurança da Informação é complementada por normas específicas de Segurança da Informação (circulares SI, integrantes do conjunto de normativos do Itaú Unibanco) em conformidade com os aspectos legais e regulamentares e aprovadas pela Superintendência de Continuidade de Negócios e Gestão de Crises e pela Superintendência de Segurança da Informação, subordinadas à Diretoria de Segurança Corporativa, na estrutura da Área Seguros, Controles e Apoio Operacional da Instituição. Devem ser observadas, também, as regras estabelecidas na política sobre Gerenciamento de Risco Operacional em Serviços Terceirizados.

6. GLOSSÁRIO

Instituição: Itaú Unibanco Holding S.A., suas empresas controladas no Brasil e exterior.

Matriz: Itaú Unibanco Brasil.

Segregação de funções: o ato pelo qual o Colaborador não pode exercer mais que uma função no processo de aprovação.

7. ÓRGÃO RESPONSÁVEL

A Diretoria de Segurança Corporativa é responsável por manter e atualizar esta política.

ANEXO E – PSI Bradesco

Bradesco

Política Corporativa de Segurança da Informação

Versão 6.0

Departamento de Segurança Corporativa

A **Política Corporativa de Segurança da Informação** tem como diretrizes básicas:

1. assegurar a confidencialidade, integridade e disponibilidade das informações da Organização, mediante utilização de mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;

2. garantir a proteção adequada das informações e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados;

3. assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização, estando sujeitos à monitoração e auditoria;

4. assegurar a participação dos colaboradores no Programa Corporativo de Conscientização e Educação em Segurança da Informação; e

5. garantir o cumprimento dessa Política e das Normas Corporativas de Segurança da Informação da Organização.

****

Declaramos que a presente é cópia fiel da Política Corporativa de Segurança da Informação, aprovada na RECA nº 1.762, de 9.5.2011, cuja última revisão, sem alterações, foi registrada na ata da RECA nº 2.125, de 28.10.2013.

Banco Bradesco S.A.

Alexandre da Silva Glüher
Diretor Executivo Gerente

ANEXO F – PSI Santander

Santander
FINANCIAMENTOS

REF.: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA CORRESPONDENTE BANCÁRIO DO SANTANDER.

1. SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao Santander e prejudicar nosso crescimento e vantagem competitiva. Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação do Santander.

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando o Santander a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

- **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1. Proteção da Informação

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos do Santander, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Toda informação relacionada às operações do Santander, gerada ou desenvolvida nas dependências do Santander ou do Correspondente, durante a execução das atividades de prestador de serviços de correspondente no país para o Santander, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios do Santander.

É diretriz que toda informação de propriedade do Santander seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

2.2. Responsabilidades

É missão e responsabilidade de cada Correspondente, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento

da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pelo Correspondente, por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

Para auxiliar a todos os colaboradores nessa missão, o Santander criou a área de Segurança da Informação, que administra as disciplinas de conhecimento que dão suporte a essa ciência. A Superintendência de Segurança da Informação é responsável por editar as políticas e padrões que apóiam a todos na proteção dos ativos de informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema. A Central de Atendimento do Correspondente/Revendedor está apta a orientar e tratar as questões relacionadas ao tema.

2.3. Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pelo Santander e/ou obtidas pelo Correspondente em decorrência da execução do contrato de prestação de serviços de correspondentes no país.

São responsáveis pela observância desta Política os diretores, empregados, agentes e consultores (incluindo advogados, auditores e consultores financeiros) do Correspondente.

O Correspondente que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito do Santander. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pelo Santander. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades de correspondente no país.

O Correspondente deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.

O Correspondente deverá informar prontamente ao Santander sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política: (i) o atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunal arbitrais e de órgãos públicos administrativos; (ii) a divulgação das informações confidenciais aos agentes, representantes (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e empregados das partes; e, (iii) as informações confidenciais que forem divulgadas após o consentimento, por escrito, do Santander.

Se a qualquer uma das partes ou seus representantes legais, que detém as informações confidenciais, for solicitado ou requerido, oralmente ou por escrito, solicitações de informações de documentos, mandados de investigações civis ou qualquer outro pedido similar, para revelar tais informações confidenciais, deverá notificar prontamente a outra parte para que esta tenha tempo hábil para verificação, inclusive, se for o caso, aplicar as ressalvas contidas nos termos desta Política.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o Correspondente de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

2.4. Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de Segurança da Informação, por meio da Central de Atendimento do Revendedor. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- uso ilegal de software;
- introdução (intencional ou não) de vírus de informática;
- tentativas de acesso não autorizado a dados e sistemas;
- compartilhamento de informações sensíveis do negócio;
- divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração do Santander e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os Correspondentes às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, o Correspondente deve entrar em contato com a Central de Atendimento do Correspondente/Revendedor.

3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEG. INFORMAÇÃO

3.1. Classificação da Informação

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas pelo Correspondente de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário. Cabem ao Correspondente todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem do Santander, podendo levar à extinção das operações ou prejuízos graves ao crescimento.

São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas do Santander frente ao mercado;
- Todo o material estratégico do Santander (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações do Santander, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

3.2. Acesso a Sistemas e Recursos de Rede

O Correspondente é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Periodicamente, os acessos concedidos devem ser revistos pelo Correspondente.

3.3. Utilização dos Recursos de Informação

Apenas os equipamentos e software disponibilizados e/ou homologados pelo Santander podem ser instalados e conectados à rede do Santander.

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

3.4. Autenticação e Senha

O Correspondente é responsável por todos os atos executados com seu identificador (login / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os Correspondentes devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum. Ou seja, não contá-la a ninguém e não anotá-la em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

3.5. Direito de Acesso (Autorização)

O Correspondente é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que são atribuídos aos seus funcionários, estagiários, prestadores de serviços, parceiros e visitantes, sendo intransferíveis.

A solicitação de acesso à informação deve decorrer da necessidade funcional do Correspondente. .

3.6. Direitos de Propriedade

Todo produto resultante do trabalho dos Correspondentes (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade do Santander.Em caso de extinção ou rescisão do contrato de prestação de serviços de correspondente no país, por qualquer motivo, deverá o Correspondente devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços ao Santander, ou emitir declaração de que as destruiu.

3.7. Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Organização.

3.8. Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

3.9. Conversas em Locais Públicos e registro de informações

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas ao Santander.

3.10. Leis e Regulamentos

É de responsabilidade do Correspondente conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

Santander Financiamentos
Banco Santander (Brasil) S.A.