DOI: 10.5102/un.gti.v4i2.2966

Um novo olhar sobre as políticas de segurança da informação para o segmento de telefonia do Brasil*

A new look at information security policies for the telephony segment Brazil

Mauricio R. Lyra[1]
Kleuber Tormim[2]
Vitor T. Nishi[3]

Resumo

A construção de políticas de segurança nas organizações, nos últimos anos, vem, em sua grande parte, se baseando nas normas ISO17799 e 27002. Em 2010 um consórcio formado por importantes atores internacionais no cenário da segurança da informação propõe 12 princípios relevantes a serem considerados na construção dessas políticas. O trabalho que se apresenta usa esses critérios na análise da política de segurança de 04 grandes empresas do segmento de telefonia do Brasil. Um olhar atento dessas políticas à luz dos critérios mostra que diferente de um cenário homogêneo e linear, como esperado inicialmente, o cenário que se apresenta é heterogêneo e não linear, mostrando grande disparidade entre as empresas analisadas. Por fim a pesquisa conclui que, apesar do segmento analisado ser um dos mais competitivos, regulados, legislados e com um volume consideravelmente grande de informações brutas que são tratadas, o uso da governança da segurança da informação ainda não é visto como um viabilizador da governança corporativa e uma forma de ser ganhar uma vantagem estratégica em relação à concorrência.

Palavras-chave: Segurança da Informação. Compliance. Políticas. Telefonia.

Abstract

The process to build security policies in organizations in recent years has, for the most part, been based on the standards ISO17799 and 27002. In 2010 a consortium of major international actors in the scenario of information security proposes 12 relevant principles to be considered on building these policies. The work that is presented here, uses these criteria in the analysis of security policy of 04 large companies in Brazil telephony segment. A careful look on these policies, in light of the adopted criteria, shows that, different from a homogeneous and linear scenario as originally we hoped, the scenario presented is heterogeneous and non-linear, showing great disparity between the companies we analyzed. Finally it concludes that despite the analyzed segment is one of the most competitive, regulated, legislated and with a considerably large volume of raw information that are daily processed, the use of governance principles in information security is still not seen as an enabler of corporate governance and a way to be gain a strategic advantage over the competition.

Keywords: Information Security. Compliance. Policy. Politics.

* Recebido em 13/08/2014
Aprovado em 02/10/2014

[1] Doutor em Ciência da Informação pela UNB. Professor do curso de pós graduação de Governança de TI no UniCEUB. Professor dos cursos de graduação em Ciência da computação e Engenharia da Computação do UniCEUB. Profissional no ramo de segurança da informação e autor do livro Segurança e Auditoria em sistemas informação pela editora Ciência Moderna.

[2] Possui graduação em Ciência da Computação pelo Centro Universitário de Brasília (UniCEUB), trabalhou três anos na CTIS como Analista de Suporte, atualmente é Consultor Citsmart na Central IT Governança Corporativa, implantando a Governança de TI com apoio de Software ITSM. Possui certificações Itil, Cobit, 20000, 27000 e Green IT.

[3] Bacharel em engenharia da computação pelo UniCEUB, aluno do curso de pós graduação de Governança de TI no UniCEUB. Gestor de ambientes de testes de TI em empresa de telefonia.

1 Introdução

A segurança da informação é uma preocupação básica que permeia todas as organizações e compreende aspectos, como confidencialidade, integridade e disponibilidade, visando proteger a informação que é um ativo dos ativos organizacionais mais importantes de uma empresa.

Tendo como princípio a segurança da informação, faz-se necessário a construção de políticas voltadas para os temas, como um instrumento viabilizador para que os conceitos, regras e estratégia da organização sejam difundidas, aplicadas e suportadas.

A construção de políticas de segurança da informação, ao longo dos anos, baseou-se basicamente nas normas propostas pela ISO, porém em 2010, um consórcio formado pelo ISACA, ISF e International Information System Security Certification Consortium [(ISC)2] propôs 12 princípios não proprietários, independentes e agrupados em 3 grupos categorizados como Suportar o Negócio, Defender o Negócio e Promover o comportamento responsável em segurança da informação, como apresentados e consolidados na Figura 1.1, que poderiam direcionar a construção de políticas de segurança da informação de forma a agregar valor as instituições mantenedoras de maneira não apenas tática e normatizada, mas também alinhando e considerando as necessidades estratégicas do negócio como ponto fundamental em uma política de segurança (SOUZA NETO, 2012).

Figura 1 – Princípios de Governança da Segurança da Informação

SN01	Concentrar-se no negócio para garantir que a segurança da informação esteja integrada nas atividades essenciais de negócio
SN02	Entregar qualidade e valor para as partes interessadas para garantir que a segurança da informação agregue valor e atenda requisitos de negócios.
SN03	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.
SN04	Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação.
SN05	Avaliar ameaças à informação atuais e futuras para analisar e avaliar ameaças emergentes de segurança da informação para que ações motivadas e oportunas de mitigação de risco possam ser tomadas.
SN06	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.
DN01	Adotar uma abordagem baseada em risco para garantir que o risco é tratado de uma maneira consistente e efetiva.
DN02	Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas.
DN03	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.
DN04	Desenvolver sistemas de forma segura para construir sistemas de qualidade, com relação custo/benefício aceitável, nos quais os gerentes de negócio possam confiar.
PC01	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.
PC02	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.

Fonte: (SOUZA NETO, 2012).

Com base nos princípios propostos pelo consórcio descrito anteriormente, decidiu-se realizar uma pesquisa qualitativa e quantitativa, visando analisar a aderência de políticas da segurança da informação dentro de um nicho de mercado competitivo, sujeito a um número considerável de regulamentações e legislações e com um volume muito alto de dados gerados, classificados, mantidos e protegidos.

Devidas as características do nicho de mercado, optou-se por buscar políticas dentro de operadoras de telecomunicações que é um segmento no Brasil de ampla concorrência, composto basicamente por 8 empresas que dispõem de um portfólio diversificado de produtos oferecidos concorrendo entre si em diversos segmentos do mercado. É um nicho sujeito a uma série de regulamentações e legislações que está em constante modificação e deve lidar com um volume de dados considerável.

Por motivos legais de privacidade, os nomes das empresas não serão divulgados, sendo tratada apenas como Empresa A, Empresa B, Empresa C e Empresa D.

2 Referencial teórico

Para construção do referencial teórico deste trabalho, primeiramente foi pesquisado na literatura da área o conceito de segurança, segurança da informação e as políticas de segurança da informação das organizações analisadas. Em seguida procurou-se levantar o valor das informações organizacionais, sua forma de classificação e sua importância para a continuidade do negócio. Numa visão da gestão da segurança da informação, Souza Neto (2012) apresenta doze princípios da Governança da Segurança da Informação propostos pelo ISACA, ISF e *International Information System Security Certification Consortium*.

2.1 Conceito de segurança da informação

A ISACA, *Systems Audit and Control Association*, define segurança da informação 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). A segurança da informação é uma forma de escudo usado para resguardar esse ativo intangível que é a informação e é dentro das organizações que a mesma se encontra de forma mais intensificada.

É importante ressaltar que é impossível conseguir segurança absoluta e investir em segurança exige um alto custo. Segundo o dicionário Houaiss et al. (2006), segurança é um estado em que se está livre de perigos e incertezas. Uma importante medida a ser tomada buscando a segurança da informação é a criação de uma política de segurança da informação com o intuito de minimizar os riscos à segurança.

Para Cernev e Leite (2005), deve-se tomar muito cuidado com a definição de segurança pela confusão corrente do termo com risco, privacidade e confiança. No caso da confiança explica: "confiança engloba e significa muito mais do que segurança. Confiança é o pilar de sustentação de qualquer negócio ou empreendimento, tradicional ou eletrônico, dentro ou fora da Internet, sendo a segurança um dos seus principais construtos" (CERNEV; LEITE, 2005, p. 1).

Existem alguns termos relacionados à gestão da segurança da informação que merecem atenção; são eles (SÊMOLA, 2003; BEAL, 2005):

- Ativo: é todo recurso que pode sofrer algum tipo de ataque, logo, precisa de proteção.
- Ameaça: é algo que oferece um risco e tem como foco algum ativo. Uma ameaça também pode aproveitar-se de alguma vulnerabilidade do ambiente.
- Vulnerabilidades: os ataques com mais chances de dar certo são aqueles que exploram vulnerabilidades, seja ela uma vulnerabilidade do sistema operacional, aplicativos ou políticas internas.
- Ataque: evento decorrente da exploração de uma vulnerabilidade por uma ameaça.
- Incidente: evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

2.2 Conceito de política de segurança da informação

O *The Site Security Handbook - Request for Comments* 2196 (RFC 2196) é um manual para desenvolvimento de políticas de segurança de computador e procedimentos para *sites* que têm seus sistemas na Internet. O propósito desse manual é proporcionar um guia prático aos administradores, tentando tornar segura uma grande variedade de informações e serviços. De acordo com esse manual, uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

De acordo com a norma, Política de Segurança da Informação é um documento para prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. As normas ISO 17799 e BS 7799 são padrões de excelência internacional que orientam a organização do Sistema de Gestão de Segurança da Informação (SGSI). Devemos observar que o desenvolvimento e implantação de um Sistema de Gestão de Segurança da Informação, além da organização da documentação, exigem a implementação de controles para atender aos objetivos de segurança da organização. A norma está dividida em 10 capítulos principais, contendo 127 controles de segurança e mais de 500 subcontroles, mantendo seu foco na gestão do risco, a partir da análise do risco e os dispositivos de controle e avaliação permanente das ameaças e vulnerabilidades que incidem sobre os ativos da informação de uma empresa. A ISO 27001 é considerada a parte que orienta a implementação do

sistema de segurança da informação objetivando a sua verificação e certificação.

Segundo Cerias (CER 01)[1], existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Ainda, de acordo com a norma NBR ISO/IEC 17799, os elementos da política de segurança que devem ser considerados são:

- A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente.
- A Legalidade: deve estar em conformidade com as leis.
- A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
- A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
- A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

2.3 Implementando a Governança da Segurança da Informação

O IT Governance Institute[2] (ITGI), estabelecido em 1998 para melhoria do pensamento e dos padrões internacionais de direção e controle da tecnologia da informação nas organizações, define Governança de Segurança da Informação como um subconjunto da Governança Corporativa que fornece direção estratégica, garante que os objetivos sejam alcançados, gerencia os riscos de forma adequada, usa os recursos organizacionais responsavelmente, e monitora o sucesso ou falha do programa de segurança corporativa.

Para implementar a gestão da segurança da informação, Adriana Beal (2005) sugere o uso da metodologia PDCA, muito utilizado em sistemas de gestão da qualidade. PDCA, do inglês, PLAN - DO - CHECK - ACT é um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos. É também conhecido como o ciclo de *Deming*.

Com o uso do método PDCA, a Beal (2005) estipulou as seguintes etapas aplicadas à gestão da segurança da informação:

- Planejamento da segurança – começando do nível mais alto, identificam-se os processos críticos de negócio e dos fluxos de informação associados, para depois descer para o nível dos sistemas e serviços de informação e da infraestrutura de TI que dá suporte a tais sistemas e serviços;
- Implementação da segurança – as atividades necessárias para se colocar em prática aquilo que foi planejado para atender aos requisitos de segurança da organização;
- Avaliação e ação corretiva – deve-se coletar o maior número possível de informações e averiguar se a segurança implantada atende aos requisitos da fase de planejamento;
- Análise crítica independente da segurança da informação – recomenda que seja feito, por auditoria interna ou prestador de serviços especializado na área, um levantamento que ajude a garantir que as práticas da organização permaneçam condizentes com sua política e adequadas para situação de risco existente.

Quando se implementa um processo de gestão da segurança da informação, procura-se eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível. (Caruso e Steffen, 1999).

Seguindo os princípios descritos anteriormente, o consórcio formado pelo ISACA, ISF e *International Information System Security Certification Consortium* [(ISC)2] propôs um total de 12 princípios fundamentais, divididos em 3 tarefas principais, conforme apresentado por Souza Neto (2012), que buscam implementar valores de governança dentro das políticas de segurança da informação. A implementação desses princípios visa tornar a política de segurança de informação mais eficaz e eficiente no mecanismo de agregação de valor ao negócio que este viabilizador proporciona.

Para Souza Neto (2012), existem três tarefas principais que contém um total de 12 princípios fundamentais, propostos pelo consórcio ISACA, ISF e International

1 CERIAS – The Center for Education and Research in Information Assurance and Security < http://www.cerias.purdue.edu/>, acessado em 17 de maio de 2014.

2 ITGI – IT Governance Institute <http://www.itgi.org/>, acessado em 17 de maio de 2014.

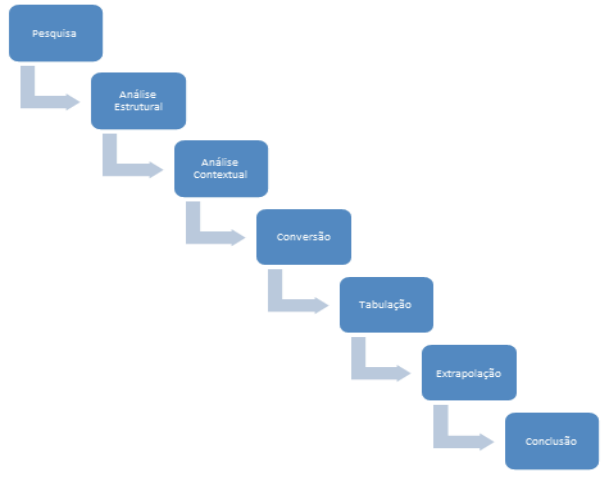
Information System Security Certification Consortium [(ISC)2], que buscam transformar a segurança da informação como um pilar viabilizador da governança corporativa, agregando valor as suas organizações.

3 Metodologia

3.1 Processo

Este estudo se caracteriza por uma avaliação primariamente qualitativa e secundariamente quantitativa, em que foi aplicada uma abordagem estruturada em cascata, partindo desde a pesquisa da massa de dados, passando por uma contextualização da mesma, até chegar em uma conclusão extrapolada de inferências baseadas em tabelas e gráficos, conforme pode ser visto na Figura 2.

Figura 2 – Visão Consolidada do Processo



Fonte: Dos autores

O passo inicial foi o levantamento da massa de dados para pesquisa. Nesse passo buscou-se, junto a prestadores de serviços ou funcionários das empresas operadoras de telefonia as políticas de segurança, em que, dentre as 8 operadoras possíveis, conseguimos as políticas de 4.

O passo seguinte foi realizar uma análise da estrutura e do conteúdo das políticas, de maneira a verificar se a forma como foi escrita o texto da política seria mais formal ou mais intuitiva, se sua preocupação primária era ou não atender as normas das ISO17779 e ISO27002 e, por fim, se os temas foram abordados de forma clara e genérica ou foram abordados de forma específica e pouco genérica.

Subsequentemente, iniciamos uma análise do conteúdo das políticas buscando menções aos princípios propostos inicialmente na Figura 1 Cada princípio foi analisado individualmente, buscando no texto referência, menções ao contexto subjetivo apresentado na Figura 3.

Figura 3 – Tabela de conversão de princípios

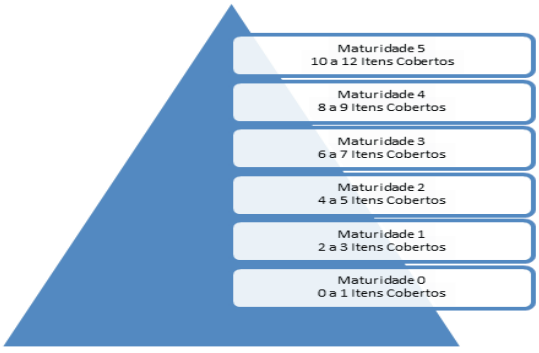
SN01	Mencões que a política deve ser alinhada ao negócio
SN02	Menções que política deve se preocupar com o valor agregado ao negocio
SN03	Menções que a política deve ser aderente a regulamentações e/ou legislações
SN04	Menções que resultados de análises e auditorias devem ser fornecidos e utilizados
SN05	Menções que a análise de riscos deve ser considerada em cada ação tomada
SN06	Menções de melhoria continua da política
DN01	Menções de foco na gestão de risco
DN02	Menções de controle de acesso a informação
DN03	Menções de foco na continuidade de aplicações criticas
DN04	Menções de desenvolvimento de sistemas de forma segura
PC01	Menções de ações de uso responsável e profissional dos ativos e recursos da empresa
PC02	Menções de ações de treinamento e divulgação da segurança na entidade

Fonte: (SOUZA NETO, 2012).

O passo seguinte foi montar uma tabela, contendo os 12 princípios e as 4 empresas analisadas, de forma organizar a identificar quais foram os princípios atendidos e não atendidos, conforme os parâmetros propostos na Figura 3, assim realizando uma conversão dos dados contextuais em dados numéricos, possibilitando a tabulação dos resultados.

Uma vez sendo possível quantificar a aderência de uma política aos princípios propostos, aplicamos uma escala de maturidade, atribuindo, de acordo com a quantidade de itens aderentes, um nível de maturidade para cada empresa, conforme pode ser visto na Figura 4.

Figura 4– Escala de Maturidade



Fonte: Dos autores

Além da aplicação da escala de maturidade descrita, a tabulação dos dados permitiu o próximo passo, que foi a construção de gráficos da quantidade, distribuição e concentração de princípios atendidos por empresa, possibilitando a visualização dos dados em um novo panora-

ma, no qual foi possível, novamente, extrapolar dos dados numéricos para inferências contextuais, o que permitiu, por fim, chegar as conclusões.

4 Resultados e análises

Conforme descrito na metodologia, o primeiro passo para iniciar a análise dos resultados foi consolidar em dados de aderência dos princípios em uma tabela, conforme visto na Tabela 5, de forma permitir uma tabulação desses resultados.

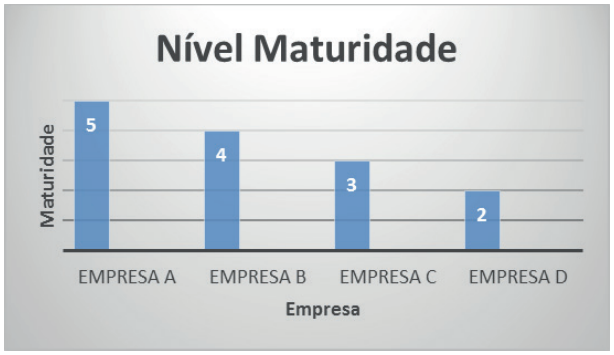
Tabela 1 – Resultados Consolidados

Código Princípio	Empresa A	Empresa B	Empresa C	Empresa D
SN01	Sim	—	Sim	—
SN02	Sim	—	—	—
SN03	Sim	Sim	—	—
SN04	Sim	—	—	—
SN05	Sim	Sim	Sim	—
SN06	Sim	—	—	Sim
DN01	Sim	Sim	Sim	—
DN02	Sim	Sim	Sim	Sim
DN03	—	Sim	—	Sim
DN04	—	Sim	—	Sim
PC01	Sim	Sim	Sim	—
PC02	Sim	Sim	Sim	—

Fonte: Dos autores

Aplicando-se a escala de maturidade apresentada na Figura 4, podemos definir o grau de maturidade das empresas analisadas, conforme apresentado na Figura 4.

Figura 5 – Nível de Maturidade

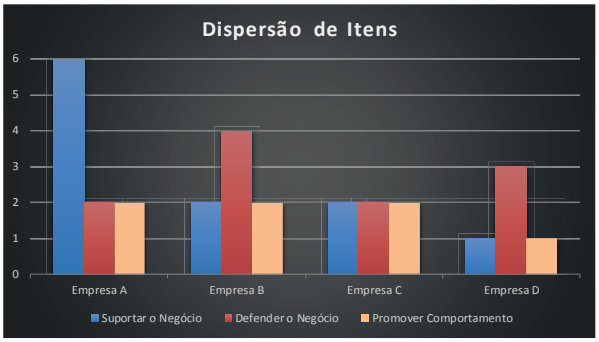


Fonte: Dos autores

Ao analisar o nível de maturidade das empresas, podemos perceber que, diferentemente do esperado inicialmente, as empresas não apresentaram um resultado homogêneo. Cada empresa apresentou um nível de maturidade distinto, o que revela, somado à avaliação da estrutura das políticas analisadas, que a segurança da informação não é vista como um agregador de valor ao negócio e sim apenas um cumprimento de requisição para uma certificação ISO 27002.

Esse ponto é reforçado ao analisar a distribuição dos princípios atendidos pelas empresas, conforme Figura 6.

Figura 6 – Dispersão de Itens



Fonte: Dos autores

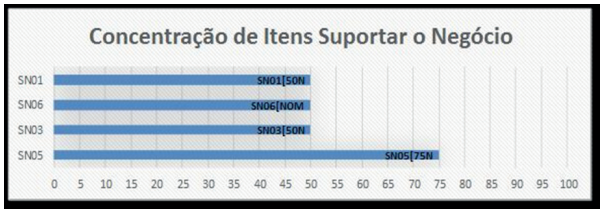
Pode-se observar que apenas uma das empresas avaliadas tem como preocupação primária, na construção de sua política de segurança, o grupo de princípios Suportar o Negócio, ou seja, apenas uma empresa tem a visão de utilizar a política como um viabilizador para agregar valor ao negócio.

A figura 6 também nos demonstra, que os grupos Defender o Negócio e Promover o comportamento responsável em segurança da informação possuem uma aderência a seus itens distribuída de forma mais homogênea entre as empresas, reforçando a preocupação das empresas em utilizar a política da segurança da informação como um instrumento mais tático e operacional e menos estratégico.

Percebe-se que, dentro do grupo "Suportar o Negócio", que o princípio "Avaliar ameaças à informação atuais e futuras para analisar e avaliar ameaças emergentes de segurança da informação para que ações motivadas e oportunas de mitigação de risco possam ser tomadas", foi o item mais atendido, com 3 empresas aderentes, seguidos pelos princípios "Cumprir os requisitos legais e regulatórios pertinentes para garantir que obrigações estatutárias sejam cumpridos, as expectativas das partes interessadas sejam gerenciadas e penalidades civis ou criminais sejam evitadas", "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" e "Con-

centrar-se no negócio para garantir que a segurança da informação esteja integrada nas atividades essenciais de negócio", com 2 empresas aderentes, como podemos ver na Figura 7.

Figura 7 – Concentração de Itens no Grupo Suportar o Negócio

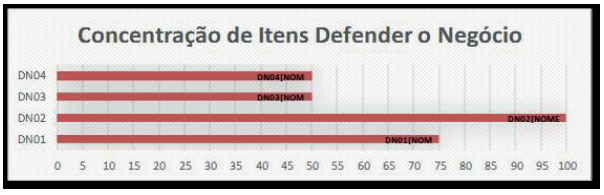


Fonte: Dos autores

Isso mostra que a maior parte das empresas analisadas tem preocupação com o gerenciamento de riscos à segurança da informação, mais que uma preocupação com aderência a regulamentos e legislações e que com a melhoria dos processos de segurança.

Ao analisar o grupo "Defender o Negócio", temos o princípio "Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas" coberto por todas as políticas, seguido pelo princípio "Adotar uma abordagem baseada em risco para garantir que o risco é tratado de uma maneira consistente e efetiva" que é coberto por 3 empresas e os demais cobertos por 2 empresas cada, como pode ser visto na Figura 8.

Figura 8 – Concentração de Itens no Grupo Defender o Negócio

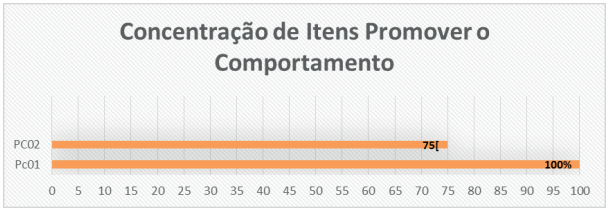


Fonte: Do autor

Pode-se inferir que o controle do acesso as informações é uma preocupação em comum a todas as empresas e que a preocupação com o gerenciamento de riscos em 3 das 4 empresas é plausível, uma vez que em 3 empresas o item do grupo de "Suporte ao Negócio" mais coberto foi justamente o de gerenciamento de riscos.

Em relação ao grupo "Promover o Comportamento", o princípio "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" todas as empresas tiverem itens que abordam o assunto e o outro item 3 atenderam, conforme Figura 9.

Figura 9 – Concentração de Itens no Grupo Promover o Comportamento



Fonte: Dos autores

Apenas a Empresa D não possuía itens em sua política aderentes ao princípio "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". Apesar de a política ser baseada na ISO 17779, políticas de treinamento e de conscientização dos funcionários não foi inclusa no documento.

Ao analisar os itens com menor cobertura em relação às políticas verificadas, os princípios "Entregar qualidade e valor para as partes interessadas para garantir que a segurança da informação agregue valor e atenda requisitos de negócios" e "Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação", do grupo de "Suportar o Negócio" foram previstos em apenas 1 das 4 empresas analisadas, o que mostra, como citado anteriormente, que não existiu um preocupação, na maioria das empresas, em agregar valor ao negócio por meio da segurança e que a melhoria continua da segurança também não foi um princípio levado em conta.

5 Conclusão

Apesar das características do segmento de telecomunicações no Brasil demandarem uma visão mais corporativa, competitiva e dinâmica das empresas, o resultado do nível de maturidade das empresas e o foco das empresas não foram o esperado quando a avaliação das empresas foi iniciada. Era de se esperar que um dos focos da governança corporativa nas empresas fosse em

utilizar as políticas de segurança da informação como viabilizador, agregando valor ao negócio e aumentando a competitividade das empresas no segmento, porém o que observamos foi um nível de maturidade heterogêneo e pouco foco no grupo Suportar o Negócio.

Percebe-se que apenas uma das empresas avaliadas possui uma preocupação em alinhar a segurança da informação com negócio, portanto, foco no grupo Suportar o Negócio e em paralelo que todas tenham um foco primário nos grupos Defender o Negócio e Promover o Comportamento. Isso sugere que a política da segurança da informação ainda é vista mais como um documento tático e operacional, com o intuito apenas de garantir as recomendações da norma ISO 27002, do que como um potencial viabilizador da governança na empresa.

Avaliando individualmente cada grupo, essa preocupação com o nível tático é reforçada ao observamos que princípios baseados em entrega de valor e melhoria continua não são prioridade, porém princípios baseados em controle de acesso e gerenciamento de riscos são focos comuns a todas empresas.

Essa análise, por fim, sugere que a adoção das boas práticas de governança de segurança da informação dentro das empresas do segmento de telefonia do Brasil, ainda tem muito a evoluir e contribuir para a diferenciação das organizações em um segmento de mercado bastante competitivo.

Referências

BEAL, Adriana. *Segurança da informação:* princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. *Segurança em informática e de informações*. São Paulo: SENAC, 1999.

CERIAS – The Center for Education and Research in Information Assurance and Security. West Lafayette, [2014?]. Disponível em: <http://www.cerias.purdue.edu/>. Acesso em: 17 maio 2014.

CERNEV, Adrian Kemmer; LEITE, Jaci Corrêa. *Segurança na Internet:* a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil. Rio de Janeiro: ENANPAD, 2005.

ITGI – IT Governance Institute. *About ITGI*. Rolling Meadows, [2014]. Disponível em: <http://www.itgi.org/>. Acesso em: 17 maio 2014.

SOUZA NETO, João. *Gestão e governança de segurança da informação no ambiente de TI*. Material de curso. CEGSIC 2012-2014. 2012. TCC (Graduação) - Curso de Especialização em Gestão da Segurança da Informação e Comunicações, Universidade de Brasília, Brasília, 2012.