Universidade de Brasília
Instituto de Psicologia
Departamento de Processos Psicológicos Básicos
Programa de Pós-Graduação em Ciências do Comportamento

Efeitos de procedimentos de controles de segurança da informação sobre a conduta de colaboradores: Uma análise comportamental.

Rafael Almeida de Paula

Orientador: Prof. Dr. Jorge Mendes de Oliveira-Castro Neto

Brasília, dezembro de 2020

Universidade de Brasília
Instituto de Psicologia
Departamento de Processos Psicológicos Básicos
Programa de Pós-Graduação em Ciências do Comportamento

Efeitos de procedimentos de controles de segurança da informação sobre a conduta de colaboradores: Uma análise comportamental.

Rafael Almeida de Paula

Orientador: Prof. Dr. Jorge Mendes de Oliveira-Castro Neto

Tese Apresentada ao Programa de Pós-Graduação em Ciências do Comportamento, Instituto de Psicologia, Área de Concentração em Análise do Comportamento, como parte dos requisitos para a conclusão do curso de Doutorado.

Brasília, dezembro de 2020

Banca Examinadora

A Banca Examinadora foi composta por:

_____

Prof. Dr. Jorge Mendes de Oliveira-Castro Neto (Presidente)

Universidade de Brasília – Instituto de Psicologia

_____

Profa. Dra. Carla Peixoto Borges (Membro Efetivo)

Universidade de Brasília – Departamento de Administração

_____

Prof. Dr. Júlio César de Aguiar (Membro Efetivo)

Fundação Getúlio Vargas – FGV

_____

Prof. Dr. Paulo Roberto Cavalcanti (Membro Efetivo)

Centro Universitário de Brasília – UniCeub

_____

Profa. Dra. Ariela Oliveira Holanda (Membro Suplente)

Instituto Federal do Paraná – IFPR

Agradecimentos

Primeiramente, a Deus por estar presente em todos os dias da minha vida e me conceder mais essa graça.

Agradeço aos meus pais, Hélio e Elenita, pelo amor incondicional e por todo apoio e incentivo que sempre deram aos meus estudos, especialmente, nessa conquista.

Aos meus filhos, Pedro e Júlia, pela paciência e compreensão nos momentos que não pude estar mais próximo e por serem a minha motivação para buscar sempre ser melhor.

À minha companheira, minha esposa, Alice, agradeço a paciência, apoio, compreensão e incentivo ao longo desses anos.

Aos professores Ariela Holanda, Carla Peixoto, Júlio Aguiar e Paulo Cavalcanti por prontamente aceitarem participar da minha banca examinadora e pelo cuidado e dedicação na avaliação do meu trabalho.

Agradeço aos meus colegas de trabalho Sandro Tomazelle, Gilvan Nogueira e Rilson Ramos, cujo apoio foi fundamental para a conclusão dessa tese. Aos colegas de pós-graduação, pelo companheirismo, discussões e ideias que contribuíram para a conclusão deste trabalho.

Por fim, um agradecimento especial ao meu orientador Jorge, pelo exemplo profissional, pelas valiosas orientações, mas, principalmente, por ter sido meu grande incentivador para enfrentar esse desafio, meu muito obrigado!

Sumário

Introdução....13
Comportamento e a gestão da segurança da informação....14
Análise Comportamental do Direito....24
Análise Comportamental do Direito aplicada ao SGSI....32
Objetivos....38
Estudo 1....39
Método....41
Resultados....43
Discussão....60
Estudo 2....67
Método....68
Resultados....77
Discussão....87
Estudo 3....91
Método....93
Resultados....95
Discussão....108
Discussão Geral....117
Considerações Finais....126
Referências....130
Apêndice A....1
Apêndice B....28
Apêndice C....30

Lista de Tabelas

Tabela 1. Quadro comparativo entre o direito e o SGSI como sistemas sociais funcionalmente especializados. 37

Tabela 2. Categorias comportamentais identificadas na política de segurança da informação da organização participante. 47

Tabela 3. Relação das contingências planejadas por item com a meta social do sistema de gestão de segurança da informação da organização. 62

Tabela 4. Consolidação dos estados motivacionais e reforços para os colaboradores identificados nas contingências planejadas por categoria comportamental. 64

Tabela 5. Relação das categorias comportamentais por contexto da contingência planejada. 66

Tabela 6. Distribuição das empresas participantes por número de usuários internos. 96

Tabela 7. Tempo de política de segurança da informação formalizada. 96

Tabela 8. Adoção da prática de registrar e monitorar as atividades dos usuários internos. 97

Tabela 9. Número de violações da política de segurança da informação tratadas nos últimos cinco anos. 98

Tabela 10. Frequência de ocorrência das categorias de padrões comportamentais. 100

Tabela 11. Relação da forma de monitoramento das atividades dos usuários com a indicação de baixa frequência das categorias de padrões comportamentais. 101

Tabela 12. Média de frequência das categorias de padrões comportamentais por perfil de empresa de acordo com a forma de monitoramento das atividades dos usuários. 102

Tabela 13. Frequência de sanções aplicadas. 102

Tabela 14. Medidas complementares/efeitos decorrentes do enforcement da PSI. 104

Tabela 15. Relação da aplicação de sanções com o porte da empresa. 105

Tabela 16. Relação do porte da empresa com as afirmações acerca da necessidade de investir em soluções complementares para controlar os comportamentos dos colaboradores e do tratamento das violações da PSI prontamente realizado na esfera técnica. 106

Tabela 17. Relação da aplicação de sanções com a maturidade da empresa na gestão da segurança da informação. 107

Tabela 18. Relação da maturidade em gestão da segurança da informação com as afirmações acerca da necessidade de investir em soluções complementares para controlar os comportamentos dos colaboradores e do tratamento das violações da PSI prontamente realizado na esfera técnica. 108

Lista de Figuras

Figura 1. Modelo PDCA aplicado aos processos de um SGSI (ABNT, 2013a). 15
Figura 2. Descrição da contingência planejada na primeira categoria. 48
Figura 3. Explicitação das metas sociais relacionadas à contingência planejada para a primeira categoria. 49
Figura 4. Identificação das premissas factuais relevantes da contingência estabelecida na primeira categoria. 51
Figura 5. Descrição da contingência planejada para a segunda categoria. 52
Figura 6. Explicitação das metas sociais relacionadas à contingência planejada para a segunda categoria. 53
Figura 7. Identificação das premissas factuais relevantes da segunda categoria. 54
Figura 8. Descrição da contingência planejada para a terceira categoria. 56
Figura 9. Explicitação das metas sociais relacionadas à contingência planejada para a terceira categoria. 57
Figura 10. Identificação das premissas factuais relevantes da terceira categoria. 58
Figura 11. Descrição da contingência planejada para a quarta categoria. 59
Figura 12. Explicitação das metas sociais relacionadas à contingência planejada para a terceira categoria. 59
Figura 13. Identificação das premissas factuais relevantes da quarta categoria. 60
Figura 14. Processo de gestão de incidentes de segurança da informação. 72
Figura 15. Processo disciplinar estabelecido pela organização. 74
Figura 16. Exemplo de identificação do primeiro nó da norma de segurança de informação. 75
Figura 17. Exemplo de análise das contingências vigentes em um nó da norma de segurança de informação. 76
Figura 18. Primeiro nó da norma de segurança da informação. 78
Figura 19. Análise das contingências vigentes no primeiro nó da norma de segurança de informação (i.e., registrar suspeita de incidente/convocação ou não da ETIR). 82
Figura 20. Segundo nó da norma de segurança da informação. 84
Figura 21. Análise das contingências vigentes no segundo nó da norma de segurança de informação (i.e., tratamento do incidente de SI/não apuração de responsabilidade). 86
Figura 22. Forma como os registros das atividades dos usuários internos são usados na identificação e tratamento das violações da PSI. 98
Figura 23. Avaliação do enforcement da política de segurança da informação. 103
Figura 24. Consolidação da frequência das categorias de padrões comportamentais. 111

“Há dois fatores indispensáveis a uma vida satisfatória e relativamente feliz. Um é segurança e o outro é liberdade. Você não consegue ter uma vida digna na ausência de um deles. Segurança sem liberdade é escravidão; liberdade sem segurança é caos...”.

Zygmunt Bauman

Resumo

O tratamento dos riscos relacionados ao comportamento dos colaboradores nas organizações representa um grande desafio na implantação dos sistemas de gestão da segurança da informação. A principal medida adotada é a definição de políticas de segurança da informação, cuja maioria dos estudos restringe-se aos aspectos formais de sua elaboração ou aborda as ações de conscientização como instrumentos de sua implantação. Nesse trabalho é proposto um novo modelo para tratar esses riscos, calcado no arcabouço teórico e metodológico estabelecido pela análise do comportamento, em especial, a teoria analítico-comportamental do direito, mediante a interpretação dos sistemas de gestão de segurança da informação (SGSIs) como subsistemas sociais funcionalmente especializados. Para aferir a viabilidade dessa proposta, isto é, a análise comportamental dos sistemas de gestão de segurança da informação, foram realizados três estudos. No Estudo 1 foi realizada a análise comportamental da política de segurança da informação (PSI) de um órgão da administração pública federal, em que foram identificadas, descritas e analisadas as contingências planejadas no normativo. Os resultados demonstraram que o *enforcement* da política está calcado na aplicação de sanções e contribuíram para a identificação de falhas, incoerências e medidas complementares para o controle mais eficaz e eficiente dos comportamentos que violam os requisitos de segurança da informação da organização participante. O Estudo 2 avançou na aplicação desse modelo, mediante a análise comportamental da norma social do SGSI estabelecido na organização participante, enquanto uma rede de padrões comportamentais entrelaçados. Com a sua consecução, foram identificados os principais nós comportamentais, a partir dos quais foram identificadas e analisadas as contingências que de fato estavam vigentes e controlavam comportamentos relevantes para o SGSI. A principal constatação do Estudo 2 foi que, apesar de prevista na PSI, a organização não adota a prática de sancionar as condutas que violam seus requisitos de segurança da informação.

Ou seja, a PSI instituída dificilmente exerce controle sobre os comportamentos a que se destina. Acerca disso, destaca-se que os resultados do referido estudo corroboraram essa conclusão, pois verificou-se que essa ineficiência, em controlar o comportamento dos colaboradores, levou a organização a investir em medidas complementares para dificultar as condutas que violam seus requisitos de segurança da informação. No mesmo sentido, foi verificado que os incidentes de segurança da informação são, usualmente, prontamente tratados na esfera técnica, o que reduz seus impactos e, consequentemente, a percepção de gravidade pelo restante da organização, fato que reduz a probabilidade de aplicação das sanções previstas pelas autoridades administrativas. Sendo assim, o Estudo 2 também apontou a possibilidade de medidas alternativas com vistas ao controle mais eficiente dos comportamentos que violam a PSI da organização participante. No Estudo 3 buscou-se obter uma visão mais abrangente dos principais achados dos primeiros dois estudos, mediante a aplicação de um questionário junto a 21 diretores de tecnologia da informação de empresas brasileiras. Seus resultados corroboraram os principais achados dos primeiros dois estudos, isto é, que o *enforcement* das PSIs está calcado na aplicação de sanções, que as empresas não aplicam ou raramente aplicam essas sanções, logo investem em mecanismos de proteção complementares para dificultar a ocorrência de violações de sua PSI e que, nos casos em que esses mecanismos não são suficientes para impedi-las, os incidentes de segurança da informação são prontamente tratados pelas unidades de tecnologia da informação, reduzindo seu efeito aversivo para o restante da organização. Tomados em conjunto, os três estudos demonstraram a viabilidade da interpretação analítico-comportamental dos SGSIs e apontam um novo e promissor caminho para a mitigação dos riscos organizacionais.

Palavras-chave: análise comportamental do direito, segurança da informação, política de segurança da informação, comportamento, usuário.

Abstract

The treatment of risks related to employee behavior in organizations represents a major challenge in the implementation of information security management systems. The main measure adopted is the definition of information security policies, which most of the studies are restricted to formal aspects of their elaboration or address awareness programs as instruments for their implementation. In the present work, a new model is proposed to deal with these risks, based on the theoretical and methodological framework established by behavior analysis, in particular, the behavioral analysis of law, through the interpretation of information security management systems (ISMSs) as functionally specialized social subsystems. To assess the feasibility of this proposal, that is, the behavioral analysis of information security management systems, three studies were carried out. In Study 1, a behavioral analysis of the information security policy (ISP) of a federal public administration organization was carried out, in which the contingencies planned in the policy were identified, described and analyzed. Results showed that the enforcement of the policy is based on the application of sanctions and contributed to the identification of flaws, inconsistencies and complementary measures for a more effective and efficient control of behaviors that violate the information security requirements of the participating organization. Study 2 advanced the application of this model, through the behavioral analysis of the social norm, as a network of interlocked behavioral patterns, of the ISMS established in the participating organization. Based upon this analysis, the main behavioral nodes were identified, from which the contingencies that were in effect and that controlled relevant behavior for the ISMS were analyzed. The main finding from Study 2 was that, although foreseen in the ISP, the organization does not adopt the practice of sanctioning the conducts that violate its information security requirements. In other words, the instituted ISP hardly will exert control over its target behaviors. It is highlighted that the results of the referred study corroborated this

conclusion, as it was found that this inefficiency, in controlling the behavior of employees, led the organization to invest in complementary measures to hinder the conducts that violate its information security requirements. In the same sense, it was found that information security incidents are usually promptly handled in the technical sphere, which reduces their impacts and, consequently, makes them appear less serious to the rest of the organization, a fact that reduces the likelihood of sanctions being applied by the administrative authorities. Thus, Study 2 also stressed the possibility of alternative measures for a more efficient control of behaviors that violate the participating organization's ISP. In Study 3, we sought to obtain a more comprehensive view of the main findings of the first two studies, by applying a questionnaire to 21 information technology directors of Brazilian companies. Results corroborate the main findings of the first two studies, that is, that the enforcement of ISPs is based on the application of sanctions, that companies do not apply or rarely apply these sanctions, consequently, they invest in complementary, technical, protection mechanisms to hinder the occurrence of violations of their ISP and that, when these mechanisms are not sufficient to prevent them, information security incidents are promptly dealt with by the information technology units, reducing their aversive effect for the rest of the organization. Taken together, the three studies demonstrated the feasibility of the behavior-analytic interpretation of ISMSs and indicate a new and promising way to mitigate organizational risks.

Keywords: behavioral analysis of law, information security, information security policy, behavior, user.

Os processos de negócio das empresas dependem cada vez mais de sistemas informatizados, o que, por sua vez, requer a gestão dos riscos inerentes à adoção desses sistemas. Como consequência, as empresas têm investido cada vez mais na proteção do seu principal ativo que é a informação (Bulgurcu, Cavusoglu & Benbasat, 2010; Knapp & Ferrante, 2012). Esses investimentos vão desde a segurança física, passando pela segurança lógica, que trata do uso de soluções informatizadas, alcançando as pessoas que acessam e manipulam essas informações (Pfleeger & Pfleeger, 1997; Sêmola, 2014).

No contexto de um sistema de gestão de segurança da informação (e.g., equipamentos, *softwares* e pessoas), cada componente pode ser visto como um elo de uma corrente, sendo o fator humano (i.e., o comportamento dos usuários) comumente indicado como sendo seu elo mais fraco, ou seja, as condutas dos colaboradores são frequentemente indicadas como um dos principais pontos de vulnerabilidade dentro das organizações (e.g., Mitnick & Simon, 2002; Sasse, Brostoff & Weirich, 2001; Furnell & Thomson, 2009; Vance, Anderson, Kirwan & Eargle, 2014). Por isso, verifica-se que por mais que sejam feitos investimentos em novas tecnologias, mediante a implantação de mecanismos de proteção usuais, a vulnerabilidade inerente ao comportamento humano pode não ser tratada adequadamente (Boss & Kirsch ,2007; Bulgurcu, Cavusoglu & Benbasat, 2009; Bulgurcu et al., 2010).

De acordo com Workman, Bommer e Straub (2008), em que pese haver medidas de proteção das informações disponíveis, os colaboradores insistem em ignorá-las dando causa à ocorrência de incidentes de segurança da informação. Ainda nessa linha, Boss e Kirsch (2007) afirmam que os indivíduos ou não priorizam as questões que envolvem a segurança da informação ou não tem consciência dos riscos aos quais estão expostos. Verifica-se, portanto, que para a mitigação efetiva dos riscos organizacionais, há necessidade de uma abordagem mais

abrangente, na qual o fator humano revela-se crítico para a adequada proteção das informações organizacionais (Soomro, Shah & Ahmed, 2016; Ki-Aries & Faily, 2017).

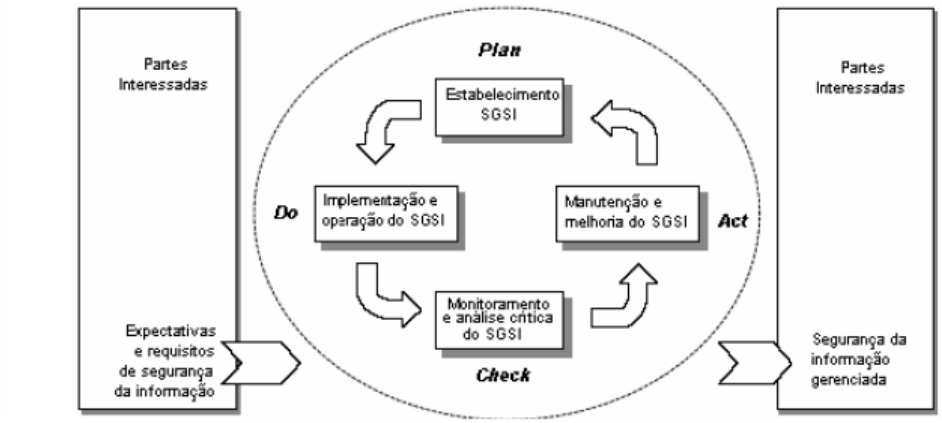
Diante desse cenário, o presente trabalho explora a interação entre a gestão da segurança da informação nas organizações e a Psicologia. Por meio da adoção do arcabouço teórico e metodológico estabelecido pela análise do comportamento, em especial a teoria analítica-comportamental do direito, investigou-se a eficácia e eficiência dos procedimentos de controle usualmente adotados pelas organizações para mitigar os riscos relacionados às condutas de seus colaboradores.

A seguir, será apresentado como as organizações tipicamente abordam as questões relacionadas ao comportamento de seus colaboradores, no contexto da gestão da segurança da informação, e discutido alguns exemplos de estudos realizados acerca do tema. Nas duas seções seguintes, será, respectivamente, abordada a Análise Comportamental do Direito, como base teórica para a consecução desse trabalho, e discutida a adaptação dessa teoria para a sua aplicação no contexto da gestão da segurança da informação nas organizações. Por fim, serão apresentados os três estudos realizados que demonstram a viabilidade da adaptação teórica proposta e os resultados alcançados.

Comportamento e a gestão da segurança da informação

Diante da necessidade de uma abordagem sistêmica e considerando as orientações contidas nas boas práticas que tratam da gestão da segurança da informação (Associação Brasileira de Normas Técnicas [ABNT], 2013a , 2013b), as organizações, tipicamente, empregam esforços na especificação e implementação de sistemas de gestão de segurança da informação (SGSIs) segundo uma abordagem por processos que contempla não só o estabelecimento e implementação de um SGSI, mas também sua operação, monitoramento, análise crítica,

manutenção e melhoria contínua, de acordo com o modelo conhecido como “Plan-Do-Check-Act”, ou PDCA, ilustrado na Figura 1.



***Plan* (planejar) (estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* (fazer) (implementar e operar o SGSI)**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* (checar) (monitorar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (agir) (manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Figura 1. Modelo PDCA aplicado aos processos de um SGSI (ABNT, 2013a).

Observa-se na Figura 1, que o modelo PDCA prevê a implementação dos SGSIs em um ciclo de melhoria contínua. Na etapa de planejamento (*Plan*) são selecionados os procedimentos de controle a serem implementados (e.g., instalação de programa *antivírus* em todos os computadores da organização). Na segunda etapa (*Do*), a implementação é realizada (i.e., a instalação dos programas *antivírus* nos computadores), em seguida, os resultados da implementação são avaliados (*Check*), ou seja, verifica-se, por exemplo, se a instalação dos programas *antivírus* reduziu a ocorrência de incidentes de segurança da informação. Por fim,

ações corretivas e preventivas são executadas com vistas à melhoria do SGSI implantado (*Act*), de acordo com a análise crítica realizada dos resultados das etapas anteriores.

Em relação aos riscos que envolvem o comportamento dos colaboradores, a definição de uma política de segurança da informação (PSI) é o principal controle recomendado nas boas práticas e é considerado um dos fatores críticos de sucesso para a implementação da segurança da informação nas organizações (ABNT, 2013b). Como pode ser observada na Figura 1, a definição da PSI está prevista na etapa de planejamento do SGSI, em seguida a política é implementada e depois passa a ser utilizada como critério de monitoramento e melhoria do SGSI. Outro ponto destacado nas boas práticas como sendo crítico para a implementação da segurança da informação nas organizações são as *ações de conscientização*, ou seja, a divulgação de informações acerca dos cuidados necessários para assegurar a segurança das informações (e.g., não compartilhar senhas, não instalar programas suspeitos, entre outros).

Observa-se, portanto que para analisar a eficiência e eficácia do tratamento da questão humana dentro de um SGSI, há a necessidade de se avaliar os normativos e regras que constituem a política de segurança da informação (e.g., regras de uso do correio eletrônico, uso da Internet, controle de acesso físico e lógico, previsão de aplicação de sanção em caso de descumprimento, dentre outros). Trata-se do principal controle para mitigar os riscos inerentes ao fator humano e uma das medidas mais importantes para se estabelecer um SGSI (ABNT, 2013b; Von Solms, 2006) por meio das quais as organizações orientam seus colaboradores quanto ao comportamento desejado em termos de segurança da informação (Lee & Lee, 2002; ABNT, 2013b; Tribunal de Contas da União, 2012).

Höne e Eloff (2002) ressaltam que a elaboração de uma PSI é um grande desafio para as organizações, pois pairam dúvidas acerca do seu conteúdo, forma de apresentação, instância de aprovação, dentre outras. Ainda acrescentam que diante dessas dificuldades, os responsáveis pela

elaboração das políticas recorrem a modelos disponíveis na Internet e exemplos de políticas de segurança da informação estabelecidas em outras organizações. Os autores ainda destacam que muitas vezes o uso da técnica de “copiar e colar” resulta em uma política de segurança da informação pouco efetiva e que não reflete a realidade da organização. Por outro lado, Imoniana (2004) concluiu, em seu estudo acerca da validação de modelos de PSIs, que as organizações não poderiam implementar plenamente políticas de segurança da informação distantes dos padrões e das boas práticas, sugerindo certa similaridade entre as PSIs uma vez observadas essas orientações.

Nessa esteira, Alshaikh, Maynard, Ahmad e Chang (2015) realizaram uma revisão da literatura acerca da definição de políticas, sob a ótica da gestão da segurança da informação, e constataram quatro principais falhas, quais sejam: ausência de visão que abarque todo ciclo de vida de uma política; falta de consistência na terminologia e semântica utilizada na confecção dos documentos; níveis distintos de detalhamento da descrição das atividades gerenciais englobadas pela política; e dificuldades em separar o gerenciamento da política de segurança de outras iniciativas como a gestão de riscos e ações de conscientização.

Já Al-Mayahi e Mansoor (2014) realizaram estudo em que propõem uma PSI para proteger os sistemas informatizados dos Emirados Árabes Unidos. Em linhas gerais, os autores sugerem na política a definição de responsabilidades, requisitos para a transmissão da informação (e.g., uso de telefone/fax), política de pessoal (e.g., processo disciplinar no caso de violação da política), padrões de senhas e requisitos técnicos (e.g., segurança no uso do correio eletrônico, banco de dados, etc.). Cabe destacar que os autores reconhecem que para que a política proposta seja efetiva, torna-se imprescindível o engajamento dos colaboradores, entretanto, verifica-se que, em relação ao comportamento dos colaboradores, a política apenas prevê a possibilidade de ações disciplinares no caso de descumprimento.

Talbot e Woodward (2009), reforçam que as PSIs são críticas para a organização e acrescentam que a segurança da informação impulsionada pela tecnologia e não pela definição de uma política revela-se uma forma inadequada para a proteção das informações organizacionais. Em seu estudo, os autores identificaram falhas na implementação da política de segurança da informação em uma organização não identificada. As falhas não se restringiram à documentação da política, mas também contemplaram fatores que comprometiam sua efetividade na organização, dentre eles a cultura de ignorar políticas no âmbito da organização e falhas na exigência do cumprimento da política. Os autores recomendaram a realização de treinamentos e *ações de conscientização* acerca da política e o tema segurança da informação, bem como a adoção de ações que assegurem o cumprimento da política, como o estabelecimento de um processo formal para o registro das ocorrências de inconformidades e a adoção de mecanismos que permitam monitorar a conformidade com a política.

Como pode ser observado, os estudos apresentados concentraram-se na forma de se definir uma PSI e seu conteúdo, também sinalizaram a necessidade de se estabelecer uma "cultura de segurança", mediante a realização de *ações de conscientização* como mecanismo para a implementação das PSIs no âmbito das organizações, ou seja, como forma de controlar o comportamento de seus colaboradores e assegurar a observação da política de segurança da informação estabelecida.

Vários estudos destacam a importância das *ações de conscientização* como mecanismo para a implantação de uma PSI nas organizações. Por exemplo, Klein e Luciano (2016) realizaram estudo para verificar a percepção dos usuários acerca das ameaças, controles e esforço para agir de forma segura. A pesquisa verificou a conformidade das práticas de segurança de usuários brasileiros em relação ao uso dos serviços de correio eletrônico (*e-mail*), mediante aplicação de questionários aos usuários que receberam alguma orientação sobre segurança da

informação da empresa onde trabalham. Os resultados demonstraram que a realização de *ações de conscientização* em segurança da informação exerce influência sobre a atitude dos colaboradores, isto é, os colaboradores tendem a relatar um comportamento seguro quando indagados. Também ratificaram que o comportamento dos colaboradores de uma organização tem um papel importante na mitigação dos riscos organizacionais e que há a necessidade de identificar os fatores que influenciam o comportamento seguro dos usuários.

Pimenta e Quaresma (2016) realizaram um estudo para verificar se os comportamentos e atitudes dos usuários representam um risco ou uma proteção em termos de segurança da informação nas organizações. Os autores fizeram um levantamento, mediante questionário disponibilizado na Internet, para um grupo de usuários predominantemente de Portugal. Em linhas gerais, os participantes respondiam a questões acerca da observância de recomendações de segurança da informação extraídas da literatura consultada pelos autores (e.g., uso de senhas fortes). Os resultados do estudo demonstraram que as atitudes (i.e., relatos) e os comportamentos declarados pelos participantes revelaram-se, em sua maioria, corretos, logo os usuários demonstraram representar mais um mecanismo de proteção do que um risco para as organizações.

Considerando a importância do fator humano para estabelecer um sistema de gestão de segurança da informação nas organizações, vários outros estudos foram realizados com o intuito de tornar as *ações de conscientização* mais efetivas (e.g., Snyman & Kruger, 2017; Tsohou, Karyda & Kokolakis, 2015; Bauer, Bernroider & Chudzikowski, 2017; Hinson, 2013). Ocorre que as conclusões desses estudos também foram baseadas nas intenções e atitudes declaradas pelos participantes, ou seja, foram baseadas nos relatos desses participantes e não nos comportamentos observados. Acerca disso, impende ressaltar que as conclusões dos estudos mencionados, baseadas na declaração do usuário, necessitam de uma confirmação empírica tendo em vista que

o comportamento declarado (dizer) pode não coincidir com o comportamento executado (Davies, Foxall & Pallsiter, 2002; Foxall, 2002; Oliveira-Castro & Foxall, 2005). Nessa esteira, cabe destacar que muito se questiona sobre as relações entre as atitudes (dizer) e os comportamentos (fazer) relativos à segurança da informação. Ou seja, há indícios na literatura de que a percepção de risco do usuário está mais associada à sua intenção em se comportar do que ao comportamento de fato. Isto é, os usuários demonstram preocupação com a questão de segurança da informação, mas não se comportam de forma a se proteger quando necessário (Acquisti & Grossklags, 2004).

Verifica-se do exposto, que as principais medidas adotadas pelas organizações, no tocante ao comportamento dos usuários, para o estabelecimento de um SGSI têm se concentrado na definição de uma política de segurança da informação e na adoção de *ações de conscientização* para a sua implantação. Ocorre que há dados que sugerem que essas ações nem sempre são suficientes para mitigar os riscos a que se propõem, pois ainda ocorrem inúmeros incidentes decorrentes de engenharia social, isto é, resultado da manipulação dos usuários para executar determinadas ações, como acessar páginas falsas, ou para a divulgação de informações confidenciais (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2012; Mann, 2012). Segundo as estatísticas do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil)[1], nos últimos cinco anos, foram reportados 3.926.637 incidentes de segurança da informação ocorridos em redes de computadores conectadas à Internet no Brasil, desses, aproximadamente 836.117 (21%) foram classificados como fraude, que são incidentes cujas causas estão usualmente ligadas ao emprego de alguma técnica de engenharia social.

[1] Fonte: https://www.cert.br/stats/incidentes/, acesso em 03/04/2019.

Acerca disso, há que se ressaltar que esses dados não surpreendem, pois a predição de comportamentos com base em narrativas ou declarações deve ser vista com cautela. O cuidado deve ser ainda maior, quando se consideram os resultados advindos de outras áreas de pesquisas, como, por exemplo, no contexto da análise comportamental do consumidor, os quais indicam que as atitudes (i.e., o que os consumidores dizem e declaram) não se mostram consistentes ou boas preditoras do comportamento de consumo observado (Foxall, 1997). As *ações de conscientização* em segurança da informação, descritas nos estudos anteriores, se inserem no contexto do que Foxall (1997) denominou de uma abordagem social-cognitiva de *marketing*. Esta abordagem parte da premissa que o comportamento (fazer) é causado por e, consequentemente, consistente com a atitude (dizer), ou seja, tacitamente se assume que ao saber a atitude de alguém, isso equivale a ser capaz de predizer as suas ações (Fazio & Zanna, 1981). Na quase totalidade das pesquisas, os autores denominam de *atitude* os relatos dos consumidores a respeito do que eles fazem ou fariam. Essa premissa tem sido questionada com base na revisão de vários estudos acerca da consistência entre atitude (relatos) e comportamento (fazer), cujos resultados indicam baixa correlação entre eles (Wicker, 1969).

Diante das limitações associadas a essa abordagem, Foxall (1997) propõe a adoção do behaviorismo para a análise do comportamento do consumidor, ou seja, a adoção de um modelo de acordo com o qual o comportamento é explicado por meio das contingências entre as respostas e as suas consequências, na presença de situações antecedentes (Skinner, 1969; Foxall, 1998; Foxall, 2017). As limitações apontadas por Foxall (1997) acerca da abordagem social-cognitiva, em especial, a premissa de haver consistência entre a atitude (dizer) e o comportamento (fazer), devem ser consideradas nos estudos mencionados anteriormente acerca da implementação de *ações de conscientização* em segurança da informação, em especial, quanto à premissa

estabelecida pelas melhores práticas de que essas ações são fatores críticos de sucesso para o estabelecimento de um SGSI.

Nesse sentido, a adoção do arcabouço teórico e metodológico da análise do comportamento para avaliar os riscos relativos ao comportamento dos indivíduos na implantação de SGSIs nas organizações parece ser promissora. Há estudos no campo da análise do comportamento cujos resultados se aproximam, funcionalmente, dos resultados apresentados nas pesquisas de comportamento dos usuários dentro do contexto de segurança da informação. Por exemplo, os estudos sobre escolhas intertemporais e probabilísticas indicam que os indivíduos tendem a dar um maior desconto no valor de determinado reforço na ocorrência de atrasos ou diminuição da sua probabilidade de ocorrência. Ou seja, mantida a magnitude dos reforços constantes, os indivíduos tendem a preferir um reforço de menor valor, mas imediato (menor atraso), ou mais provável do que um reforço de maior valor, com mais atraso ou menos provável (e.g., Rachlin, 2000; Green & Myerson, 2004). Entretanto, cabe ressaltar que no caso de consequências aversivas as escolhas tendem a se inverter. Ou seja, em um contexto de consequências reforçadoras (ganhos), a escolha tende a ser a menos arriscada (ou menos atrasada), já em um contexto de consequências aversivas (perdas) os indivíduos tendem a escolher a opção mais arriscada (ou mais atrasada).

Por exemplo, entre duas alternativas de igual valor esperado (i.e., probabilidade multiplicada pelo valor), em que a primeira alternativa consiste em 90% de chance de ganhar R$ 100,00 e a segunda alternativa consiste em 10% de chance de ganhar R$ 900,00, as pessoas tendem a escolher a primeira alternativa, isto é, a menos arriscada. No entanto, em um contexto de perda, a escolha tende a se inverter. Ou seja, entre duas alternativas de igual valor esperado, em que a primeira alternativa consiste em 90% de chance de ser multado em R$ 100,00 e a segunda alternativa consiste em 10% de chance de ser multado R$ 900,00, a maioria das pessoas

tende a escolher a segunda alternativa, isto é, a mais arriscada (cf. Aguiar & Oliveira-Castro, 2020).

Nessa linha, Acquisti (2004) adotou a teoria do desconto para explicar a resistência dos usuários em seguir as recomendações e medidas de proteção de segurança da informação. De acordo com o autor, as pessoas tendem a descontar futuros custos ou benefícios. Isto é, a pesquisa aponta que o risco percebido pelo usuário de uma falha de segurança, em certas condições, não terá efeito tão aversivo quanto ao do reforço imediato obtido com a execução do comportamento dito arriscado, considerando a probabilidade do risco concretizar (menos provável) e o tempo decorrido (atraso) para que seus efeitos sejam sentidos pelo usuário (e.g., instalar um aplicativo suspeito com a promessa de ter acesso a filmes recém-lançados ou clicar em um link de uma mensagem eletrônica de origem desconhecida com a expectativa de ter acesso a um conteúdo de interesse).

Além disso, a adoção da análise do comportamento permitirá uma análise funcional dos comportamentos dos colaboradores, das contingências planejadas nas PSIs (i.e., as regras que definem as condutas e as possíveis consequências) e das contingências vigentes na organização (i.e., aquelas que influenciam o comportamento dos colaboradores, mas não necessariamente estão previstas em normativos da organização), possibilitando, por exemplo, o estudo dos efeitos reforçadores (Skinner, 1953) de programas de incentivos para aqueles colaboradores cujo desempenho reduz riscos organizacionais e impedem a ocorrência de incidentes de segurança da informação, conforme sugerido por Mitnick e Simon (2002).

Depreende-se de todo exposto, que o estudo da implementação de SGSIs nas organizações carece de um modelo estruturado para aferir a eficácia e eficiência das ações empreendidas com vistas ao controle do comportamento de seus colaboradores, fator crucial para a mitigação dos riscos organizacionais. Nesses termos, propõe-se no presente trabalho uma nova forma de

analisar a implementação das políticas de segurança da informação nas organizações e consequentemente analisar a implementação dos SGSIs no que tange ao controle dos riscos inerentes ao comportamento dos colaboradores, considerando que a elaboração e implantação de uma PSI constituí no principal controle para tratar esses riscos. A presente proposta se afasta da avaliação típica de aspectos formais que envolvem a elaboração dos normativos ou das *ações de conscientização* deflagradas pelas organizações e foca no comportamento do indivíduo mediante a investigação das contingências estabelecidas pelas PSIs e das contingências vigentes e por vezes não programadas institucionalmente por meio de normativos formais.

Para a elaboração desta proposta, recorreu-se ao arcabouço teórico estabelecido pela análise do comportamento, em especial, a teoria proposta pela Análise Comportamental do Direto (Aguiar, 2017), apresentada a seguir, cuja adaptação permitirá o que se denomina neste trabalho de análise comportamental dos sistemas de gestão de segurança da informação, através da releitura das questões relativas às condutas dos colaboradores em um SGSI, como um subsistema social funcionalmente especializado, à semelhança do que foi proposto por Aguiar (2017) para o sistema jurídico.

Análise Comportamental do Direito

A Análise Comportamental do Direito busca esclarecer como o direito influencia o comportamento das pessoas. Trata-se de uma interpretação do direito que combina a teoria do comportamento operante com a teoria dos sistemas sociais funcionalmente especializados para o seu estudo (Aguiar, 2017).

A organização da sociedade em sistemas sociais funcionalmente especializados surge quando padrões relativamente estáveis de influência comportamental recíproca entre as organizações e seu ambiente social externo se especializam no cumprimento de determinadas funções sociais que buscam solucionar macroproblemas sociais, ou seja, aqueles que são

recorrentes e que ameaçam a sobrevivência e reprodução dos grupos sociais como um todo (Aguiar, 2017; Oliveira-Castro, Oliveira & Aguiar, 2018). São exemplos de sistemas sociais funcionais, além do sistema jurídico, os sistemas econômico, político, científico e educacional. Os sistemas sociais funcionalmente especializados são compostos pelos seguintes elementos: organizações e seus produtos, consequências condicionadas socialmente generalizadas, macroproblemas, problemas e regras sociais.

A partir da definição acima, tem-se que o primeiro componente dos sistemas sociais, as organizações, se vale do conceito de organizações de Skinner (1953), a qual se baseia no domínio por parte de um indivíduo de um reforçador, o qual controla o comportamento de outros indivíduos com vistas à geração de algum produto. Outro componente importante nos sistemas sociais funcionalmente especializados são as consequências condicionadas socialmente generalizadas (CCSG), que são resultados do pareamento com diversos reforçadores ou punidores, mediados socialmente, ou seja, por meio de outros comportamentos humanos (Aguiar, 2017). A título de exemplo, tem-se o sistema econômico, cuja CCSG é o pagamento em dinheiro. Portanto, reforça-se o comportamento do produtor pelo pagamento em dinheiro com a venda do seu produto, da mesma forma que se reforça o comportamento da mão de obra com o pagamento do salário. Observa-se que as consequências condicionadas socialmente generalizadas têm importante papel na coordenação dos padrões comportamentais entrelaçados que se estendem no tempo e no espaço (Aguiar, 2017).

Entretanto, para que uma consequência seja reforçadora ou punidora de determinado comportamento, o indivíduo deve encontrar-se no estado motivacional apropriado, no caso dos sistemas sociais funcionalmente especializados, o indivíduo deve se deparar com um problema socialmente relevante, ou macroproblema, que funciona como operação motivadora (Michael, 2000) e representa o terceiro elemento dos sistemas sociais funcionalmente especializados.

Ocorre que os macroproblemas são muito abstratos para que se tornem fatores causais eficazes (operação motivadora ou consequência) do comportamento individual. Nesse sentido, o macroproblema é desdobrado em vários problemas sociais relevantes (e.g., assassinatos, latrocínio e furto), quarto elemento característico dos sistemas sociais funcionais, cuja solução depende de comportamentos precorrentes, que em sua grande maioria consistem na enunciação de regras, último elemento dos sistemas sociais funcionalmente especializados (Aguiar, 2017).

Cabe destacar que a análise comportamental do direito adota um conceito funcional de regras, isto é, a enunciação de regras é um comportamento verbal cuja probabilidade de ocorrência depende de sua capacidade de alterar o comportamento de um indivíduo ou grupo de indivíduos (Aguiar, 2014). Por exemplo, a citação de determinada jurisprudência por um promotor solicitando uma pena máxima pode funcionar como estímulo discriminativo para o juiz, sinalizando um possível aumento na probabilidade de consequências aversivas, como o juiz ter sua decisão reformada em instâncias superiores, caso aplique outros fundamentos na dosimetria da pena. As regras ainda contêm, de forma explícita ou implícita, premissas factuais que vinculam a alteração do repertório comportamental dos destinatários da regra à obtenção do estado de coisas que favoreçam o bem-estar da sociedade.

A aplicação desse modelo-analítico comportamental para explicar o sistema jurídico parte da premissa que a função social do direito é solucionar o macroproblema do controle coercitivo de comportamentos definidos como socialmente indesejáveis, considerando essa ser a forma tipicamente encontrada no direito para controlar os comportamentos (Kelsen & Knight, 1967; Albert & Maluschke, 2013; Schauer, 2015). Isto é, o sistema jurídico é constituído, essencialmente, por proibições, ou seja, contingências sociais que buscam reduzir a ocorrência de comportamentos considerados socialmente indesejáveis (Aguiar, 2017). Esta constatação é de grande importância, pois revela que os comportamentos socialmente indesejáveis, ou seja,

aqueles comportamentos que o direito busca reduzir sua ocorrência, são mantidos por reforçadores disponíveis nos contextos em que ocorrem. Comportamentos socialmente indesejáveis são definidos pelo sistema político, por meio de aprovação de leis.

Em relação à definição das organizações e seus produtos, merece destaque que as organizações jurídicas variam de país para país, por exemplo, existem os tribunais, ministério público, escritórios de advocacia, dentre outros. Acerca disso, vale ressaltar que, em que pesem as possíveis diferenças formais e/ou funcionais dessas organizações, todas lidam com o problema de aplicação ou não das sanções jurídicas, ou, como define Aguiar (2017), o problema do *enforcement*, ou a força do direito. O autor ainda acrescenta que o conceito de *enforcement* pode ser definido pela combinação das "propensões gerais a punir dos membros das organizações jurídicas atuando enquanto tal" (Aguiar, 2017, p. 106). Nesse sentido, os diversos padrões comportamentais que constituem o *enforcement* podem ser considerados pontos de alavancagem do sistema jurídico, ou seja, pontos em um sistema, nos quais pequenas mudanças causam grandes alterações comportamentais (Meadows & Wright, 2008).

A consequência condicionada socialmente generalizada do sistema jurídico é a aplicação de sanções. Aguiar (2017) destaca que para que uma consequência funcione como sanção, esta deve ter função aversiva (i.e., diminuir a frequência de uma resposta quando produzida por ela) para os destinatários da regra jurídica e tornar-se, consistentemente, contingente ao comportamento considerado indesejado. Nesse sentido, o efeito da consequência aversiva deve ter magnitude suficiente para sobrepor o efeito reforçador do comportamento considerado indesejável, caso contrário, ela não conseguirá reduzir a probabilidade de ocorrência do comportamento objeto da regra jurídica. Da mesma forma, as sanções previstas no direito devem ser aplicadas de forma consistente nas ocorrências dos comportamentos considerados

indesejados, sob o risco da sanção perder seu caráter aversivo percebido pelos destinatários da regra jurídica, ou seja, perder seu poder de dissuasão (Skinner, 1953).

Convém ressaltar que a aplicação de sanções é resultado de um conjunto de padrões comportamentais entrelaçados, em que a probabilidade de ocorrência de um deles afeta a probabilidade de ocorrência dos demais (Aguiar, 2017). Nessa esteira, a teoria analítica-comportamental do direito define as normas jurídicas como sendo normas sociais especializadas no controle coercitivo de comportamentos considerados indesejáveis. Acerca disso, cabe esclarecer que a teoria não distingue normas sociais formais e informais, pois, de acordo com a teoria analítico-comportamental, a existência de regras enunciadas é apenas parte dos comportamentos que formam as normas sociais (Aguiar, 2013; Aguiar, 2017).

A título de exemplo, a legislação prevê punições para os casos de violência contra a mulher. Entretanto, em muitos casos em que pessoas próximas à vítima denunciam os atos abusivos, a própria vítima não os confirma, impedindo a imputação de responsabilidade e eventual aplicação de sanção. Observa-se que apesar de haver dispositivo legal que caracteriza o crime e prevê a punição (regra jurídica), a norma jurídica vigente, da vítima não confirmar as agressões perante a autoridade competente, pode desestimular a aplicação da regra. Isto é, as pessoas apesar de presenciarem os atos agressivos, não obtém reforço para o comportamento de denunciar, que em último caso seria a aplicação de sanção ao agressor. Pelo contrário, o comportamento de denunciar até pode ser punido, por exemplo, mediante ameaças do agressor em caso de novas denúncias. Observa-se que as contingências vigentes (norma jurídica) não reforçam o comportamento de denunciar previsto em lei (regra jurídica).

No entanto, há o reconhecimento que a enunciação de regras é fundamental para o surgimento de ordens sociais. Aguiar (2017) ainda destaca a importância de entender que as regras jurídicas, assim como as normas jurídicas, são padrões comportamentais estendidos no

tempo e no espaço, e que o texto tem um importante papel na descentralização desses padrões verbais, mas esclarece que se tratam de comportamentos, cujos textos servem apenas como estímulos discriminativos.

Do exposto, tem-se que a análise comportamental da norma jurídica investiga as contingências responsáveis pela ocorrência dos comportamentos jurídicos, ou seja, aqueles que visam aumentar ou diminuir a probabilidade de ocorrência do controle coercitivo dos comportamentos indesejados. Já a análise comportamental das regras jurídicas investiga as premissas que sustentam tais regras, ou seja, avaliam a capacidade de tais regras controlarem os comportamentos a que se destinam (Aguiar, 2017). Verifica-se, portanto que os resultados da análise comportamental das normas jurídicas são premissas da análise comportamental das regras jurídicas e vice-versa. Acerca disso, o autor esclarece que essa circularidade é característica das ciências que estudam os sistemas sociais funcionalmente especializados.

Para a análise comportamental das normas jurídicas Aguiar (2017) propõe dois componentes estruturais: o comportamento jurídico e a rede comportamental jurídica. Os comportamentos jurídicos são aqueles que formam a rede de padrões comportamentais entrelaçados que compõem as normas jurídicas. Aguiar (2017) esclarece que esses comportamentos, além de aumentar ou diminuir a probabilidade de aplicação das sanções, precisam ocorrer da forma requerida socialmente. Como destaca o autor, em termos funcionais, os comportamentos jurídicos podem ser punitivos relativos à ocorrência efetiva ou potencial de um comportamento indesejado, ou defensivos relativos à ocorrência efetiva ou potencial de uma sanção. Já a rede comportamental jurídica pode ser definida como um conjunto de comportamentos jurídicos punitivos e defensivos entrelaçados existentes em um determinado momento. Destaca-se que o que une essa rede de padrões comportamentais jurídicos é a

consequência condicionada socialmente generalizada do direito, qual seja, a aplicação de sanções aos comportamentos considerados socialmente indesejáveis, ou no direito, denominado delito.

A partir dessas definições, a análise comportamental das normas jurídicas, enquanto redes de comportamentos jurídicos entrelaçados, é composta por três etapas: 1) mapeamento dos nós que compõem a rede comportamental jurídica; 2) análise das contingências em cada nó da rede; e 3) conforme o caso, propor alterações nas regras jurídicas (Aguiar, 2017).

Cabe destacar que o autor define o nó em uma rede comportamental como sendo composto por pelo menos dois padrões comportamentais, sendo que o primeiro funciona como estímulo discriminativo ou operação motivadora para o segundo, e o segundo funciona como consequência reforçadora ou punitiva para o primeiro. Ainda de acordo com Aguiar (2017), verifica-se que por meio da análise comportamental das normas jurídicas é possível identificar os pontos de alavancagem dos subsistemas que a compõem e com isso planejar contingências mais eficientes para o exercício do controle pretendido pela norma. Essas contingências, no contexto da teoria analítico-comportamental do direito, são denominadas regras jurídicas e responsáveis pelo controle coercitivo dos comportamentos considerados indesejáveis. Logo, a relação causal entre o controle coercitivo de determinado comportamento e a obtenção de um estado das coisas desejável revela-se como um pressuposto fundamental para as regras jurídicas (Aguiar, 2017).

Do exposto, a teoria analítico-comportamental do direito propõe um modelo de análise comportamental das regras jurídicas em que se denomina de premissas factuais relevantes a relação causal entre a contingência coercitiva e o estado desejável das coisas, de meta social o estado desejável das coisas e de contingência jurídica a contingência coercitiva estabelecida entre o comportamento indesejável (delito) e a sanção. Este modelo pode ser traduzido na seguinte formula:

{**DADO QUE** [as seguintes *premissas factuais relevantes* são válidas segundo o estado atual da arte das várias ciências], **SE** [tal consequência mediata ou imediata da imposição da contingência jurídica abaixo é uma *meta social*, ou seja, um estado de coisas politicamente definido como favorável ao bem-estar do grupo social como um todo], **ENTÃO** [a seguinte *contingência jurídica* deve ser instituída pelo sistema jurídico (**SE** tal conduta, **ENTÃO**, tal sanção)]}.

Cabe ressaltar que as metas sociais são divididas em imediatas e mediatas. A primeira trata da redução da ocorrência do comportamento considerado indesejável que é sancionado (e.g., furto, roubo, latrocínio, feminicídio). Já a segunda, trata do estado das coisas causalmente relacionado à respectiva meta imediata (e.g., proteção a vida, da propriedade, de ir e vir). Ainda em relação às metas sociais, convém destacar que pode haver consequências indesejadas a partir do estabelecimento de uma contingência jurídica. Nesses casos, a consequência pode não ser considerada uma meta social, o que pode auxiliar na conclusão de que a contingência jurídica analisada não deva ser instituída ou aplicada como vem sendo pelas autoridades jurídicas (Aguiar, 2017).

Em relação às premissas factuais relevantes, trata-se das relações causais entre a instituição de uma contingência jurídica e o alcance da meta social pretendida. Isto é, o sistema jurídico precisa controlar os comportamentos tidos como indesejáveis e que de fato comprometem o alcance da meta social desejada. Cabe destacar que as regras jurídicas podem basear-se em premissas factuais relevantes distintas, a depender do tipo de contingência responsável pela ocorrência do comportamento a ser sancionado, como pela ligação desse comportamento à meta social mediata (Aguiar, 2017; Holanda, Oliveira-Castro & Silva, 2018).

Aguiar (2017) ainda propõe que, ao realizar a análise comportamental de qualquer regra jurídica, as premissas factuais relevantes podem ser categorizadas da seguinte forma:

probabilidade de ocorrência do comportamento a ser controlado; potencial efetividade da sanção; consequências indesejadas da aplicação da sanção; e nexo causal entre a conduta sancionada e a meta social mediata. Observa-se que as primeiras três categorias estão relacionadas com meta social imediata, já última refere-se à meta social mediata.

Por fim, o modelo analítico-comportamental do direito define a contingência jurídica como a relação contingente, definida pela regra jurídica, entre o comportamento indesejado e a consequência aversiva, ou sanção. Nesse sentido, as regras jurídicas precisam estabelecer contingências jurídicas para serem completas (Todorov, 2006). Acerca disso, Aguiar (2017) destaca que muitas vezes as leis não consignam a contingência entre o comportamento e a sanção de forma explícita e que, por outras vezes, as consequências aversivas instituídas pelas leis não são classificadas como sanções pela teoria tradicional do direito por não terem, em geral, caráter coercitivo. Ainda acrescenta que o próprio comportamento jurídico pode representar consequências aversivas e conclui que todos esses aspectos devem ser considerados na análise comportamental da regra jurídica.

Análise Comportamental do Direito aplicada ao SGSI

De todo exposto, verifica-se que para a adequada proteção das informações nas organizações, a gestão da segurança da informação se sustenta em três pilares de proteção: equipamentos, sistemas informatizados e pessoas, formando um sistema de gestão de segurança da informação. Em relação aos dois primeiros pilares, verifica-se que se trata de objetos afetos ao campo da ciência da computação, cujos mecanismos de proteção, ou controles, são usualmente implementados através do emprego de tecnologias já difundidas nesse meio, como uso de salas cofre para a proteção de equipamentos, uso de sistemas *antivírus* para a proteção contra programas maliciosos e assim por diante. No entanto, em relação às pessoas, fator crítico para o estabelecimento de um SGSI, verificou-se que o principal mecanismo de proteção é

implementado por meio da definição de uma política de segurança da informação e a realização de *ações de conscientização*.

Ocorre que os estudos identificados na literatura se concentram na definição dos elementos que devem compor uma política de segurança da informação, portanto tratam de aspectos formais da elaboração desses documentos, e na análise de *ações de conscientização* em que a premissa adotada, de que a atitude dos colaboradores (dizer) é uma boa preditora do comportamento (fazer), deve ser vista com cautela pelos motivos já expostos. Observa-se, portanto que há uma lacuna a ser preenchida que avalie o comportamento, não as atitudes (i.e., relatos), dos colaboradores e as variáveis que influenciam esses comportamentos. A presente pesquisa traz uma nova proposta para a análise do efeito dos procedimentos de controles de segurança da informação sobre o comportamento dos colaboradores, mediante a adoção do arcabouço teórico proposto pela análise do comportamento, em especial a teoria analítico-comportamental do direito. Nesse sentido, propõe-se um enquadramento das questões que envolvem o fator humano de um SGSI, ou seja, o comportamento dos colaboradores, como um subsistema social funcionalmente especializado, à semelhança do que foi proposto por Aguiar (2017) para o direito, isto é, uma interpretação analítico-comportamental dos sistemas de gestão de segurança da informação.

A viabilidade da presente proposta, isto é a análise comportamental dos sistemas de gestão da segurança da informação, pode ser aferida mediante a identificação nesses sistemas de gestão dos componentes característicos de um sistema social funcionalmente especializado, quais sejam: macroproblemas, organizações e seus produtos, consequências condicionadas socialmente generalizadas, problemas e regras sociais. Para isso, recorre-se às normas ABNT NBR ISO/IEC 27001 e 27002, que proveem um modelo para a definição, implementação, operação e

monitoramento de um SGSI e estabelecem diretrizes e princípios para a manutenção e melhoria na gestão da segurança da informação nas organizações, respectivamente.

Conforme já exposto, em relação à questão comportamental o principal controle a ser implementado para o estabelecimento de um SGSI em uma organização é a definição de uma política de segurança da informação. Verifica-se na norma ABNT NBR ISO/IEC 27002 que, dentre outros elementos, a política deve contemplar as consequências de sua violação, isto é, em termos comportamentais, a previsão de aplicação de sanções no caso de seu descumprimento. Essa previsão é corroborada na norma ABNT NBR ISO/IEC 27001 que recomenda a definição de um processo disciplinar formal para funcionários que tenham cometido uma violação da segurança da informação. Verifica-se, portanto que o estabelecimento de um SGSI implica no controle coercitivo dos comportamentos indesejáveis, isto é, em desconformidade com a sua PSI. Nesses termos, observa-se que, à luz da teoria proposta por Aguiar (2017), um SGSI lida com o macroproblema de exercer o controle coercitivo dos comportamentos que violem sua política de segurança da informação.

Em relação às organizações e seus produtos, a ABNT NBR ISO/IEC 27002 reserva o capítulo 6 para tratar da organização da segurança da informação. De acordo com a norma deve ser estabelecida uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação dentro das organizações. A norma ainda destaca que a direção deve aprovar a PSI, atribuir as funções de segurança em sua estrutura e coordenar e analisar criticamente a implementação da segurança da informação em toda organização. Observa-se que não há indicação da estrutura que deve sustentar a implantação de um SGSI, pois essa estrutura pode variar de organização para organização de acordo com o seu porte, mercado de atuação, entre outros fatores. Entretanto, há indicação na norma para que a coordenação e as responsabilidades pela segurança da informação contem com a contribuição de toda organização

(e.g., gerentes, usuários, auditores, técnicos TI, gestão de pessoas, assessoria jurídica, etc.). Verifica-se, portanto, que, em que pese não ser possível prever a estrutura organizacional de um SGSI, pois este varia de organização para organização, é possível constatar que, dentro do contexto deste trabalho, ou seja, da análise comportamental do SGSI, essas organizações e seus respectivos produtos lidarão com o macroproblema de controlar os comportamentos indesejados de seus colaboradores. A título de exemplo, a norma estabelece que "Dependendo do tamanho da organização, tais responsabilidades podem ser conduzidas por um fórum de gestão exclusivo ou por um fórum de gestão existente, a exemplo do conselho de diretores." (ABNT, 2013b, p. 10). Verifica-se que, caso ocorra um incidente de segurança em uma organização, esse incidente pode ser tratado no âmbito de um fórum, ou comitê, já em outra organização o incidente pode ser tratado pelo diretor de recursos humanos ou pelo seu Presidente. O que deve ser ressaltado é que independentemente da estrutura adotada, ela lidará com o problema de aplicar ou não uma sanção ao comportamento em análise.

Outro componente relevante nos sistemas sociais funcionalmente especializados são as consequências condicionadas socialmente generalizadas (CCSG), pois exercem um importante papel na coordenação dos padrões comportamentais entrelaçados que compõem o sistema. Nesse sentido e considerando que o macroproblema de um SGSI é o controle coercitivo dos comportamentos indesejados, a consequência condicionada socialmente generalizada dos SGSIs é a aplicação das sanções. Pois conforme já relatado, as principais normas que disciplinam a gestão da segurança da informação e o estabelecimento de SGSIs nas organizações indicam a necessidade de se definir sanções para os comportamentos que violem seus requisitos de segurança da informação.

Ocorre que o controle coercitivo dos comportamentos indesejados, ou seja, o macroproblema do SGSI, assim como ocorre com o direito, é relativamente abstrato para os

atores deste sistema. Nesse sentido, o macroproblema do SGSI deve ser desdobrado em problemas relevantes como o compartilhamento de senhas, acesso a sítios na Internet com conteúdo impróprio, instalação de programas potencialmente maliciosos, dentre outros. Por fim, tem-se que o tratamento desses problemas relevantes no âmbito de um SGSI baseia-se na definição de uma política de segurança da informação e normativos complementares que, dentre outros elementos, devem detalhar procedimentos e regras que os colaboradores devem observar (ABNT, 2013b), ou seja, as regras sociais desse sistema.

Como pode ser observado na Tabela 1, a releitura de um SGSI, no que tange ao controle dos riscos inerentes ao comportamento de seus colaboradores, se assemelha ao que foi proposto por Aguiar (2017) para o direito. Verifica-se que ambos estão calcados na definição de normativos e na previsão de sanções em caso de descumprimento, ou seja, ambos visam o controle coercitivo de comportamentos indesejáveis. Essa semelhança é de suma importância e revela a viabilidade da interpretação analítico-comportamental dos SGSIs, à luz da Análise Comportamental do Direito. Partindo da premissa de que ambos os sistemas lidam com o mesmo macroproblema e considerando a semelhança entre os demais componentes, a aplicação do modelo proposto por Aguiar (2017) nesse novo contexto se mostra não só viável, mas promissora para tratar os riscos inerentes aos comportamentos dos colaboradores no que diz respeito à segurança da informação.

Depreende-se do exposto, que a interpretação analítico-comportamental dos sistemas de gestão da segurança da informação, por meio da aplicação do modelo teórico proposto para a Análise Comportamental do Direito, aponta um novo caminho para tratar os riscos que envolvem a questão comportamental no contexto da gestão da segurança da informação nas organizações. Nesse sentido, há necessidade de aprofundar a aplicação do modelo analítico-comportamental do direito, mediante a análise das contingências planejadas em uma PSI, ou seja, a análise

comportamental das regras enunciadas nesse normativo, assim como das contingências que, de fato, estão vigentes e influenciam os comportamentos que compõem os principais nós que constituem a norma social de um sistema de gestão de segurança da informação instituído.

Tabela 1.

Quadro comparativo entre o direito e o SGSI como sistemas sociais funcionalmente especializados.

Componente	Direito	SGSI
Macroproblema	Controle coercitivo dos comportamentos considerados indesejáveis pela sociedade.	Controle coercitivo dos comportamentos que violem sua PSI.
Organização e produtos	Varia entre países.	Varia entre organizações.
CCSG	Aplicar sanção.	Aplicar sanção.
Problemas[a]	Feminicídio, assassinato, roubo, dentre outros.	Compartilhamento de senhas, acesso a sítios na Internet com conteúdo impróprio, instalação de programas potencialmente maliciosos, dentre outros.
Regras sociais	Constituição Federal, Leis, Decretos, etc.	PSI e normativos complementares.

[a] Trata-se de rol exemplificativo de comportamentos indesejáveis resultado do desdobramento do macroproblema cujas soluções, usualmente, consistem na enunciação de regras.

Em relação à análise das contingências planejadas em uma PSI, a interpretação aqui proposta revela a necessidade de uma análise funcional dos comportamentos indesejados quando da sua definição, pois as sanções previstas no normativo devem ter efeitos com magnitude maiores que os reforçadores dos comportamentos indesejados (Holanda, Oliveira-Castro & Silva, 2018). Quanto à análise da norma social do SGSI, a partir da análise da PSI e verificação da estrutura organizacional que o sustenta (e.g., comitê gestor de segurança, equipe de tratamento de incidentes de segurança da informação, gestor de segurança), será possível identificar os nós que

compõem a referida norma social e, por sua vez, os pontos de alavancagem dentro desse subsistema contribuindo para a programação de contingências mais eficientes para o controle dos comportamentos indesejados.

A consecução desses estudos poderá trazer novos dados que auxiliem as organizações na mitigação dos riscos corporativos. Seus resultados também poderão apontar para uma nova direção para o tratamento dos riscos, sob o prisma do comportamento dos colaboradores, em especial, no tocante à revisão das recomendações contidas nas boas práticas que tratam da gestão da segurança da informação. Por fim, a presente pesquisa estende a teoria proposta pela análise comportamental do direito para outra área de conhecimento, podendo contribuir para o aprimoramento da teoria mediante a sua aplicação em outro contexto.

Depreende-se do exposto, que a interpretação analítico-comportamental dos sistemas de gestão da segurança da informação, por meio da aplicação do modelo teórico proposto para a Análise Comportamental do Direito, aponta um novo caminho para tratar os riscos que envolvem a questão comportamental no contexto da gestão da segurança da informação nas organizações, permitindo aos profissionais da área a elaboração de normativos baseados em princípios da análise do comportamento, passíveis de verificações empíricas (cf. Aguiar, 2014; Oliveira-Castro, Oliveira & Aguiar, 2018).

Objetivos

Esta pesquisa tem como objetivo geral testar a viabilidade da interpretação analítico-comportamental dos sistemas de gestão de segurança da informação, por meio da identificação e descrição das contingências previstas nas políticas de segurança da informação e a verificação das contingências vigentes no comportamento dos principais atores que compõem esse sistema.

Para a consecução da presente pesquisa, foram realizados três estudos:

Estudo 1: Identificar e descrever as principais contingências planejadas em uma política de segurança da informação e em normativos complementares de uma organização, com base na teoria analítico-comportamental do direito;

Estudo 2: Analisar as contingências que, de fato, estão vigentes e influenciam os comportamentos que compõem os principais nós que constituem a norma social do sistema de gestão de segurança da informação instituído na organização, bem como coletar e analisar dados secundários acerca do grau de aplicação da política de segurança da informação;

Estudo 3: Avaliar o potencial de generalização dos resultados alcançados com as análises funcionais das contingências, planejadas e/ou vigentes, e dos comportamentos identificados nos estudos anteriores, mediante a análise complementar de duas premissas adotadas para o estabelecimento das contingências planejadas nas PSIs (i.e., a probabilidade de ocorrência da conduta indesejada e a potencial eficácia da sanção), bem como da relação de características das organizações com o modelo usualmente adotado para o estabelecimento dos SGSIs, ou seja, baseado na aplicação de sanções.

Estudo 1

Em um ambiente de negócios cada vez mais interconectado a informação torna-se um dos ativos mais importantes de qualquer organização moderna (e.g., Braga, 2000; Lira, Cândido, Araújo & Barros, 2008; Sêmola, 2014). Nessa esteira, a segurança da informação busca proteger esse importante ativo dos diversos tipos de ameaças, assegurando a continuidade do negócio, mitigando os riscos e buscando maximizar o retorno sobre os investimentos realizados, bem como ampliar as oportunidades de negócio (ABNT, 2013b).

O estabelecimento de um sistema de gestão de segurança da informação (SGSI) em uma organização visa à estruturação dos processos de segurança da informação (e.g., gestão de incidentes de segurança da informação, de riscos e de continuidade), baseada em uma abordagem

de riscos para o negócio (ABNT, 2018), em um ciclo de melhoria contínua. Isto é, um SGSI deve assegurar a seleção de procedimentos de controle de segurança da informação adequados e suficientes para proteger os ativos de informação e propiciar confiança às partes interessadas (ABNT, 2013a).

Em relação ao comportamento dos colaboradores nas organizações, o principal procedimento de controle para tratar seus riscos e fator crítico de sucesso para implementação de um SGSI é a definição de uma política de segurança da informação (Martins & Santos, 2005; ABNT, 2013b). O conteúdo de uma política de segurança da informação varia, entre as organizações, em função do seu grau de maturidade e informatização, mercado de atuação, requisitos de segurança, dentre outros aspectos. Entretanto, em linhas gerais, uma política de segurança da informação usualmente contempla a definição de segurança da informação, suas metas e escopo. Consigna o comprometimento da alta direção, especifica os procedimentos de controles de segurança da informação a serem implementados (e.g., política se senhas, requisitos de controle de acesso, regras de uso de correio eletrônico)**,** define responsabilidades e prevê as consequências de sua violação (Tribunal de Contas da União, 2012; ABNT, 2013b).

Do exposto, verifica-se que a política de segurança da informação de uma organização é uma norma de cumprimento obrigatório e visa, dentre outras coisas, controlar o comportamento de seus colaboradores no sentido de proteger as informações organizacionais e consequentemente a própria organização. Nesse sentido, constata-se sua semelhança com o direito, pois, conforme explica Aguiar (2014), as leis também são estabelecidas com a função de controlar os padrões comportamentais. Nessa esteira, e adotando a teoria proposta para a Análise Comportamental do Direito, para aferir a eficácia e eficiência de uma política de segurança da informação como instrumento para controlar o comportamento dos colaboradores, há necessidade de realizar a análise comportamental das regras que a compõe, isto é, identificar as contingências planejadas

no normativo, ou seja, as condutas, suas sanções ou, menos comum, seus reforços (Oliveira, 2016).

O presente estudo buscou identificar, descrever e analisar as contingências planejadas na política de segurança da informação estabelecida em uma organização que optou por não ser identificada. Para a sua consecução, foi aplicado o modelo proposto pela Análise Comportamental do Direito, conforme proposto por Aguiar (2017), e adaptado a presente pesquisa.

Método

Participante

O Estudo 1 foi realizado em um órgão da Administração Pública Federal, com sede em Brasília. A organização possui em torno de 3.000 (três mil) usuários (e.g., servidores ativos, terceirizados e estagiários) e possui política de segurança da informação formalmente estabelecida há mais de 10 (dez) anos.

Material

Para a consecução do primeiro estudo, houve necessidade de acessar a política de segurança da informação instituída pela organização e suas normas complementares, a documentação relativa à análise de riscos realizada pela organização que embasou a sua elaboração e o regulamento geral do órgão.

Procedimentos

De acordo com a Análise Comportamental do Direito, as regras são definidas como padrões comportamentais verbais, cuja probabilidade de ocorrência depende de sua capacidade de alterar o comportamento de seu destinatário (Aguiar, 2017). Estas regras contêm premissas factuais que vinculam a alteração do comportamento em questão ao estado desejável das coisas.

Nessa esteira, a teoria analítico-comportamental do direito propõe um modelo para análise comportamental da regra jurídica que pode ser exposto da seguinte forma:

{**DADO QUE** [as seguintes *premissas factuais relevantes* são válidas segundo o estado atual da arte das várias ciências], **SE** [tal consequência mediata ou imediata da imposição da contingência jurídica abaixo é uma *meta social*, ou seja, um estado de coisas politicamente definido como favorável ao bem-estar do grupo social como um todo], **ENTÃO** [a seguinte *contingência jurídica* deve ser instituída pelo sistema jurídico (**SE** tal conduta, **ENTÃO**, tal sanção)]}.

Isto posto, visando a análise comportamental das regras que compõem a política de segurança da informação da organização participante (i.e., análise das contingências planejadas na política de segurança da informação) o presente estudo foi dividido em cinco etapas:

1. Identificação das regras na política de segurança da informação que tratam do comportamento esperado dos colaboradores;
2. A classificação dos comportamentos identificados na primeira etapa em categorias, a partir da sua análise funcional (i.e., antecedentes e consequentes);
3. Descrição das contingências planejadas na política de segurança da informação, a partir das categorias identificadas na segunda etapa;
4. Explicitação das metas sociais relacionadas às contingências planejadas;
5. Identificação das premissas factuais relevantes considerando as quatro categorias básicas propostas pela Análise Comportamental do Direito e adaptadas no presente estudo, são elas: impacto da ocorrência da conduta para a organização; a potencial eficácia da sanção; o nexo causal entre a conduta sancionada e a meta social mediata; e as possíveis consequências indesejadas em decorrência da aplicação da sanção.

Convém ressaltar que na análise da política de segurança da informação em tela, além de seus artigos, parágrafos e incisos, também foi considerada a análise de risco que fundamentou a sua elaboração. Merece ainda destaque, que a análise realizada no presente estudo considerou a última versão da política de segurança da informação, estabelecida em maio de 2019, no entanto, ressalta-se que a organização já regulamenta a gestão de segurança da informação há mais de 10 anos, o que revela certo grau de maturidade em relação ao tema segurança da informação.

Resultados

Uma política de segurança da informação define as diretrizes para a gestão da segurança da informação como um todo, nesse sentido, uma PSI contempla definições de procedimentos (e.g., como solicitar a troca de senhas), responsabilidades (e.g., atribuições do Comitê de Segurança da Informação), conformidade com outros regulamentos, dentre outras. Entretanto, considerando o escopo dessa pesquisa, o foco de análise recaiu nas regras que versam sobre o comportamento esperado dos colaboradores, considerando que a política de segurança da informação deve preencher a lacuna entre as expectativas da organização e a forma como os colaboradores devem agir para assegurar a proteção de suas informações (Alqahtani, 2017).

A política de segurança da informação analisada no presente estudo é composta por 88 artigos, dentre os quais, 12 foram selecionados por tratarem do comportamento esperado dos colaboradores da organização. Ou seja, nessa primeira etapa o objetivo foi definir o escopo da análise a ser realizada, excluindo os dispositivos que, por exemplo, definem: conceitos aplicados na norma (e.g., “Conteúdo evasivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos, possibilitando o vazamento de informações”); procedimentos de trabalho (e.g., “A solicitação de acesso à rede de computadores deve conter nome completo, matrícula e o tipo de acesso a ser concedido”); e responsabilidades (e.g., “Caberá à unidade de TI a realização, periódica, da gestão dos riscos dos ativos de TI”).

O resultado da primeira etapa restringiu o escopo do presente estudo à análise dos seguintes itens da política de segurança da informação:

1. É proibido aos usuários compartilhar sua senha de acesso à rede de computadores.
2. O uso não apropriado do acesso à internet e à intranet será passível de apuração de responsabilidade.
3. Os serviços de correio eletrônico corporativo serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.
4. O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.
    a. Por uso não apropriado, considera-se o envio de mensagens de correio eletrônico contendo:
        i. materiais obscenos, ilegais ou antiéticos;
        ii. materiais preconceituosos ou discriminatórios;
        iii. materiais caluniosos ou difamatórios;
        iv. propagandas com objetivos comerciais;
        v. listas de endereços eletrônicos dos usuários do correio eletrônico corporativo;
        vi. vírus ou qualquer outro programa malicioso;
        vii. material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;
        viii. material protegido por leis de propriedade intelectual;
        ix. entretenimentos;

x. assuntos ofensivos;

xi. arquivos de áudio, vídeo, imagem ou texto que não sejam de interesse específico do trabalho;

xii. SPAM.

5. É responsabilidade do usuário do correio eletrônico corporativo:
    a. utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais;
    b. não permitir acesso de terceiros ao correio eletrônico por meio de sua senha.
6. Será vedada a cópia, em diretório da rede de computadores, dos seguintes tipos de arquivos:

    i. imagens, músicas e filmes de qualquer formato;

    ii. programas não homologados ou não licenciados;

    iii. programas de conteúdo prejudicial à segurança do ambiente computacional;

    iv. outros arquivos digitais cuja utilização não seja relacionada ao trabalho.

    a. Será autorizado o armazenamento de arquivos elencados no *caput*, desde que expressamente justificado.
7. Será responsabilidade do usuário da rede de computadores:
    a. utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais;
8. É vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.

9. É vedada a instalação e a utilização de programas e aplicativos de computador não homologados ou que descaracterizem os propósitos da organização ou que possam oferecer riscos à segurança dos ativos de informação ou danificar o ambiente tecnológico.
10. É vedada a conexão direta de equipamento ou dispositivo portátil particular na rede de computadores, sem a prévia verificação e autorização da equipe técnica de TI.
11. Os dispositivos portáteis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus e outros programas maliciosos ao serem conectados à rede ou a equipamento pertencente à organização.
12. Durante a execução das suas atividades profissionais, todos os usuários, seja presencialmente, seja em *home office*, devem observar as seguintes recomendações:
    a. guardar em local seguro informações sensíveis ou críticas que estejam armazenadas em papel, mídia eletrônica ou outro meio, especialmente quando o local de trabalho estiver desocupado;
    b. desligar ou hibernar os computadores ao final do expediente;
    c. bloquear os computadores com senha no caso de ausências curtas, por exemplo, para almoço, lanche e reuniões;
    d. utilizar somente equipamentos da própria organização na realização do trabalho presencial.

Em relação aos itens acima, cumpre ressaltar que a numeração dos artigos, parágrafos e incisos foi substituída, bem como o texto sofreu pequenas mudanças, sem alteração de conteúdo. Isso foi necessário para contribuir para a preservação da identidade da organização participante.

Merece ainda destaque que a política de segurança da informação instituída não prevê consequências reforçadoras para os comportamentos conformes, o normativo apenas estabelece que a sua inobservância implicará em responsabilidade administrativa na forma da lei, ou seja, consequência punitiva (i.e., sanção) caso seus requisitos de segurança da informação sejam descumpridos.

Uma vez definido o escopo da análise a ser realizada, os itens selecionados na primeira etapa foram agrupados em categorias comportamentais a partir da análise funcional de cada comportamento identificado em cada um dos itens, conforme detalhado no Apêndice A.

Da análise realizada nessa segunda etapa, os itens da política de segurança da informação da organização participante foram organizados em quatro categorias, conforme disposto na Tabela 2.

Tabela 2.

Categorias comportamentais identificadas na política de segurança da informação da organização participante.

Categoria	Descrição	Itens da PSI
Compartilhamento de senhas	Colaborador compartilhar senhas de acesso aos recursos informatizados com terceiros.	1 e 5.b
Uso inadequado dos recursos de TI	Utilização dos recursos disponibilizados com fins particulares, em atividades ilegais ou que possam comprometer a segurança das informações do Órgão.	2, 3, 4, 5.a, 6 e 7
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)	Condutas que possam comprometer a integridade do ambiente de TI, seja por intervenções físicas (e.g., uso de equipamentos que não são do órgão) ou lógicas (e.g., instalação de programas não homologados e uso de dispositivos móveis para manipulação de arquivos).	8, 9, 10 e 11
Descuidos no posto de trabalho	Ações que possam comprometer a segurança das informações organizacionais mediante acesso físico ao posto de trabalho do colaborador.	12

Passa-se então à análise comportamental das categorias identificadas em que se descrevem as contingências planejadas naquele conjunto de regras da política de segurança da informação, nos termos da contingência de quatro termos (i.e., padrão comportamental, consequência, contexto e estado motivacional), conforme proposto por Aguiar (2017). Em relação às consequências, convém destacar que esta foi dividida em reforçadora, pois, caso não houvesse reforço o comportamento não se manteria no repertório comportamental do colaborador; e em sanções, isto é, a consequência punitiva, prevista na política de segurança da informação, com vistas a reduzir a frequência de ocorrência do comportamento indesejado (Catania, 1999).

Nesses termos, observa-se na Figura 2 a descrição da contingência planejada na primeira categoria, qual seja: o compartilhamento de senhas.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Terceiros sem acesso aos recursos de TIC necessários à execução das atividades laborais.	Restrição da empresa na concessão de acessos. Possibilidade técnica de compartilhamento de senhas. Difícil monitoramento.	Compartilhar senhas.	Facilitar o trabalho da equipe e maior produtividade.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 2. Descrição da contingência planejada na primeira categoria.

Uma vez descrita à contingência, foi verificado se essa contingência contribui para o alcance da meta social do SGSI, isto é, se contribui para a proteção da informação dos diversos tipos de ameaças, assegurando a continuidade do negócio, mitigando os riscos e buscando maximizar o retorno sobre os investimentos realizados, bem como se amplia as oportunidades de negócio (ABNT, 2013b), isto é, se em última instância, protege a organização, conforme a Figura 3.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço de comodidade e produtividade obtida pelo compartilhamento de senhas.	A inobservância das disposições da PSI implicará responsabilidade administrativa na forma da lei.	Responsabilizar administrativamente em caso de violação da PSI.	Redução do compartilhamento de senhas.	Proteção da instituição de acessos não autorizados. Contribui para a responsabilização em caso de comprometimento de informações.

Figura 3. Explicitação das metas sociais relacionadas à contingência planejada para a primeira categoria.

Depreende-se da Figura 3, que sancionar o compartilhamento de senhas contribui para o alcance da meta social do SGSI, pois a redução da sua ocorrência contribui para a mitigação do risco de acessos não autorizados, preservando a confidencialidade e a integridade das informações organizacionais. Convém destacar, na Figura 3, a coluna “Autorização Legal”. De acordo com a Análise Comportamental do Direito, a análise das regras jurídicas prevê a indicação do normativo que permite sancionar o comportamento em análise. No caso desta pesquisa, por tratar-se de um único normativo, isto é, a política de segurança da informação institucional, que prevê a responsabilização administrativa no caso de sua inobservância, esta coluna será excluída das análises das próximas categorias comportamentais com vistas a tornar a apresentação dos resultados do Estudo 1 mais objetiva.

Por fim, foram identificadas as premissas factuais relevantes, isto é, as condições ou circunstâncias que se assumem como verdadeiras e que embasam a instituição da contingência em análise. Com base na adaptação da teoria analítica-comportamental do direito, essa

identificação foi feita em quatro categorias básicas considerando o impacto da ocorrência da conduta para a organização, a potencial eficácia da sanção, o nexo causal entre a conduta sancionada e a meta social mediata e as possíveis consequências indesejadas em decorrência da aplicação da sanção, conforme a Figura 4.

Depreende-se das premissas factuais relevantes identificadas, que a contingência planejada para a primeira categoria de comportamentos indesejáveis contribui para a proteção da instituição, logo justifica a sua definição. Para isso, como pode ser observado no quadro que descreve a potencial eficácia da sanção, espera-se que o efeito punidor da aplicação da sanção seja suficiente para reduzir a ocorrência do compartilhamento de senhas. Acerca disso, impende ressaltar que a política de segurança da informação, ora analisada, está calcada na aplicação de uma única sanção, que é a eventual responsabilização administrativa no caso de sua inobservância. Ou seja, nas demais categorias comportamentais analisadas, esse quadro se repete, pois em todos os casos se espera que o efeito punidor da aplicação da sanção seja suficiente para reduzir a frequência dos comportamentos indesejados pela organização. Logo, visando dar maior objetividade na apresentação dos resultados do presente estudo, este quadro foi excluído das demais análises podendo ser consultado no Apêndice A, onde encontra-se o detalhamento de todas as análises realizadas.

IMPACTO DA OCORRÊNCIA DA CONDUTA PARA A ORGANIZAÇÃO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS PARA A ORGANIZAÇÃO
ESTADO MOTIVACIONAL	CONTEXTO		
Terceiros sem acesso aos recursos de TIC necessários à execução das atividades laborais.	Restrição da organização na concessão de acessos. Possibilidade técnica do compartilhamento de senhas. Difícil monitoramento.	Compartilhar senhas.	Aumenta o risco de exposição de informações de negócio e o risco na responsabilização por eventuais danos.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhamento de senhas.	Responsabilizar administrativamente em caso de violação da PSI.	Efeito punidor da aplicação da sanção reduz a probabilidade de compartilhamento de senhas.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Reduzir a ocorrência de compartilhamento de senhas entre os colaboradores	Maior proteção dos ativos de informação da organização e consequentemente dela própria

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhamento de senhas.	Responsabilizar administrativamente em caso de violação da PSI.	Redução de produtividade e comportamento de contracontrole dos colaboradores.

Figura 4. Identificação das premissas factuais relevantes da contingência estabelecida na primeira categoria.

Ainda em relação à análise das premissas factuais relevantes da primeira categoria comportamental, há que se destacar que o reforço que mantém o comportamento do colaborador de compartilhar senhas é a facilidade em distribuir tarefas e, consequentemente, melhorar a

produtividade da equipe. Acerca disso, convém ressaltar que considerando que uma das consequências indesejadas da aplicação da sanção é o comportamento de contracontrole (Catania, 1999; Moreira & Medeiros, 2007) dos colaboradores, convém que a organização reavalie a contingência, pois há medidas alternativas que podem suprir a necessidade do colaborador (i.e., dividir tarefas) sem que este recorra ao comportamento de compartilhamento de senhas.

A segunda categoria comportamental consolidou as condutas que implicavam no uso inadequado dos recursos de tecnologia da informação disponibilizados pelo Órgão (e.g., acesso à rede social e uso dos recursos para fins particulares), a contingência planejada está descrita conforme Figura 5.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Privação de conteúdo que satisfaça necessidades pessoais (e.g., redes sociais e sítios de entretenimento). Maior esforço no uso dos recursos de TI ao separar atividades pessoais das profissionais (e.g., necessidade de usar mais de uma solução de e-mail, simultaneamente, para atender suas demandas). Se valer dos mecanismos de proteção da organização para seus interesses pessoais (e.g., cópias de segurança automáticas de arquivos pessoais).	Possibilidade técnica do uso inadequado. Difícil monitoramento. Boa infraestrutura de TI disponibilizada pela organização (e.g., espaço de armazenamento e velocidade de rede de comunicação de dados).	Usar inadequadamente recursos de TI.	Maior facilidade na utilização dos recursos de TI seja para fins profissionais ou pessoais (e.g., acesso a redes sociais, comodidade no gerenciamento de mensagens eletrônicas, cópias de segurança para arquivos pessoas, dentre outros).	O uso não apropriado dos recursos de TI é passível de apuração de responsabilidade. Ainda no caso de acesso à Internet, este pode ser bloqueado.

Figura 5. Descrição da contingência planejada para a segunda categoria.

Cabe destacar que essa categoria contempla a regra da PSI que trata do acesso inapropriado à Internet. Nessa regra, além da eventual responsabilização administrativa, também

foi prevista como sanção o bloqueio do acesso à Internet e comunicação à chefia imediata, caso seja constatada a ocorrência da conduta indesejada por meio de auditoria. Por isso, essa possibilidade foi destacada ao longo da análise realizada.

Quanto ao alcance da meta social do SGSI estabelecido, verifica-se, na Figura 6, que a sanção da categoria comportamental contribui não só para a proteção das informações, como também para a otimização do uso dos recursos de TI.

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES		IMEDIATA	MEDIATA
A eventual responsabilização administrativa e/ou o bloqueio de acesso e comunicação à chefia, nos casos de acesso à Internet, tendem a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o acesso inapropriado.	Responsabilizar administrativamente em caso de violação da PSI. Bloquear o acesso e comunicar a chefia, no caso de acesso à Internet.	Redução do uso inapropriado dos recursos de TI.	Proteção da instituição de mecanismos que possam comprometer a integridade, confidencialidade e disponibilidade de seus serviços de TI. Controle de distribuição de conteúdo potencialmente malicioso. Otimização do uso dos recursos de TI.

Figura 6. Explicitação das metas sociais relacionadas à contingência planejada para a segunda categoria.

As premissas factuais relevantes para programação da contingência na segunda categoria foram identificadas conforme a Figura 7.

IMPACTO DA OCORRÊNCIA DA CONDUTA PARA A ORGANIZAÇÃO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS PARA A ORGANIZAÇÃO
ESTADO MOTIVACIONAL	CONTEXTO	Usar inadequadamente recursos de TI.	Riscos de exposição dos ativos de informação; aumento de demanda infraestrutura de TI; facilitar a distribuição de programas maliciosos; e de responsabilização da empresa por uso de programas não licenciados.
Privação de conteúdo que satisfaça necessidades pessoais (e.g., redes sociais e sítios de entretenimento). Maior esforço no uso dos recursos de TI ao separar atividades pessoais das profissionais (e.g., necessidade de usar mais de uma solução de e-mail, simultaneamente para atender suas demandas). Se valer dos mecanismos de proteção da organização para seus interesses pessoais (e.g., cópias de segurança automáticas de arquivos pessoais).	Possibilidade técnica do uso inadequado. Difícil monitoramento. Boa infraestrutura de TI disponibilizada pela organização (e.g., espaço de armazenamento e velocidade de rede de comunicação de dados).		

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI e, no caso de acesso à Internet, seu bloqueio e comunicação à chefia imediata.	Reduzir o uso inadequado dos recursos de TI.	Maior proteção dos ativos de informação da organização, bem como da imagem da instituição e, consequentemente, dela própria. Otimização do uso dos recursos de TI.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso inadequado dos recursos de TI.	Responsabilizar administrativamente em caso de violação da PSI e, no caso de acesso à Internet, seu bloquear o acesso e comunicar a chefia imediata.	Uso de serviços de correio eletrônico externos para atividades laborais. Risco de comprometimento da confidencialidade da informação. Uso excessivo de serviços de armazenamento em nuvem para o compartilhamento de arquivos, com potencial para o vazamento de informações. Comportamento de contracontrole do colaborador e/ou do responsável pela unidade

Figura 7. Identificação das premissas factuais relevantes da segunda categoria.

Quanto às premissas factuais relevantes, convém relembrar que na análise da potencial eficácia da sanção, assim como ocorre com a eventual responsabilização administrativa, nos casos de acessos inadequados à Internet, a organização espera que o bloqueio do acesso e a comunicação à chefia imediata do colaborador tenham efeitos punitivos com magnitudes suficiente para reduzir a ocorrência desse acessos inapropriados. Acerca disso, cabe ressaltar que uma das possíveis consequências indesejadas da aplicação da sanção, identificadas na Figura 7, é o comportamento de contracontrole do responsável pela unidade de lotação do colaborador. Ou seja, é preciso avaliar se existem outras contingências vigentes que possam controlar o comportamento dos responsáveis pelas unidades da organização, reduzindo a eficácia da contingência planejada.

Ainda em relação às possíveis consequências indesejadas da aplicação da sanção, verificou-se que a contingência planejada para a segunda categoria comportamental contribui para a otimização do uso dos recursos de TI, essa é uma das metas sociais mediatas alcançada. Entretanto, da aplicação da sanção nesses casos, verificou-se a possibilidade de uso de serviços de TI externos (e.g., correio eletrônico e armazenamento de arquivos) para atividades laborais, pois o que reforça essa categoria de comportamentos é a facilidade de uso dos recursos informatizados. Constata-se, portanto a necessidade de uma análise pela organização dessas consequências e avaliar se o impacto da possível exposição das informações organizacionais, mediante uso de serviços externos de TI para o trabalho, é maior do que o uso inapropriado dos recursos de TI. Acerca disso, convém ainda ressaltar que o resultado dessa análise pode levar à adoção de medidas alternativas, como a redução do tamanho das caixas postais e de espaços de armazenamento de arquivos, com o intuito de reduzir o impacto no uso dos recursos de TI, ou ao planejamento de contingências complementares que visem reduzir o risco de exposição de informações da organização.

A terceira categoria comportamental contemplou as condutas que, de alguma forma, podem comprometer o ambiente de tecnologia da informação da organização, seja por meio de uma intervenção física (e.g., conexão de equipamento particular na rede de comunicação de dados do Órgão) ou lógica (e.g., instalação de um programa não licenciado). A contingência planejada foi descrita conforme a Figura 8.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Os recursos disponibilizados no ambiente tecnológico não atendem às necessidades particulares dos usuários. Atrasos na execução de tarefas.	Possibilidade técnica (e.g., disponibilidade de programas não homologados).	Usar recursos de informática que possam comprometer o ambiente de tecnologia da informação do Órgão (físico e/ou lógico).	Acesso à recursos indisponíveis no ambiente tecnológico da organização. Agilidade na execução da tarefa.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 8. Descrição da contingência planejada para a terceira categoria.

Em relação à explicitação das metas sociais visadas com a contingência planejada, verifica-se na Figura 9, que em relação à meta social mediata, a contingência contribui para a otimização dos recursos de TI, bem como para a preservação da imagem da organização, isto é, a imagem institucional é vista como um ativo a ser protegido. Acerca disso, cabe destacar que a credibilidade é um fator indispensável para as organizações e que a construção e manutenção de uma boa imagem, além de outros fatores, é fundamental para o estabelecimento de relações sociais ou econômicas dessas organizações com o seu público alvo (Silva, 2008; Campos & Pressler, 2018).

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o uso de recursos que não integram o ambiente tecnológico homologado pela organização.	Responsabilizar administrativamente em caso de violação da PSI.	Redução das tentativas de uso de recursos que não compõem o ambiente tecnológico da organização.	Maior proteção dos ativos de informação da organização e consequentemente dela própria. Proteção da imagem da instituição (Responsabilização da organização por uso ilegal de programas). Otimização do uso dos recursos de TI.

Figura 9. Explicitação das metas sociais relacionadas à contingência planejada para a terceira categoria.

Quanto às premissas factuais relevantes, identificadas na Figura 10, convém ressaltar que um dos impactos para a organização identificados nessa categoria comportamental é o vazamento de informações, pois uma das condutas inseridas nessa categoria é a conexão de computador particular do colaborador na rede corporativa, situação em que há o risco do computador do colaborador funcionar como uma *backdoor*[2] na rede corporativa da organização, promovendo o vazamento de informações ou mesmo a sobrecarga da infraestrutura de TI.

[2] O termo *backdoor* é comumente usado em Segurança da Informação para tratar de programas que permitem acessos não autorizados à sistemas computacionais contornando os mecanismos de proteção empregados.

IMPACTO DA OCORRÊNCIA DA CONDUTA PARA A ORGANIZAÇÃO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS PARA A ORGANIZAÇÃO
ESTADO MOTIVACIONAL	CONTEXTO	Comprometer o ambiente de tecnologia da informação do Órgão (físico e/ou lógico).	Possível aumento de demanda de infraestrutura de TI para suportar os novos programas. Custos para regularização de licenças. Risco de responsabilização por uso de programas não licenciados. Risco de uso de programas com potencial danoso para a organização. Risco de vazamento das informações organizacionais e de comprometimento da disponibilidade dos recursos de TI.
Os recursos disponibilizados no ambiente tecnológico não atendem às necessidades particulares dos usuários. Atrasos na execução de tarefas.	Possibilidade técnica.		

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Reduzir o uso de recursos de informática que possam comprometer o ambiente de tecnologia da informação do Órgão (físico e/ou lógico).	Maior proteção dos ativos de informação da organização e consequentemente dela própria. Otimização do uso dos recursos de TI. Proteção da imagem da organização.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico).	Responsabilizar administrativamente em caso de violação da PSI.	Comportamento de contracontrole dos colaboradores (e.g., instalação de programas não autorizados em equipamentos do órgão ou para contornar controles estabelecidos e uso de outras soluções de armazenamento sem a exigência de verificação).

Figura 10. Identificação das premissas factuais relevantes da terceira categoria.

Por fim, a quarta categoria comportamental recomenda uma série de cuidados aos colaboradores durante a execução de suas atividades profissionais, como guardar em local seguro informações sensíveis ou críticas que estejam armazenadas em papel, mídia eletrônica ou outro

meio, e bloquear os computadores com senha no caso de ausências. Nesses termos, a contingência planejada está descrita na Figura 11.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Omitir comportamentos requeridos na manipulação de informações sensíveis no posto de trabalho.	REFORÇO	SANÇÃO
Estímulo aversivo – procedimentos atrasam as atividades rotineiras.	Possibilidade de não realizar. Difícil monitoramento e auditoria.		Menos esforço na realização de atividades rotineiras.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 11. Descrição da contingência planejada para a quarta categoria.

Em relação à última categoria, as metas sociais relacionadas e as premissas factuais relevantes foram documentadas conforme as figuras 12 e 13, respectivamente.

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	Responsabilizar administrativamente em caso de violação da PSI.	IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao custo dos cuidados indicados.		Redução da probabilidade de descuido na manipulação de informações sensíveis no posto de trabalho.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

Figura 12. Explicitação das metas sociais relacionadas à contingência planejada para a terceira categoria.

Acerca dessa última contingência, impende ressaltar o contexto em que os comportamentos ocorrem, isto é, a dificuldade de aferir se as recomendações da política de segurança da informação estão sendo cumpridas e da realização de auditorias. Essa dificuldade certamente reduz a eficácia da contingência, logo, verifica-se que a organização deve avaliar outras medidas para assegurar o comportamento que considera adequado.

IMPACTO DA OCORRÊNCIA DA CONDUTA PARA A ORGANIZAÇÃO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS PARA A ORGANIZAÇÃO
ESTADO MOTIVACIONAL	CONTEXTO	Omitir comportamentos requeridos na manipulação de informações sensíveis no posto de trabalho.	
Estímulo aversivo – procedimentos atrasam as atividades rotineiras.	Possibilidade de não realizar. Difícil monitoramento e auditoria.		Risco de divulgação de informações sensíveis.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Reduzir a omissão de comportamentos requeridos na manipulação de informações sensíveis no posto de trabalho.	Maior proteção das informações organizacionais e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Descuidos no posto de trabalho.	Responsabilizar administrativamente em caso de violação da PSI.	Comportamento de contracontrole.

Figura 13. Identificação das premissas factuais relevantes da quarta categoria.

Discussão

O objetivo do Estudo 1 foi identificar e descrever as principais contingências planejadas na política de segurança da informação da organização participante com base na adaptação da teoria analítico-comportamental do direito (Aguiar, 2017).

Da análise da política de segurança da informação instituída pela organização, foram extraídos 12 itens que tratam do comportamento esperado dos colaboradores ou daqueles que são considerados inadequados pela organização. Esses itens foram agrupados em quatro categorias

comportamentais, a partir das análises funcionais de cada um deles. Acerca do cumprimento dessas regras, verificou-se que a política de segurança da informação prevê, ao longo do texto, que o descumprimento dos seus dispositivos implicará responsabilidade administrativa na forma da lei. Constata-se, portanto, que assim como usualmente ocorre no direito (cf. Aguiar, 2006), a política de segurança da informação estabelecida pela organização visa controlar os comportamentos dos colaboradores que considera inadequados por meio de sanções.

Acerca disso, impende ressaltar que as eventuais sanções, no caso em tela, sanções administrativas, podem ter ou não função punitiva (i.e., a consequência da sanção reduzir a frequência do comportamento inadequado). Da mesma forma, essas sanções podem ou não funcionar como estímulos aversivos condicionados, isto é, levar a novos comportamentos reforçados negativamente, mediante a redução da probabilidade da aplicação da sanção em questão (Moreira & Medeiros, 2007). Nessa esteira, destaca-se que a política de segurança da informação prevê outras duas atividades que também podem funcionar como estímulos aversivos condicionados, são elas: a previsão de registro e monitoramento da utilização de recursos tecnológicos, com vistas a detectar e evidenciar incidentes de segurança (passíveis de responsabilização); e a realização de auditorias nos ativos de TI da organização, visando avaliar a conformidade técnica com os normativos aplicáveis e a apuração de eventos que possam expor os ativos de informação da organização.

Um importante ponto na descrição das contingências planejadas na PSI é a identificação da relação dessas contingências com a meta social do sistema de gestão de segurança da informação da organização, isto é, identificar se essas contingências contribuem para a proteção das informações com vistas à assegurar a continuidade do negócio, mitigar seus riscos, maximizar o retorno sobre os investimentos realizados e ampliar as oportunidades de negócio (ABNT, 2013b). Nesses termos, verificou-se que as contingências planejadas contribuem para o

alcance da meta social do sistema de gestão de segurança da informação estabelecido, pois na medida em que buscam assegurar a integridade, confidencialidade e disponibilidade das informações da organização, bem como otimizam o uso dos recursos de TI e tratam a imagem da organização como um ativo, essas contingências visam, em última instância, a proteção da instituição, conforme discriminado na Tabela 3.

Tabela 3.

Relação das contingências planejadas por item com a meta social do sistema de gestão de segurança da informação da organização.

Meta Social do SGSI	Itens da PSI
Assegurar a continuidade do negócio	2, 3, 4, 5.a, 6, 7, 8, 9, 10 e 11
Mitigar riscos	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e 12
Maximizar o retorno sobre os investimentos	2, 3, 4, 5.a, 6, 7, 8, 9, 10 e 11
Ampliar as oportunidades de negócio	Não há

Em relação às metas sociais do SGSI, verifica-se na tabela acima que todos os itens visam mitigar os riscos e que as metas “Assegurar a continuidade do negócio” e “Maximizar o retorno sobre os investimentos” estão relacionadas (i.e., os mesmos itens da PSI contribuem para o alcance de ambas), pois na medida em que se otimiza a utilização dos recursos de TI, isto é, se racionaliza a demanda por infraestrutura de TI, contribui-se para garantir a disponibilidade dos serviços informatizados. Por exemplo, um acesso em massa a um sítio de vídeos na Internet (e.g., Youtube) pode sobrecarregar os enlaces de comunicação da organização (i.e., *links*) e indisponibilizar seu sítio corporativo na rede mundial. Nesse exemplo, a limitação do uso da rede da organização para acessar esse tipo de conteúdo contribui para a disponibilidade do *site* corporativo.

Cabe destacar, que em relação à meta “Ampliar as oportunidades de negócio” não foi identificado qualquer item na PSI que contribua para o seu alcance. Ou seja, depreende-se da análise comportamental da política de segurança da informação que o apetite ao risco da organização, isto é, o nível de risco que a organização está disposta a aceitar para implementar sua estratégia (ABNT, 2018), não é alto. Ou seja, a organização adota a estratégia de limitar o acesso aos recursos tecnológicos disponíveis (i.e., que potencialmente podem ampliar as oportunidades de negócio) ao invés de assumir riscos mais elevados. Observa-se, portanto, que a análise comportamental da política de segurança da informação nas organizações pode ser útil no sentido de verificar se há alinhamento das diretrizes de segurança da informação à estratégia da organização.

Convém ressaltar que a análise de risco realizada pela organização para a elaboração de sua política de segurança da informação contribuiu, sobremaneira, para a realização do presente estudo. Na identificação dos riscos, foram destacados o evento, causas e consequências. A partir dessas informações, foi possível identificar elementos do estado motivacional e contexto (antecedentes) da ocorrência do padrão comportamental (evento), bem como as consequências para a organização, caso o evento ocorra.

Nessa esteira, a análise comportamental da PSI revelou que estado motivacional e os reforços, que mantém os comportamentos considerados indesejados pela organização no repertório dos colaboradores, são bem similares nas quatro categorias comportamentais, conforme pode ser observado na Tabela 4.

Tabela 4.

Consolidação dos estados motivacionais e reforços para os colaboradores identificados nas contingências planejadas por categoria comportamental.

Categoria Comportamental	Estado motivacional	Reforço para o colaborador
Compartilhamento de senhas	Terceiros sem acesso aos recursos de TIC necessários à execução das atividades laborais	Facilitar o trabalho da equipe e maior produtividade
Uso inadequado dos recursos de TI	Privação de conteúdo que satisfaça necessidades pessoais (e.g., redes sociais e sítios de entretenimento) Maior esforço no uso dos recursos de TI ao separar atividades pessoais das profissionais (e.g., necessidade de usar mais de uma solução de e-mail, simultaneamente para atender suas demandas) Se valer dos mecanismos de proteção da organização para seus interesses pessoais (e.g., cópias de segurança automáticas de arquivos pessoais)	Maior facilidade na utilização dos recursos de TI seja para fins profissionais ou pessoais (e.g., acesso a redes sociais, comodidade no gerenciamento de mensagens eletrônicas, cópias de segurança para arquivos pessoas, dentre outros)
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)	Os recursos disponibilizados no ambiente tecnológico não atendem às necessidades particulares dos usuários Atrasos na execução de tarefas	Acesso à recursos indisponíveis no ambiente tecnológico da organização Agilidade na execução da tarefa
Descuidos no posto de trabalho	Estímulo aversivo – procedimentos atrasam as atividades rotineiras	Menos esforço na realização de atividades rotineiras

Da análise da Tabela 4, verifica-se que, nas quatro categorias comportamentais identificadas, é comum a necessidade de facilitar o uso dos recursos tecnológicos que estão disponíveis e, em última instância, facilitar as tarefas do dia-a-dia, sejam elas estritamente

laborais (e.g., ter acesso a um relatório da organização) ou pessoais (e.g., interagir em uma rede social). Ou seja, a adoção de medidas gerenciais alternativas, que viabilizam o uso facilitado desses recursos e, ao mesmo tempo, mantém os riscos da organização em níveis aceitáveis, pode ser mais eficiente que a contingência planejada na política de segurança da informação. A título de exemplo, verificou-se na primeira categoria comportamental (i.e., a proibição do compartilhamento de senhas) que na descrição da contingência planejada (Figura 2), o estado motivacional é a falta de acesso aos recursos de TI necessários para as atividades laborais. Observa-se que uma revisão da política de classificação das informações da organização (i.e., revisão dos acessos não concedidos considerando as atividades dos colaboradores) pode revelar-se mais eficaz que a contingência planejada na política de segurança da informação, pois atenderá à demanda do colaborador que compartilha sua senha (i.e., estado motivacional) sem incorrer na possível consequência indesejada da aplicação da sanção, que é o comportamento de contracontrole.

Os contextos em que os comportamentos ocorrem também merecem uma análise mais detalhada. Ao longo do estudo foram identificados quatro contextos: restrição na concessão de acesso; possibilidade técnica; difícil monitoramento; e a boa infraestrutura de TI disponibilizada pela organização. Conforme pode ser observado na Tabela 5, os contextos “possibilidade técnica” e “difícil monitoramento” são mais frequentes entre as categorias comportamentais.

Tabela 5.

Relação das categorias comportamentais por contexto da contingência planejada.

Contexto	Categoria Comportamental
Restrição na concessão de acesso	Compartilhamento de senhas
Possibilidade técnica	Compartilhamento de senhas
	Uso inadequado dos recursos de TI
	Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)
	Descuidos no posto de trabalho
Difícil monitoramento	Compartilhamento de senhas
	Uso inadequado dos recursos de TI
	Descuidos no posto de trabalho
Boa infraestrutura de TI disponibilizada pela organização	Uso inadequado dos recursos de TI

Acerca disso, convém resgatar que política de segurança da informação, ora analisada, busca controlar os comportamentos dos colaboradores por meio de sanções (i.e., eventual responsabilização administrativa) e prevê o registro e monitoramento da utilização de recursos tecnológicos e a realização de auditorias nos ativos de TI da organização, atividades estas que podem funcionar como estímulos aversivos condicionados e, consequentemente, também controlar o comportamento dos colaboradores. Entretanto, como pode ser observado na Tabela 5, três categorias comportamentais, das quatro identificadas, tem como contexto para a ocorrência dos comportamentos a dificuldade do monitoramento. Isto é, para os comportamentos contemplados nessas categorias, a possibilidade de monitoramento e a eventual auditoria da utilização dos recursos de TI dificilmente terão efeito aversivo como planejado na política de segurança da informação. O exemplo mais evidente dessa situação são as recomendações

contidas na quarta categoria comportamental, que visam reduzir o risco de exposição de informações sensíveis por meio de acesso ao posto de trabalho do colaborador. O contexto em que o comportamento de descuido ocorre contempla a dificuldade da organização em registrar e monitorar o cumprimento das recomendações, bem como em realizar auditorias. Verifica-se, portanto, que a sanção prevista na política de segurança da informação e as atividades de monitoramento e auditoria do comportamento dos colaboradores dificilmente terão função punitiva, logo, a organização deve avaliar medidas alternativas que consiga, de fato, controlar os comportamentos indesejados ou mitigar os riscos identificados.

Constata-se, portanto, que o modelo proposto pela Análise Comportamental do Direito pode ser utilizado para descrever as contingências planejadas nas políticas de segurança da informação e dessa forma contribuir para a identificação de falhas, incoerências ou mesmo de medidas complementares à definição dessas regras nos respectivos normativos. Entretanto, a análise comportamental de um SGSI, também exige a avaliação das contingências que de fato estão vigentes nesse sistema, inclusive àquelas não são planejadas pela organização. Nessa esteira, a partir das informações levantadas no Estudo 1, passa-se ao Estudo 2, em que serão analisadas as normas sociais, enquanto uma rede de comportamentos entrelaçados (Aguiar, 2017), que existem no sistema de gestão de segurança da informação estabelecido pela organização participante.

Estudo 2

A partir da análise comportamental da política de segurança da informação realizada no Estudo 1, foi possível identificar e descrever as contingências planejadas pela organização. Entretanto, conforme já exposto, o planejamento dessas contingências não assegura que estas estejam de fato vigentes. Estudos apontam que quando as contingências planejadas (regras) e as vigentes são compatíveis, o comportamento de observar a regra se mantém (Galizio, 1979), no

entanto, quando há divergências entre essas contingências, em alguns casos, o comportamento de observar a regra não se mantém, isto é, a contingência vigente controla o comportamento, em detrimento do comportamento de observar a regra (Paracampo & Albuquerque, 2005; Albuquerque & Silva, 2006).

No contexto de um sistema de gestão de segurança da informação (SGSI), o tratamento de eventuais violações da política de segurança da informação de uma organização deve ser feito mediante o estabelecimento de um processo de gestão de incidentes de segurança da informação. Esse processo deve indicar a forma como os incidentes devem ser reportados, os papéis a serem exercidos pelos membros da organização e descrever as possíveis formas de tratamento desses incidentes (ABNT, 2013a).

Nessa esteira, o segundo estudo buscou identificar os principais atores no processo de gestão de incidentes de segurança da informação da organização e então descrever e analisar a norma social do SGSI, enquanto uma rede de comportamentos entrelaçados (Aguiar, 2017), doravante chamada de norma de segurança da informação, no que diz respeito ao tratamento dado a esses incidentes (i.e., violações da política de segurança da informação). Nessa análise, foram identificadas as contingências vigentes nos principais nós que compõem a norma de segurança da informação da organização, bem como foram levantados dados secundários que revelaram o grau de aplicação (i.e., *enforcement*) da política de segurança da informação na organização participante.

Método

Participantes

Participaram do Estudo 2 os principais atores no processo de gestão de incidentes de segurança da informação da organização participante, são eles: os coordenadores das unidades que compõem a diretoria de tecnologia da informação (Coordenadoria de Governança,

Coordenadoria de Infraestrutura, Coordenadoria de Atendimento aos Usuários e Coordenadoria de Desenvolvimento); e o supervisor da Seção de Gestão de Segurança da Informação.

Material

Para a consecução do segundo estudo, foi consultado o regulamento geral do órgão, a política de segurança da informação e a norma que estabeleceu a sistemática para o tratamento dos incidentes de segurança da informação no âmbito da organização participante. Também foram analisados os relatórios de incidentes de segurança da informação produzidos nos últimos cinco anos, bem como as atas das reuniões do Comitê Gestor de Segurança da Informação (CGSI) da instituição. Por fim, foram utilizados dois roteiros de entrevistas, todos disponíveis no Apêndice B.

Procedimentos

A Análise Comportamental do Direito define as normas jurídicas, enquanto normas sociais desse sistema social funcionalmente especializado, como sendo composta por dois componentes: o comportamento jurídico e a rede comportamental jurídica. Os comportamentos jurídicos formam a rede de padrões comportamentais entrelaçados que compõem as normas jurídicas e visam aumentar ou diminuir a probabilidade de aplicação das sanções. Já a rede comportamental jurídica é definida como o conjunto de comportamentos jurídicos entrelaçados existentes em um determinado momento (Aguiar, 2017).

No Estudo 2, a norma social do SGSI estabelecido na organização (i.e., norma de segurança da informação) foi analisada à luz da teoria analítico-comportamental do direito, logo, foram identificados os padrões comportamentais que compõem os principais nós da referida norma de segurança da informação e as respectivas contingências vigentes analisadas.

Nesse contexto, a análise comportamental da norma de segurança da informação da organização participante (i.e., análise das contingências vigentes no SGSI) foi realizada em três etapas:

1. Mapeamento do processo de gestão de incidentes de segurança da informação instituído pela organização;
2. Identificação dos principais nós que compõem a rede comportamental da norma do SGSI;
3. Descrição e análise das contingências em cada nó.

Para o mapeamento do processo de gestão de incidentes de segurança da informação instituído na organização participante (i.e., primeira etapa), foi utilizado o programa Bizagi Modeler – versão 3.4, compatível com o padrão BPMN – *Business Process Model and Notation* (Chinosi & Trombetta, 2012), e disponível gratuitamente na Internet. Com o mapeamento do processo, foi possível identificar os colaboradores que exercem papéis-chaves na aplicação das regras contidas na política de segurança da informação, isto é, que lidam com o *enforcement* da PSI.

De acordo com a ABNT (2013b) um incidente de segurança da informação é qualquer evento, ou série de eventos, de segurança da informação, indesejados ou inesperados, que possam comprometer as operações da organização e a segurança das informações. A norma ainda esclarece que um evento de segurança da informação é uma ocorrência que indica uma possível violação da política de segurança da informação, falha de procedimentos de controle ou uma situação previamente desconhecida que seja relevante para a segurança das informações nas organizações. Quanto à gestão dos incidentes de segurança da informação, a referida norma define que é um processo que visa assegurar a gestão eficiente dos incidentes de segurança da informação no âmbito das organizações.

Nessa esteira, a organização participante da presente pesquisa estabeleceu norma específica para a gestão dos incidentes de segurança da informação, que assim definiu um incidente de segurança da informação: “Evento adverso confirmado ou em suspeição, limitado a computadores, dispositivos de rede e à informação dentro destes equipamentos ou em trânsito pela rede e que podem afetar negativamente a integridade, confidencialidade, autenticidade ou disponibilidade dos recursos de Tecnologia da Informação (TI)”. Da análise dessa norma, verificou-se a definição dos seguintes atores no processo de gestão de incidentes de segurança da informação: gestores das coordenações que compõe a diretoria de tecnologia da informação da organização (Coordenadoria de Governança, Coordenadoria de Infraestrutura, Coordenadoria de Atendimento aos Usuários e Coordenadoria de Desenvolvimento); a Seção de Gestão de Segurança da Informação; o diretor de TI; o coordenador de governança, unidade à qual a Seção de Gestão de Segurança da Informação está vinculada; a equipe de tratamentos de incidentes de segurança da informação (ETIR), que atua no processo de gestão de incidentes de segurança da informação; e o Comitê Gestor de Segurança da Informação, conforme ilustrado na Figura 14.

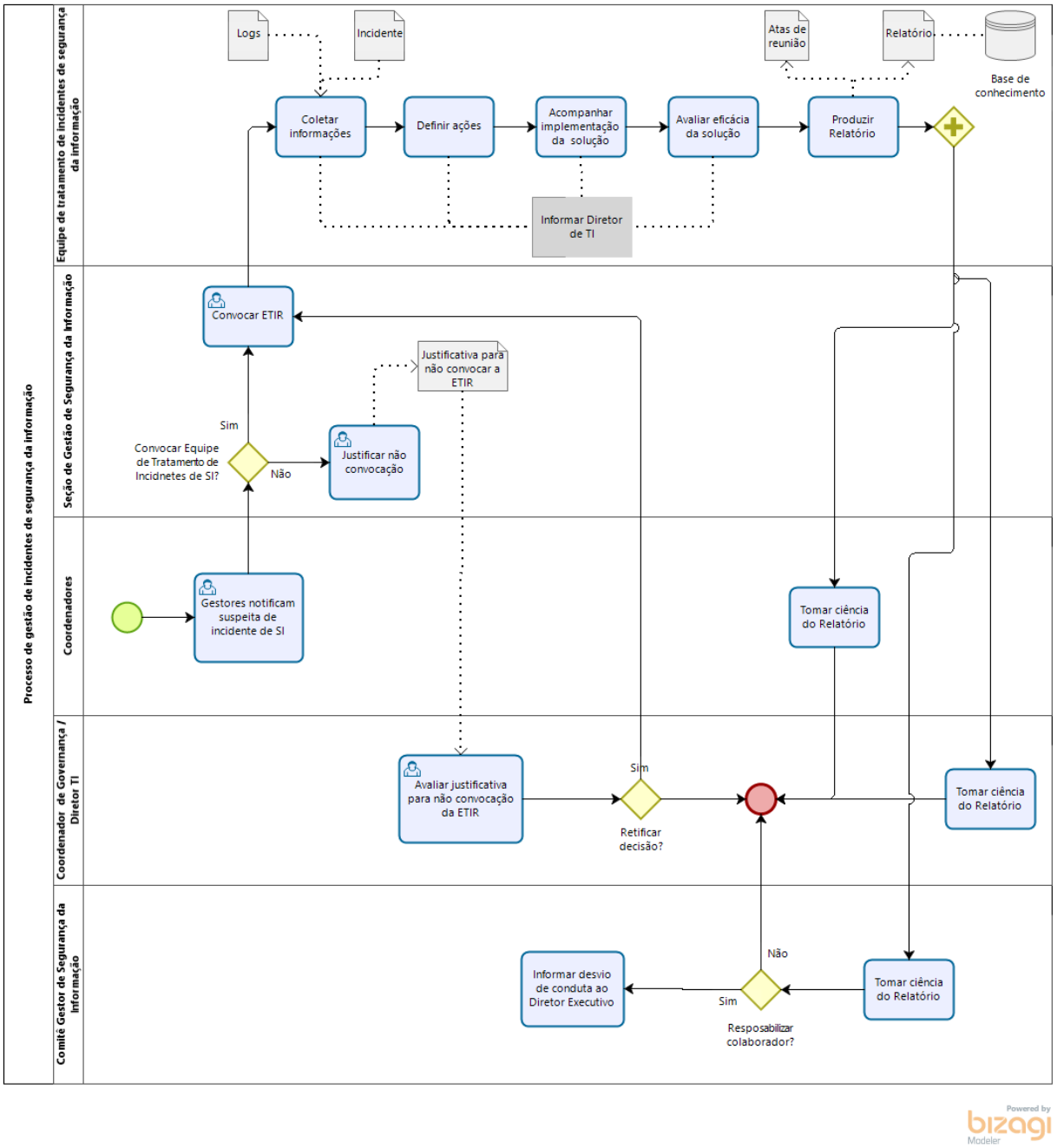


Figura 14. Processo de gestão de incidentes de segurança da informação.

Da análise do processo de gestão de incidentes de segurança da informação estabelecido pela unidade de tecnologia da informação, verificou-se que o normativo está restrito às atividades realizadas no âmbito daquela unidade. Entretanto, conforme exposto no Estudo 1, a política de

segurança da informação analisada busca controlar o comportamento dos colaboradores por meio de sanções, que, conforme já exposto, podem ter ou não função punitiva ou efeito aversivo. Sendo assim, verificou-se no caso em tela, a necessidade de ampliar o mapeamento do processo de gestão de incidentes de segurança da informação, definido pela unidade de tecnologia da informação, de forma a contemplar os outros nós da norma de segurança da informação instituída no âmbito do SGSI da organização e que atuam em unidades fora da área de tecnologia no processo de aplicação de sanções aos colaboradores. Para isso, além da norma que estabelece o processo de gestão de incidentes de segurança da informação no âmbito da unidade de tecnologia da informação, também foi necessário analisar o processo disciplinar estabelecido pela organização, já que a sanção prevista na política de segurança da informação, no caso de sua violação, é a responsabilização administrativa do colaborador.

Nesses termos, foi analisado o regulamento geral da organização participante e a legislação pertinente, a partir dos quais, conforme ilustrado na Figura 15, o processo disciplinar foi mapeado e os seguintes atores identificados: Presidente, Diretor Executivo, Diretor de Gestão de Pessoas e Comissão Disciplinar.

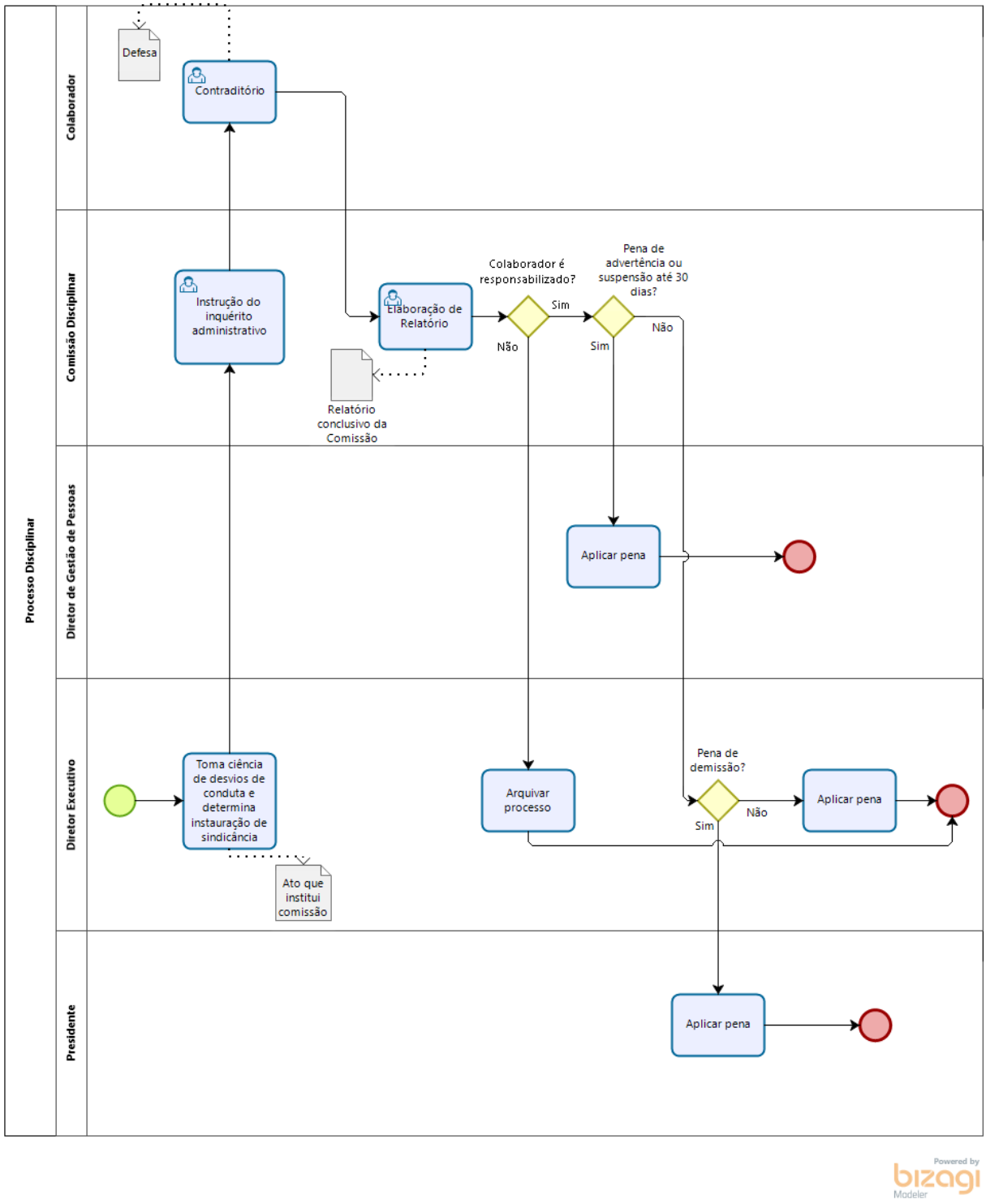


Figura 15. Processo disciplinar estabelecido pela organização.

Depreende-se dos processos acima mapeados, que cabe ao Comitê Gestor de Segurança da Informação decidir pela notificação ou não do Diretor Executivo da organização, para que este instaure o processo disciplinar para a apuração de responsabilidades e aplicação de possíveis sanções em decorrência do evento ocorrido (i.e., uma violação da política de segurança da informação). Verifica-se, portanto que este é o elo entre os dois processos, ou seja, a ligação entre o processo de gestão de incidentes de segurança da informação estabelecido pela unidade de TI e o processo disciplinar estabelecido pela organização.

Uma vez mapeado o processo de gestão de incidentes, passou-se a identificação dos principais nós da norma de segurança da informação, segunda etapa do presente estudo. Conforme exemplificado na Figura 16, o primeiro nó identificado é composto pelos seguintes padrões comportamentais: notificação da suspeita de incidente de SI; e a convocação da equipe de tratamento de incidentes de segurança da informação.

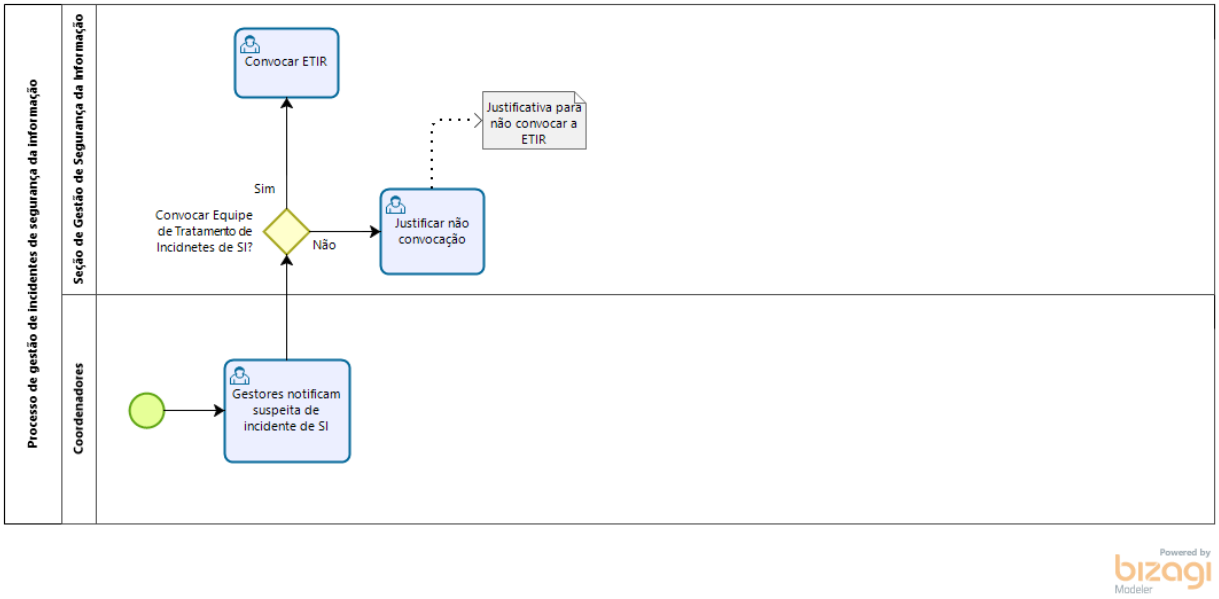


Figura 16. Exemplo de identificação do primeiro nó da norma de segurança de informação.

A última etapa foi realizada por meio de entrevistas estruturadas com esses colaboradores que exercem papéis-chaves dentro do processo de gestão de incidentes de segurança da informação, bem como mediante a análise dos relatórios de incidentes de segurança da informação produzidos nos últimos cinco anos e das atas das reuniões do Comitê Gestor de Segurança da Informação (CGSI) da instituição. Acerca disso, cumpre ressaltar que o escopo do presente estudo restringiu-se às violações e incidentes de segurança da informação ocorridos nesses últimos cinco anos, pois foi verificado junto à Seção de Gestão de Segurança da Informação que os incidentes de segurança da informação somente passaram a ter um tratamento padronizado a partir de 2014.

Nessa etapa, foram descritas e analisadas as contingências vigentes nos principais nós que formam a norma de segurança da informação da organização (i.e., norma social do SGSI). Essas análises foram realizadas nos termos da contingência de quatro termos (i.e., padrão comportamental, consequência, contexto e estado motivacional), conforme proposto na teoria analítico-comportamental do direito (Aguiar, 2017) e exemplificada na Figura 17.

NÓ	PADRÕES COMPORTAMENTAIS	CONTINGÊNCIAS	ANTECEDENTES		CONSEQUÊNCIAS
1	Registro da suspeita de incidente.	Norma institucional atribui aos coordenadores responsabilidade pela notificação de qualquer suspeita de um incidente de SI.	CONTEXTO Previsão normativa do dever de notificar qualquer suspeita de incidentes de SI.	ESTADO MOTIVACIONAL Evitar responder por eventuais danos causados pelo incidente de SI.	O registro da suspeita evita a responsabilização por omissão ou negligência (Reforço negativo para Coordenador).
	Convocação da ETIR.	Norma institucional atribui à Seção de Gestão de SI a responsabilidade pela decisão de convocar ou não da Equipe de tratamento de incidentes de SI	Previsão normativa da convocação da ETIR. Notificação da suspeita;	Evitar responder por eventuais danos causados pelo incidente de SI.	A convocação da ETIR evita a responsabilização por omissão ou negligência (Reforço negativo para Supervisor).

Figura 17. Exemplo de análise das contingências vigentes em um nó da norma de segurança de informação.

Como pode ser observado no exemplo da Figura 17, as contingências planejadas no processo de gestão de incidentes de SI estão vigentes. Ou seja, o reforçamento negativo (i.e., evitar eventuais punições por não seguir as regras planejadas) está controlando os comportamentos neste nó. Constata-se, portanto, que a terceira etapa visou identificar os reforços e consequências aversivas que contribuíram ou prejudicaram o controle dos comportamentos indesejados visados pela política de segurança da informação, isto é, que repercutiram positivamente ou negativamente no *enforcement* da PSI.

Por fim, cabe ressaltar que ao longo de todo estudo foram coletados dados secundários (e.g., tipos de incidentes, número de incidentes registrados, quantidade de processos disciplinares instaurados e sanções aplicadas) com vistas à consecução do terceiro estudo, apresentado mais adiante.

Resultados

A partir do mapeamento do processo de gestão de incidentes da organização participante, verificou-se que o *enforcement* da sua política de segurança da informação depende diretamente da atuação dos atores deste processo, em especial, dos coordenadores das unidades vinculadas à Diretoria de TI e do Supervisor da Seção de Gestão de Segurança da Informação, que são os principais responsáveis por dar início ao processo de tratamento dos incidentes (i.e., notificar suspeitas de eventuais violações da política de segurança da informação), assim como do Comitê Gestor de Segurança da Informação, responsável por deflagrar ou não o processo disciplinar.

Conforme destacado na Figura 18, verifica-se que o primeiro nó na norma de segurança da informação é composto pelos Coordenadores e a Seção de Gestão de Segurança da Informação e é formado pelos comportamentos de registrar a suspeita do incidente (Coordenadores) e a convocação ou não da ETIR (Seção de Gestão de Segurança da Informação).

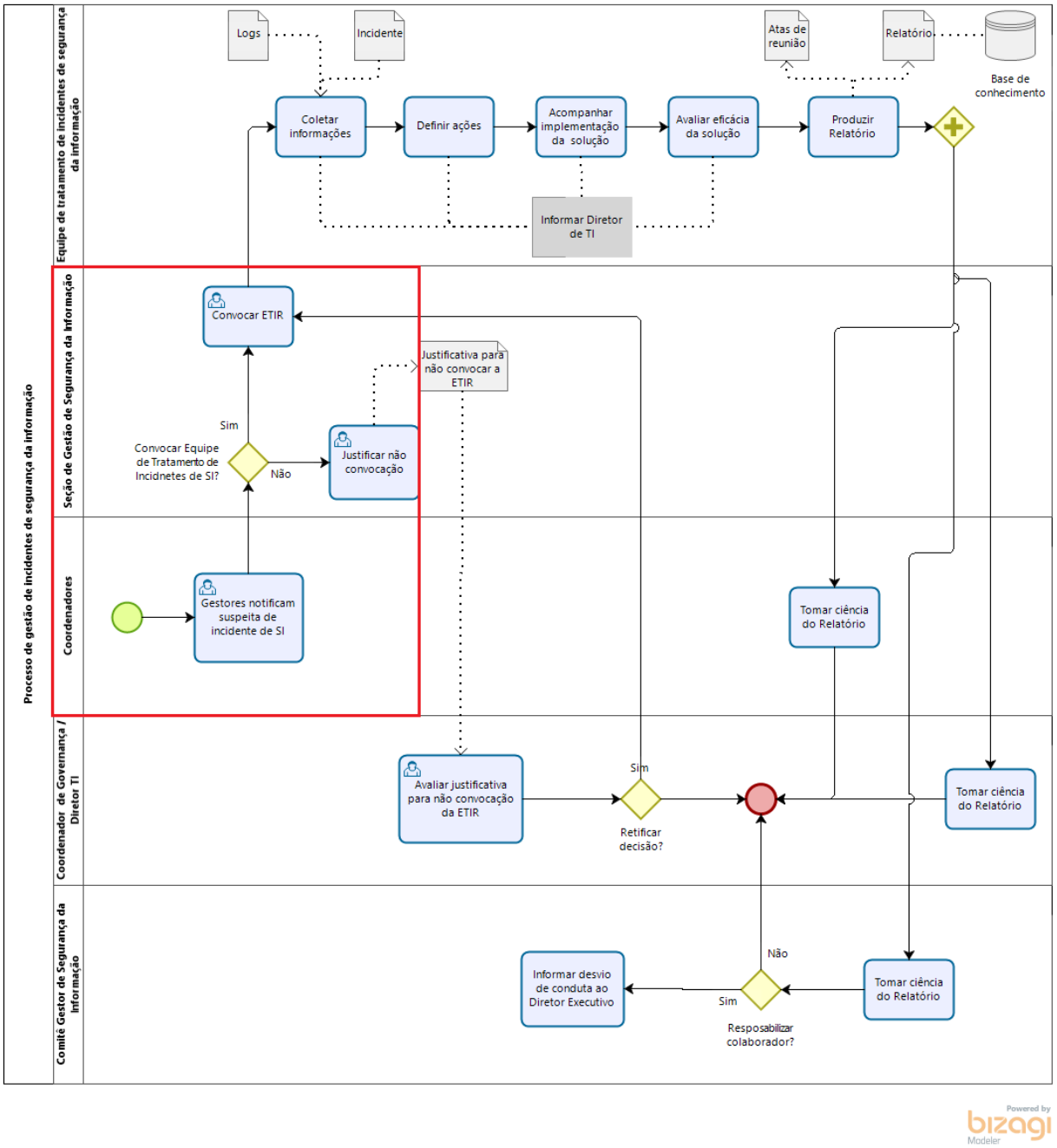


Figura 18. Primeiro nó da norma de segurança da informação.

A partir das entrevistas realizadas com os quatro Coordenadores das unidades vinculadas à Diretoria de Tecnologia da Informação, bem como com o Supervisor da Seção de Gestão de Segurança da Informação, verificou-se que os critérios que os levam a notificar a suspeita de

incidente de SI são bastante semelhantes. No caso do Coordenador de Infraestrutura, foi informado que qualquer incidente de segurança da informação em sua unidade normalmente tem grande impacto na organização. Sendo assim, todas as suspeitas são prontamente investigadas, tratadas e informadas à Seção de Gestão de Segurança da Informação quando solucionadas. O Coordenador de Atendimento aos Usuários informou que toda suspeita é notificada à Seção de Gestão de Segurança da Informação, ficando a cargo daquela Seção a decisão de tratar ou não a suspeita como um incidente de segurança da informação. Já o Coordenador de Governança informou que o principal critério adotado para a notificação das suspeitas de incidentes de segurança da informação é o possível impacto nas atividades de colaboradores estratégicos ou nos processos de negócio críticos para a organização. Por fim, o Coordenador de Desenvolvimento informou que primeiro é avaliado se a ocorrência não trata de uma falha nos sistemas, caso seja, a ocorrência é prontamente tratada. Caso contrário, a suspeita é notificada à Seção de Gestão de Segurança da Informação para análise e tratamento. Observa-se, portanto que o principal critério para a notificação das suspeitas é o possível impacto na organização, isto é, a gravidade associada ao possível incidente de segurança da informação (i.e., risco associado ao possível incidente).

Os Coordenadores também foram questionados quanto ao tratamento dado a esses incidentes e as consequências para os colaboradores que deram causa a eles. Quanto ao tratamento dos incidentes de segurança da informação, os posicionamentos dos quatro Coordenadores coincidiram no sentido de que o tratamento desses incidentes usualmente se dá na esfera técnica, isto é, o incidente é solucionado no âmbito da Diretoria de TI antes de ser informado a outras unidades da organização, como o Comitê Gestor de Segurança da Informação. Cabe ressaltar o relato do Coordenador de Infraestrutura acerca das violações das regras da PSI. De acordo com ele, a frequência dessas violações é muito baixa em decorrência da implantação

de diversas ferramentas ao longo dos últimos anos que já impedem a conduta dos usuários que violam a PSI, informação também corroborada pelo Supervisor da Seção de Gestão de Segurança da Informação.

Quanto às consequências para os usuários, os Coordenadores compartilham da visão de que como os incidentes de SI são tratados e solucionados no âmbito técnico, os demais membros da organização, como o Comitê Gestor de Segurança da Informação, apenas tomam ciência do ocorrido e das necessidades de eventuais melhorias para que o problema não volte a ocorrer. Acerca disso, cabe destacar os relatos do Coordenador de Atendimento aos Usuários e do Coordenador de Governança, que atribuem essa falta de consequência para o usuário à baixa gravidade dos incidentes de SI. Segundo eles, não há notícia da ocorrência de incidentes de segurança da informação graves, mas que caso ocorra algum, na sua visão, a direção da organização tomará providências no sentido de apurar as responsabilidades e eventualmente aplicar as sanções previstas. Convêm ainda ressaltar, que esses relatos são corroborados pelos dados levantados junto à Seção de Gestão de Segurança da Informação, em que se constatou que não houve apuração de responsabilidade em nenhum dos dez incidentes de segurança da informação tratados nos últimos cinco anos.

A partir do relato dos Coordenadores, verifica-se que estes têm conhecimento claro acerca do impacto das possíveis suspeitas de incidentes de segurança da informação na organização. Isto é, a percepção dos riscos que envolvem qualquer atividade suspeita é o principal fator que os leva à notificação da suspeita ou à própria investigação e solução do incidente de segurança da informação. Observa-se, portanto que, à luz da Análise Comportamental do Direto e considerando o escopo do presente estudo (i.e., a gestão dos incidentes de segurança da informação), o comportamento de “Registrar a suspeita dos incidentes de SI”, além de estar sob o controle de uma contingência planejada, isto é, a previsão normativa que atribui aos

coordenadores esta responsabilidade, é reforçado negativamente pela redução da probabilidade dos riscos associados àquela suspeita virem a concretizar, trazendo impacto para a organização. Constata-se, portanto que o conhecimento da suspeita e dos possíveis impactos associados a ela funciona como contexto para o comportamento de registrar a suspeita, e que a redução dos riscos para a organização é o estado motivacional dos coordenadores ao registrar a suspeita.

Em entrevista com o Supervisor da Seção de Gestão de Segurança da Informação, verificou-se que, atualmente, para todas as suspeitas de incidente de segurança da informação que eventualmente possa comprometer a confidencialidade, integridade e/ou disponibilidade das informações da organização a Equipe de Tratamento de Incidentes de Segurança da Informação é convocada. Por outro lado, o Supervisor da Seção de Gestão de Segurança da Informação, esclareceu que caso a suspeita notificada não comprometa esses requisitos (i.e., confidencialidade, integridade e disponibilidade) ou não se trate de um evento adverso, conforme definição na norma da organização (e.g., lentidão no sistema em decorrência de uma aplicação mal desenvolvida) a ETIR não é convocada. Acerca disso, o Supervisor destacou que no início da implantação do processo de gestão de incidentes de segurança da informação havia certa dificuldade para se compreender o conceito do que era um incidente de segurança da informação. Entretanto, com a consolidação do processo, essa questão foi superada. Por fim, acrescentou que não houve casos de reversão da decisão de não convocar ETIR, seja pelo Coordenador de Governança ou pelo Diretor de TI, conforme prevê o processo de gestão de incidentes de segurança da informação.

Acerca disso, impende ressaltar que como o processo prevê a justificativa para a não convocação da ETIR, essa justificativa funciona como orientação para os demais coordenadores acerca de quais elementos e critérios devem ser observados para caracterizar uma determinada ocorrência como uma suspeita a ser notificada à Seção de Gestão de Segurança da Informação.

Depreende-se dos relatos dos coordenadores e do supervisor da Seção de Gestão da Segurança da Informação que os padrões comportamentais que compõe o primeiro nó da norma de segurança da informação na organização participante podem ser descritos conforme a Figura 19.

NÓ	PADRÕES COMPORTAMENTAIS	CONTINGÊNCIAS	ANTECEDENTES		CONSEQUÊNCIAS
1	Registro da suspeita de incidente.	Norma institucional atribui aos coordenadores das unidades vinculadas à Diretoria de TI a responsabilidade pela notificação de qualquer suspeita que aponte para um incidente de SI. Dever de tratar adequadamente os riscos organizacionais.	CONTEXTO Previsão normativa do dever de notificar qualquer suspeita de incidentes de SI. Conhecimento da atividade suspeita e dos riscos associados.	ESTADO MOTIVACIONAL Reduzir a probabilidade do risco associado à suspeita vir a concretizar, causando danos para a organização. Evitar responder por eventuais danos causados pelo incidente de SI.	O registro da suspeita do incidente de segurança poderá iniciar ao tratamento do incidente de SI reduzindo os riscos para a organização. (Reforço negativo para o coordenador). Evitar responsabilização por omissão ou negligência (Reforço negativo para Coordenador).
	Convocação da ETIR.	Norma institucional atribui à Seção de Gestão de SI a responsabilidade pela análise e triagem das notificações, bem como decidir pela convocação ou não da ETIR.	Previsão normativa da convocação da ETIR. Notificação da suspeita;	Reduzir a probabilidade do risco associado a suspeita vir a concretizar, causando danos para a organização. Evitar responder por eventuais danos causados pelo incidente de SI.	A convocação da ETIR poderá mitigar os riscos associados ao incidente de SI (Reforço negativo para o supervisor). Evitar responsabilização por omissão ou negligência (Reforço negativo para Supervisor).
	Não convocação da ETIR.	Norma institucional atribui à Seção de Gestão de SI a responsabilidade pela análise e triagem das notificações, bem como decidir pela convocação ou não da ETIR.	Notificação da suspeita sem os elementos mínimos necessários que caracterizam um incidente de SI;	Evitar mobilização dos demais membros da equipe pela convocação desnecessária; Evitar que ocorrências semelhantes sejam reportadas no futuro.	Evitar a mobilização de recursos de forma desnecessária (Reforço negativo para o Supervisor). A justificativa para a não convocação serve de orientação para os demais coordenadores e contribui para o correto entendimento de quais suspeitas devem ser notificadas (Reforço positivo para o Supervisor).

Figura 19. Análise das contingências vigentes no primeiro nó da norma de segurança de informação (i.e., registrar suspeita de incidente/convocação ou não da ETIR).

Uma vez convocada a Equipe de Resposta aos Incidentes de Segurança da Informação o incidente é tratado, isto é, um conjunto de ações é tomado com vistas a solucionar o problema causado pelo incidente e, eventualmente, recuperam-se os serviços informatizados que foram afetados. Isto feito, a equipe produz um relatório final documentando todas as ações realizadas e sugestões de melhorias, em especial, as que buscam evitar que evento semelhante volte a ocorrer.

Este relatório é então submetido ao Comitê Gestor de Segurança da Informação a quem cabe decidir pela apuração ou não de responsabilidade pelo evento ocorrido. Nesses termos, identifica-se o próximo nó da norma de segurança da informação instituída pela organização. O segundo nó contempla o tratamento do incidente de SI pela ETIR e a decisão do CGSI pela não apuração de responsabilidade do colaborador que deu causa ao incidente; ou pela notificação do Diretor Executivo para que seja instaurado o procedimento de apuração de responsabilidade, conforme destacado na Figura 20.

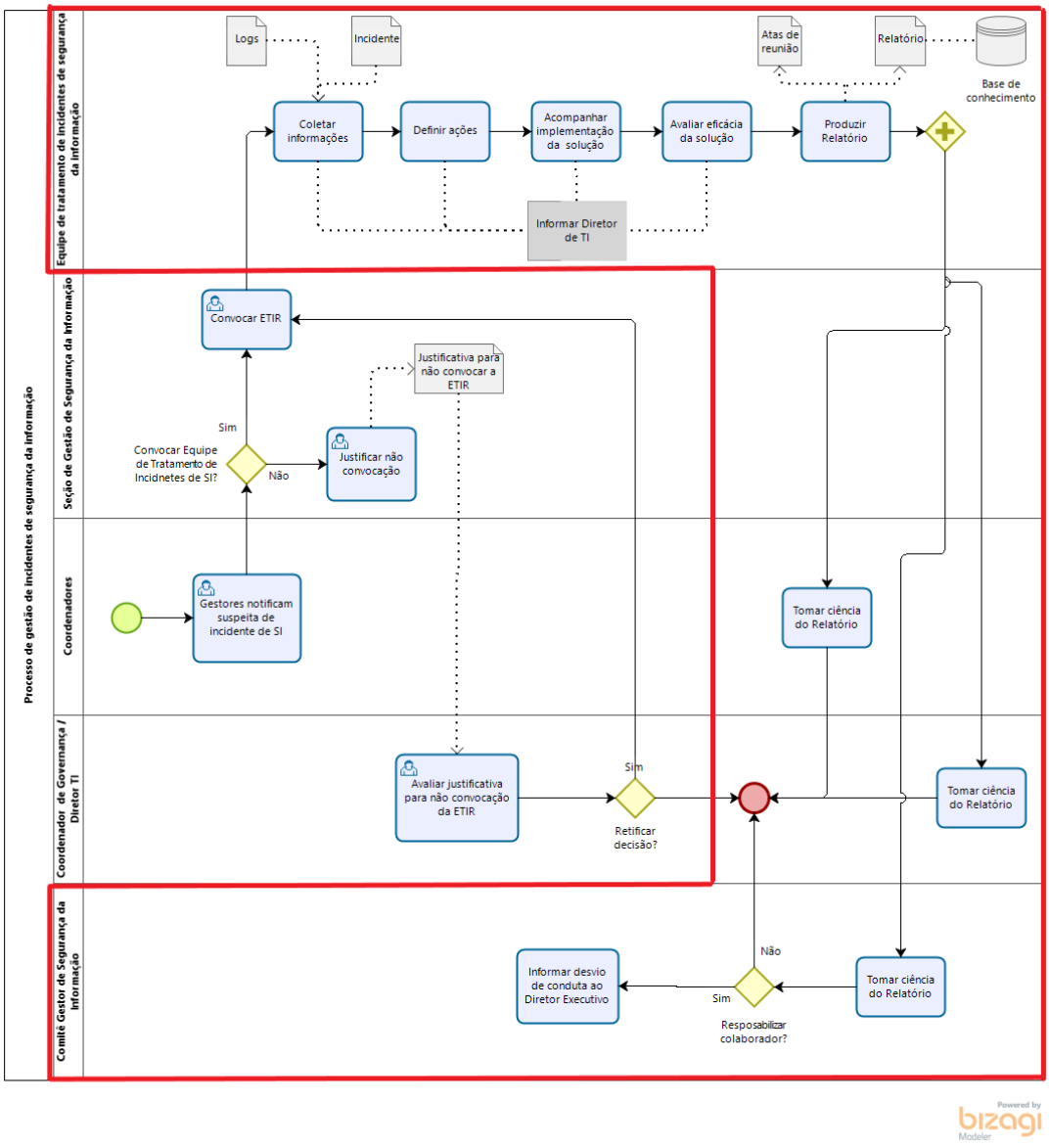


Figura 20. Segundo nó da norma de segurança da informação.

Em relação ao padrão comportamental de tratar o incidente de segurança da informação, os coordenadores e o supervisor da Seção de Gestão de Segurança da Informação informam que a solução dos incidentes de segurança da informação é prioridade no âmbito da Diretoria de TI, diante do conhecimento dos riscos associados. Também acrescentam que os incidentes de segurança da informação, em geral, são tratados com bastante eficiência e celeridade.

Novamente, observa-se nas entrevistas que os riscos associados às atividades desenvolvidas no

âmbito da unidade de tecnologia da informação estão bastante claros para os coordenadores e impulsionam as ações que buscam mitigá-los.

Quanto à decisão pela não apuração de responsabilidade, o Supervisor da Seção de Gestão de Segurança da Informação, que participa das reuniões do Comitê de Gestão de Segurança da Informação, informou que dois critérios são observados pelo Comitê para decidir ou não pela apuração de responsabilidade pela ocorrência do incidente, a reincidência e a gravidade. Em relação ao primeiro, ele informou que não há casos de reincidências nos últimos anos. Quanto à gravidade, ele esclareceu que como os incidentes, usualmente, são tratados e prontamente solucionados na esfera técnica, os impactos são bem reduzidos, logo a percepção de gravidade dos incidentes de segurança da informação pelo Comitê é baixa o que os leva apenas a tomar ciência do ocorrido e das medidas de melhorias a serem deflagradas.

Como pode ser observado, em que pese as contingências planejadas preverem a eventual sanção administrativa para o colaborador que viole os requisitos de segurança da informação da organização, de acordo com o Supervisor da Seção de Gestão de Segurança da Informação, os membros do Comitê Gestor de Segurança da Informação não percebem a violação da política de segurança da informação como sendo um risco significativo para a organização. Isto é, de acordo com o relato, o Comitê não vê necessidade de mobilizar outras áreas da organização na apuração de responsabilidade, pois os incidentes usualmente são tratados de uma forma satisfatória pela equipe técnica, mitigando os impactos dos incidentes ocorridos. Nessa esteira, verificou-se que não houve a ocorrência de apuração de responsabilidade dos colaboradores que deram causa a incidentes de segurança da informação nos últimos cinco anos no âmbito da organização participante. Sendo assim, as contingências vigentes no segundo nó (i.e., tratamento do incidente de SI/não responsabilização do colaborador) são descritas conforme a Figura 21.

NÓ	PADRÕES COMPORTAMENTAIS	CONTINGÊNCIAS	ANTECEDENTES		CONSEQUÊNCIAS
2	Tratamento do incidente de SI.	Norma institucional atribui à ETIR a responsabilidade pelo tratamento dos incidentes de SI, bem como da mitigação dos riscos de novos incidentes similares ao tratado.	CONTEXTO	ESTADO MOTIVACIONAL	Mitigação dos riscos associados ao incidente de segurança da informação (Reforço negativo para a ETIR e Coordenadores). As medidas aprimoram os mecanismos de proteção da organização evitando incidentes similares no futuro, consequentemente, aumentando a proteção da organização (Reforço positivo para ETIR e equipe técnica)
			Dever de tratar os incidentes de SI, conforme previsão normativa; Convocação da ETIR pela SSEGI; Incidente de SI triado para tratamento.	Reduzir a probabilidade do risco associado a suspeita vir a concretizar, causando danos para a organização. Evitar responder por eventuais danos causados pelo incidente de SI. Reduzir a probabilidade de ocorrência de eventos semelhantes no futuro.	
	Não apuração de responsabilidade.	Cabe ao CGSI a definição pela apuração ou não de responsabilidade pelos incidentes de segurança da informação.	Relatório do incidente de segurança da informação; Informação de baixo impacto do incidente em decorrência do pronto tratamento.	Evitar mobilização da organização para a apuração de responsabilidade por um incidente, uma vez adequadamente tratado, de baixa gravidade.	Evita desgaste com outras unidades em função da carga de trabalho para apurar responsabilidade de evento de baixa gravidade para a organização. (Reforço negativo para o Comitê).

Figura 21. Análise das contingências vigentes no segundo nó da norma de segurança de informação (i.e., tratamento do incidente de SI/não apuração de responsabilidade).

Acerca disso, impende ressaltar que apesar da constatação de que não houve casos de punição dos colaboradores que não observaram a política de segurança da informação restringir a análise deste nó, verifica-se que este é um nó crítico para o tratamento da questão comportamental no âmbito do sistema de gestão de segurança da informação da organização, isto é, trata-se de um ponto de alavancagem desse sistema (Aguiar, 2017). Nessa esteira, convém resgatar que os pontos de alavancagem de um sistema social funcionalmente especializado são

aqueles nos quais pequenas mudanças causam grandes alterações comportamentais (Meadows & Wright, 2008). Isto posto, e de acordo com a metodologia proposta para a análise da norma de segurança da informação (i.e., da norma social do SGSI estabelecido), encerra-se o presente estudo no segundo nó, pois não houve casos concretos que seguiram adiante no processo de gestão de incidentes de segurança da informação. Nesses termos, passa-se à discussão dos resultados obtidos.

Discussão

O objetivo do Estudo 2 foi descrever e analisar a norma de segurança da informação, enquanto uma rede de comportamentos entrelaçados (Aguiar, 2017), que existe no sistema de gestão de segurança da informação (SGSI) instituído na organização participante. Ou seja, o estudo visou identificar e analisar as contingências que de fato estão vigentes e controlam comportamentos relevantes para o SGSI.

A partir das entrevistas realizadas e dos dados levantados neste segundo estudo, verificou-se que a organização não tem a prática de sancionar o comportamento de seus colaboradores quando da violação de sua política de segurança da informação (PSI). Foi constatado que nos últimos cinco anos, período em que o tratamento dos incidentes de segurança da informação passou a ser padronizado, foram registrados e tratados dez incidentes de segurança da informação, para os quais não foram instaurados processos para apuração de responsabilidade, logo, também não houve a aplicação de sanções.

Acerca disso, cabe relembrar que, conforme exposto no Estudo 1, a política de segurança da informação da organização participante prevê a responsabilização administrativa como sanção em caso de sua violação, isto é, trata-se da contingência planejada para reduzir a ocorrência dos comportamentos indesejados. Nessa esteira, convém resgatar a definição de que a consequência condicionada socialmente generalizada de um SGSI, assim como do sistema jurídico, é a

aplicação de sanções. Ou seja, verifica-se no presente estudo que a consequência planejada na PSI e estabelecida pelo SGSI dificilmente terá função aversiva para os destinatários das regras da referida política, pois a consequência prevista não é consistentemente contingente aos comportamentos considerados indesejados pela organização (Aguiar, 2017).

Verifica-se, portanto, que a política de segurança da informação, como está implementada no órgão participante, dificilmente controlará os comportamentos dos colaboradores. Ou seja, trata-se de um procedimento que está conforme as boas práticas em gestão da segurança da informação (ABNT, 2013a; ABNT, 2013b), mas que, à luz da teoria analítico-comportamental, em especial a Análise Comportamental do Direito, não tem o efeito previsto nessas boas práticas e o almejado pela organização.

Entretanto, há que se ressaltar que apesar dos resultados sugerirem que a política de segurança não se revela um mecanismo eficiente para o controle dos comportamentos dos colaboradores, verificou-se que há um baixo número de registro de incidentes de segurança da informação na organização. Acerca disso, convém destacar o relato do Coordenador de Infraestrutura, corroborado pelo Supervisor da Seção de Gestão de Segurança da Informação, de que a frequência das violações da PSI é muito baixa em decorrência da implantação de diversas ferramentas ao longo dos últimos anos, que impedem que essas violações ocorram.

Verifica-se, no caso em tela, que o ambiente de trabalho da organização participante, em termos de contexto para a ocorrência dos comportamentos dos colaboradores, se aproxima do que a Análise Comportamental do Consumidor, em especial o *Behavioural Perspective Model* (BPM) proposto por Foxall (2010), denomina de um cenário fechado. De acordo com o BPM, o comportamento pode variar em um *continuum* entre aberto e fechado, no qual, quanto maior a possibilidade de escolhas, mais aberto é o cenário. Por exemplo, o consumo de alimentos durante o voo em que a única forma de pagamento é através de cartão de crédito caracteriza um cenário

fechado. Por outro lado, o mesmo consumo em uma praça de alimentação com uma oferta diversificada de produtos e de formas de pagamento caracteriza um cenário aberto (Britto, Oliveira-Castro, Holanda & dos Santos, 2018).

Nessa esteira, os colaboradores ao utilizarem os recursos de TI dentro da organização se deparam com um cenário fechado, em que há poucas possibilidades de escolha. A título de exemplo, o acesso à Internet. As únicas opções disponíveis para o colaborador são aquelas categorias de *sites* que não são bloqueadas pela organização. Ou seja, se as redes sociais estão bloqueadas, o colaborador pode tentar acessá-las, mas sempre sem sucesso. Na medida em que isso se repete, o comportamento de tentar acessar as redes sociais é enfraquecido e diminui a frequência. Convém ressaltar que mesmo a tentativa de acesso, por ser frustrada, não caracteriza um incidente de segurança da informação, daí o baixo número de incidentes registrados e tratados pela organização. Observa-se que a diminuição da frequência do comportamento indesejado pela organização não se deve à contingência planejada na política de segurança da informação (i.e., sanção administrativa no caso de sua violação), mas à implementação de mecanismos que impedem essas condutas, isto é, reduzem as opções, portanto fecham o cenário.

Observa-se que a ineficiência da política de segurança da informação instituída pela organização participante, enquanto mecanismo para controlar o comportamento dos colaboradores, leva a organização a investir em medidas alternativas para inibir as condutas indesejadas. No exemplo do acesso à Internet, verifica-se que houve a necessidade de implementar ferramentas que controlam esse acesso, isto é, houve a necessidade de fechar o cenário. Verifica-se que essa ineficiência implica em custos para a organização. Além disso, verificou-se que, mensalmente, em torno de quinhentas mil tentativas de acesso à Internet são bloqueados e foram registradas por mês, aproximadamente, cem requisições solicitando a liberação de acesso à *sites* na Internet que foram atendidas, por tratar de acessos legítimos e

necessários às atividades laborais. Constata-se, portanto, que a ineficiência da PSI, além de elevar os custos para a organização, pode também implicar em um aumento no volume de demandas para a unidade de TI.

Conclui-se, portanto, que o modelo proposto pela Análise Comportamental do Direito além de ser aplicável para a descrição e análise das contingências planejadas nas políticas de segurança da informação, conforme exposto no Estudo 1, também pode ser utilizado para a descrição e análise das contingências vigentes em um SGSI e, dessa forma, contribuir para a identificação de falhas e proposição de medidas alternativas e/ou complementares com vistas à, de fato, controlar os comportamentos indesejados dos colaboradores. A título de exemplo, destaca-se os relatos acerca da avaliação da gravidade das condutas que violam a política de segurança da informação. Ao impor uma única forma de sanção para os comportamentos indesejados, a organização acaba por tolerar condutas consideradas menos graves, mas que trazem riscos para organização, elevam custos e comprometem o objetivo do SGSI. Nesses termos, a organização participante deve avaliar uma gradação de sanções, como envio de notificações, alertas às chefias, bloqueios temporários de acesso e, eventualmente, a responsabilização do colaborador. Essa gradação de sanções, conforme a "gravidade" da conduta, sendo consistentemente contingentes às condutas que violam a PSI, muito provavelmente terá o efeito punitivo almejado pela organização.

Cabe ainda ressaltar, que por meio da aplicação do método aqui proposto, foi possível identificar os principais nós que constituem a norma de segurança da informação (i.e., a norma social do SGSI) e os respectivos pontos de alavancagem. A partir da análise das contingências vigentes nesses nós, verificou-se a necessidade de intervir no SGSI, pois, conforme exposto, a consequência planejada para os comportamentos indesejáveis (i.e., a responsabilização administrativa do colaborador) não está, de fato, vigente, o que sugere não ser suficiente para

controlar o comportamento dos colaboradores e consequentemente mitigar os riscos na organização.

Estudo 3

A partir da análise comportamental do sistema de gestão de segurança da informação estabelecido na organização participante dos estudos 1 e 2, foi possível identificar e descrever as contingências planejadas pela organização em sua PSI, explicitar as metas sociais relacionadas a essas contingências e identificar e analisar as premissas factuais relevantes que as embasaram (Estudo 1). No Estudo 2, foi descrita e analisada a norma de segurança da informação (i.e., a norma social do SGSI, enquanto uma rede de comportamentos entrelaçados) em que os principais atores no processo de gestão de incidentes de segurança da informação da organização foram identificados, assim como foram identificadas as contingências vigentes nos principais nós que compõem a referida norma de segurança da informação e, por fim, levantados dados secundários que revelaram o grau de aplicação (i.e., *enforcement*) da política de segurança da informação.

No primeiro estudo, o principal achado foi que o *enforcement* da política de segurança da informação instituída está calcado na aplicação de sanções às condutas que não observarem seus requisitos de segurança da informação (i.e., a responsabilização administrativa na forma da lei), ou seja, a sua punição. Entretanto, no segundo estudo, verificou-se que apesar da organização prever a aplicação de sanções no caso de descumprimento de sua PSI, a organização participante não adota essa prática, mas investe em outros mecanismos que impedem a ocorrência dessas violações e, nos casos em que as tentativas são bem sucedidas, estas são tratadas prontamente pela unidade de tecnologia da informação fazendo com que a consequência prevista no normativo (i.e., responsabilização administrativa) não se torne consistentemente contingente à ocorrência do comportamento indesejado.

Acerca disso, convém relembrar que a elaboração de uma PSI é um grande desafio para as organizações que, além de usualmente observarem as boas práticas (Imoniana, 2004), muitas vezes recorrem a modelos disponíveis na Internet e a exemplos de políticas de segurança da informação estabelecidas em outras organizações (Höne & Eloff, 2002), o que sugere certa semelhança entre elas. Nessa esteira, o terceiro estudo buscou complementar a análise dos principais resultados dos estudos anteriores e aferir o potencial para a generalização em outras organizações. Ou seja, buscou-se obter uma visão mais ampla acerca dos principais resultados obtidos com a análise comportamental do SGSI estabelecido na organização participante nos dois estudos anteriores.

Sendo assim, no Estudo 3, buscou-se complementar a análise de dois importantes aspectos de duas premissas factuais relevantes que sustentam as contingências planejadas para as categorias comportamentais identificadas no Estudo 1, quais sejam: a probabilidade de ocorrência da conduta indesejada e a potencial eficácia da sanção, por meio da avaliação da probabilidade de aplicação da sanção em decorrência da violação da política de segurança da informação. Conforme explicam Aguiar e Oliveira-Castro (2020), a primeira premissa estabelece que a ocorrência da conduta a ser sancionada deve ser muito provável, visto que a aplicação de sanções tem um custo social que somente se justifica quando o comportamento ocorre acima do nível tolerado. Por sua vez, a segunda premissa estabelece que a eficácia de uma regra jurídica (i.e., no contexto deste trabalho, das regras definidas na política de segurança da informação) depende da aplicação da sanção prevista, ou seja, presume-se que a aplicação da sanção ocorre com frequência suficiente para tornar a sanção eficaz.

Convém ressaltar, que no primeiro estudo a avaliação da probabilidade de ocorrência da conduta indesejada teve como critério a análise de risco que fundamentou a elaboração da

política de segurança da informação da organização participante. Ou seja, se a análise de risco apontou que a conduta representa um nível de risco suficiente que exige seu tratamento, a probabilidade de ocorrência da conduta foi considerada suficiente para se planejar a contingência na PSI. Entretanto, o risco de um evento é calculado a partir de dois parâmetros, a probabilidade de ocorrência e seu impacto para a organização. Nesse sentido, o presente estudo buscou complementar a análise realizada no Estudo 1 acerca dessa premissa prevista na teoria analítico-comportamental do direito. Já em relação à potencial eficácia da sanção, o Estudo 1 avaliou a eficácia da sanção em termos da magnitude dos seus efeitos, isto é, se são suficientes para sobrepor os efeitos reforçadores que mantém a conduta indesejada no repertório comportamental de seus colaboradores. Nessa esteira, buscou-se no presente estudo obter uma visão mais abrangente acerca da eficácia desse modelo sancionatório adotado pela maioria das empresas na implementação de seus sistemas de gestão de segurança da informação, por meio da análise da probabilidade de aplicação das sanções previstas na PSI.

Por fim, o terceiro estudo investigou possíveis relações entre as características das empresas, como seu porte e maturidade em gestão da segurança da informação, e a adoção da prática de sancionar os comportamentos que violem seus requisitos de segurança da informação.

Método

Participantes

Participaram do presente estudo 21 diretores de tecnologia da informação de empresas, públicas e privadas, no Brasil, que possuem política de segurança da informação formalmente estabelecida. Os participantes foram recrutados entre pessoas conhecidas do autor e atuaram de forma voluntária, conforme será detalhado nos Procedimentos do presente estudo.

Material

Para a consecução do terceiro estudo, foi utilizada a ferramenta Google Forms para a elaboração, envio e consolidação das respostas do questionário aplicado aos diretores de tecnologia da informação, disponível no Apêndice C.

O questionário é composto de quatro seções. A primeira destinou-se a identificação, por endereço de correio eletrônico, do respondente e a obtenção da concordância com o Termo de Consentimento Livre e Esclarecido. Convém destacar, que a solicitação do endereço de correio eletrônico corporativo do respondente teve o único propósito de auxiliar na categorização dos participantes entre instituições públicas ou empresas privadas (e.g., joão@abcd.gov.br e pedro@acme.com.br) e no acompanhamento das respostas.

A segunda seção buscou coletar dados da organização acerca do seu porte e da sua maturidade em gestão da segurança da informação, como o tempo em que há uma política de segurança da informação formalizada, se existe o registro e monitoramento das atividades dos usuários e informações sobre o processo de tratamento de incidentes de segurança da informação.

A terceira seção visou levantar informações acerca da aplicação da política de segurança da informação no âmbito da organização, isto é, seu *enforcement* (Aguiar, 2017). Ou seja, buscou-se identificar as possíveis consequências previstas nas PSIs (i.e., aversivas ou não), frequência de padrões comportamentais indesejados (e.g., compartilhamento de senhas), se as sanções previstas são aplicadas de forma consistente na ocorrência de condutas que violem seus requisitos de segurança da informação e se houve a necessidade de “fechar o cenário” dos colaboradores, no termos abordados no Estudo 2.

Por fim, a última seção foi de agradecimento e permitiu ao respondente solicitar o envio dos resultados consolidados do estudo.

Procedimentos

Inicialmente, o questionário foi enviado eletronicamente para cinco diretores de tecnologia da informação para os quais foi feito o convite para, além de participar da pesquisa, analisar criticamente o questionário e enviar suas considerações/sugestões de melhorias ou correções.

Após essa etapa de validação inicial do instrumento de coleta de dados, em que não houve qualquer sugestão de melhoria ou correções, o questionário foi enviado eletronicamente para aproximadamente 100 diretores de tecnologia da informação de empresas brasileiras de todas as regiões do país e o período de coleta dos dados foi de quatro semanas.

Convém ressaltar que, considerando que a gestão da segurança da informação é um tema sensível e que as empresas não estão predispostas a fornecer qualquer tipo de informação (Kotulic & Clark, 2004), o critério adotado para a seleção da amostra de participantes foi não probabilístico, isto é, foram convidados para colaborar com a pesquisa diretores de tecnologia da informação os quais o autor tinha algum contato.

Resultados

Participaram da pesquisa 21 diretores de tecnologia da informação de instituições, predominantemente, da administração pública federal. Ao todo, foram representadas 17 instituições públicas (81%), uma empresa privada e três empresas em que não foi possível identificar seu segmento. Em termos de porte, 76% das empresas representadas declararam ter mais de 500 usuários internos, como pode ser observado na Tabela 6.

Tabela 6.

Distribuição das empresas participantes por número de usuários internos.

Número de usuários internos de TI	Quantidade	Percentual
Menos de 500 usuários internos	5	24%
Entre 500 e 1000 usuários internos	2	9%
Acima de 1000 usuários internos	14	67%

Quanto à maturidade em gestão da segurança da informação, verificou-se que 62% das empresas possui política de segurança da informação há mais de cinco anos (Tabela 7) e que 70% (i.e., 14 empresas) tem processo de tratamento de incidentes de segurança da informação definido.

Tabela 7.

Tempo de política de segurança da informação formalizada.

Tempo de PSI formalizada	Quantidade	Percentual
Menos de 5 anos	8	38%
Entre 5 e 10 anos	9	43%
Acima de 10 anos	4	19%

Quanto à gestão da segurança da informação nessas empresas, verificou-se no Estudo 1, que uma das atividades que pode ter efeito aversivo para os colaboradores, no sentido de reduzir a frequência da ocorrência de condutas que não observam a PSI, é o monitoramento de suas atividades. Sendo assim, foi indagado se a empresa adota essa prática com vistas a identificar eventuais violações de sua PSI. Como pode ser observado na Tabela 8, a maioria dos participantes informaram que a empresa adota essa prática (91%), sendo que 62% declararam que a prática está prevista na própria política de segurança da informação.

Tabela 8.

Adoção da prática de registrar e monitorar as atividades dos usuários internos.

Adota a prática de monitoramento das atividades dos usuários	Quantidade	Percentual
Não adota	2	9%
Existe o registro e monitoramento das atividades dos usuários internos	6	29%
Existe o registro e monitoramento das atividades dos usuários internos e a prática está prevista na PSI	13	62%

Ainda em relação ao registro e monitoramento das atividades dos usuários, foi solicitado ao participante quantificar em um escala quanto a forma como a prática é realizada, isto é, se é de forma mais reativa, como em atividades de auditoria, ou se de forma proativa, em que por meio do monitoramento se dá início ao tratamento das violações dos requisitos de segurança da informação da empresa. Conforme pode ser observado na Figura 22, apenas três participantes declararam que a prática de registro e monitoramento das atividades dos usuários internos é feita de forma proativa (i.e., grau de concordância 4 e 5), ou seja, buscando se antecipar a ocorrência de eventuais incidentes de segurança da informação.

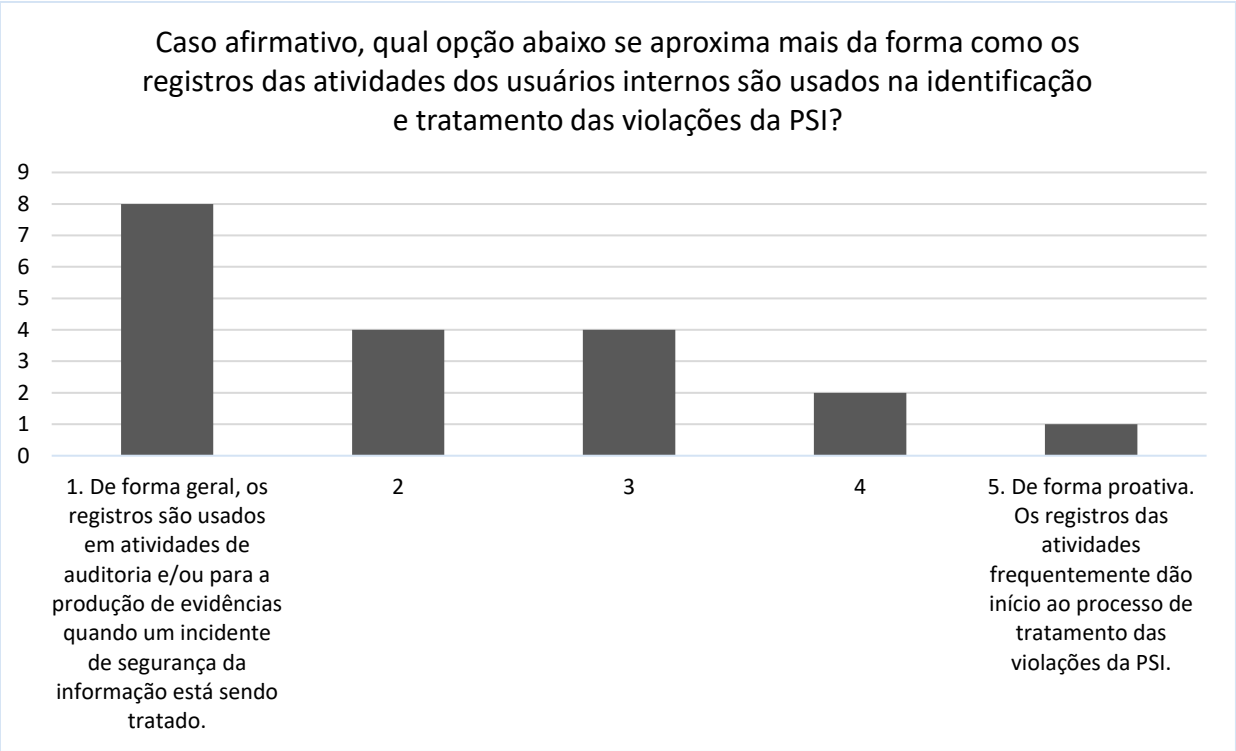


Figura 22. Forma como os registros das atividades dos usuários internos são usados na identificação e tratamento das violações da PSI.

Acerca disso, convém ressaltar que 86% participantes declararam que trataram até 20 violações da sua política de segurança da informação nos últimos cinco anos, conforme a Tabela 9.

Tabela 9.

Número de violações da política de segurança da informação tratadas nos últimos cinco anos.

Número de violações da PSI tratadas	Quantidade	Percentual
Nenhuma	4	19%
Até 20 violações	14	67%
Entre 21 e 50 violações	3	14%
Acima de 50 violações	0	0%

Em relação aos comportamentos que são considerados indesejados pelas organizações, convém resgatar a classificação feita no Estudo 1, em que as condutas analisadas foram classificadas em quatro categorias de padrões comportamentais, são elas: Compartilhamento de senhas; Uso inadequado dos recursos de TI; Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico); e Descuidos no posto de trabalho.

Considerando que uma das premissas factuais relevantes previstas pela Análise Comportamental do Direito (Aguiar, 2017; Aguiar & Oliveira-Castro, 2020) é a probabilidade de ocorrência da conduta indesejada, foi solicitado aos participantes indicar a frequência de ocorrência desses padrões comportamentais (1 - Nunca a 5 – Muito frequentemente), conforme a sua realidade, e aberta a possibilidade para que informassem outras condutas que não se encaixem nas categorias sugeridas.

Como pode ser observado na Tabela 10, aproximadamente, nove participantes indicaram que categoria comportamental “Compartilhamento de senhas” raramente ocorre (i.e., frequência 1 e 2), sendo que os demais indicaram que o padrão comportamental ocorre com alguma frequência. Em relação à categoria “Uso inadequado dos recursos de TI”, verificou-se que a maioria dos participantes (71%) indicaram a baixa frequência de sua ocorrência (i.e., frequência 1 e 2). Da mesma forma, quanto à categoria “Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)”, apenas sete participantes (35%) indicaram que o padrão comportamental ocorre com alguma frequência (i.e., frequência 3 a 5). Já em relação à categoria comportamental “Descuidos no posto de trabalho”, 14 participantes (66%) indicaram que o padrão comportamental ocorre com alguma frequência (i.e., frequência 3 a 5).

Tabela 10.

Frequência de ocorrência das categorias de padrões comportamentais.

Categorias de padrões comportamentais	Frequência de ocorrência				
	1. Nunca	2	3	4	5. Muito frequentemente
Compartilhamento de senhas	2	7	7	4	1
Uso inadequado dos recursos de TI	1	14	4	2	0
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)	3	10	4	2	1
Descuidos no posto de trabalho	1	6	10	1	3

Acerca disso, cabe destacar que dos 15 participantes que responderam que as condutas que se enquadram na categoria de padrões comportamentais "Uso inadequado dos recursos de TI" raramente ocorreram, 12 (80%) informaram que não há monitoramento das atividades dos usuários ou que o monitoramento é feito de forma reativa, ou seja, após a ocorrência do incidentes de segurança da informação (Figura 22, escala 1 e 2). Da mesma forma, em relação à categoria de padrões comportamentais "Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)", dos 13 participantes que responderam que as condutas dessa categoria raramente ocorreram, 8 (i.e., aproximadamente 61,5%) informaram que o monitoramento das atividades dos colaboradores é feito de forma reativa, conforme consta na Tabela 11.

Tabela 11.

Relação da forma de monitoramento das atividades dos usuários com a indicação de baixa frequência das categorias de padrões comportamentais.

Categorias de padrões comportamentais	Forma de monitoramento	
	Não há/Reativo (1 e 2)	Neutra ou proativa (3 a 5)
Compartilhamento de senhas	6	3
Uso inadequado dos recursos de TI	12	3
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)	8	5
Descuidos no posto de trabalho	4	3

Nessa esteira, à exceção da categoria comportamental “Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)”, para as demais categorias, os participantes cujas empresas realizam a atividade de monitoramento de forma proativa indicaram uma maior frequência média de ocorrência das referidas condutas, conforme a Tabela 12.

Por fim, em relação às categorias de padrões comportamentais, convém destacar que não houve apontamento, por qualquer participante, de alguma conduta que não se encaixasse em uma das quatro categorias comportamentais sugeridas no questionário.

Quanto às possíveis consequências previstas na política de segurança da informação, todos os participantes responderam que não há qualquer iniciativa para premiar os colaboradores por observar a política de segurança da informação. Quanto aos tipos de sanções que são aplicadas, constata-se na Tabela 13, que apenas três participantes responderam que a sanção do

tipo Advertência é aplicada frequentemente, já as demais sanções (i.e., Suspensão e Demissão), segundo os participantes, ou raramente ocorrem ou nunca ocorreram.

Tabela 12.

Média de frequência das categorias de padrões comportamentais por perfil de empresa de acordo com a forma de monitoramento das atividades dos usuários.

Categorias de padrões comportamentais	Média de frequência	
	Monitoramento Reativo	Monitoramento proativo
Compartilhamento de senhas	2,75	3,33
Uso inadequado dos recursos de TI	2,08	3
Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)	2,5	2
Descuidos no posto de trabalho	3	3,33

Tabela 13.

Frequência de sanções aplicadas.

Sanções	Frequência de aplicação			
	Não ocorreu	Raramente	Frequentemente	Sempre
Advertência	11	7	3	0
Suspensão	18	3	0	0
Demissão	18	3	0	0
Outra(s)	17	2	2	0

Há que se destacar que além das sanções de Advertência, Suspensão e Demissão, foi dada a oportunidade ao participante de informar outras medidas que são adotadas pela organização e que sejam percebidas como sancionatórias ou corretivas pelos usuários internos. Nesse sentido,

dois participantes responderam que frequentemente ocorre uma advertência mais branda, verbalmente ou por correio eletrônico, de caráter instrucional ou educativo. Outros dois participantes responderam que, apesar de raro, houve casos em que chefia imediata do colaborador foi comunicada ou o colaborar perdeu o direito de acesso ao recurso que deu causa ao incidente de segurança da informação.

Nessa esteira, verificou-se que aproximadamente 86% dos participantes afirmaram que a organização não tem a prática de sancionar as condutas que violam a política de segurança da informação instituída (i.e., frequência 1 e 2), conforme exposto na Figura 23.

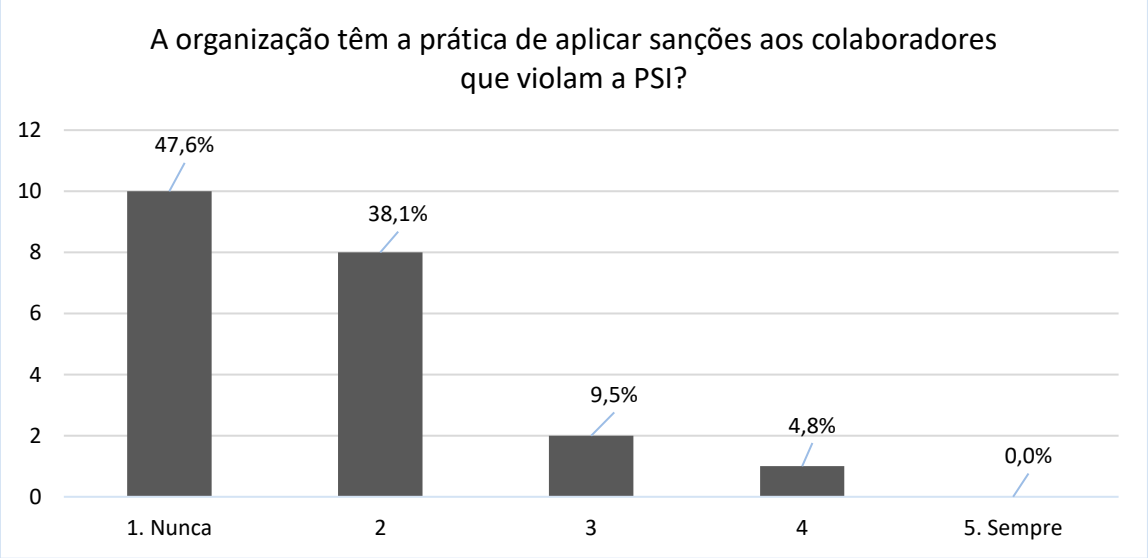


Figura 23. Avaliação do *enforcement* da política de segurança da informação.

Acerca disso, convém ressaltar que quando questionados acerca da percepção da gravidade dos incidentes de segurança da informação, 13 participantes (62%) concordaram, em algum grau (i.e., grau de concordância 4 e 5), que as violações da política de segurança da informação são, usualmente, tratadas prontamente na esfera técnica, fato que reduz a percepção de gravidade pelo restante da organização. Merece destaque, que os demais participantes não discordaram dessa afirmação, ou seja, permaneceram neutros (i.e., grau de concordância 3). Na

mesma linha, 18 participantes (85,7%) afirmaram que, apesar de haver uma política de segurança da informação formalizada, houve a necessidade de investimentos em soluções de tecnologia da informação para impedir condutas dos colaboradores que violem os requisitos de segurança da informação estabelecidos pela organização (i.e., grau de concordância 4 e 5), conforme detalhado na Tabela 14.

Tabela 14.

Medidas complementares/efeitos decorrentes do enforcement da PSI.

Medidas complementares/Efeitos do *enforcement* da PSI	Grau de concordância				
	1. Discordo plenamente	2	3	4	5. Concordo plenamente
As violações da política de segurança da informação, usualmente, são prontamente tratadas na esfera técnica, fato que reduz seus impactos e contribui para a percepção de baixa gravidade pela organização	0	0	8	7	6
Mesmo com a formalização da PSI houve a necessidade de investimentos em soluções de segurança da informação para impedir condutas dos usuários que violam os requisitos de segurança da informação da organização	0	1	2	4	14

Como já exposto, a maior parte das empresas representadas nesse estudo (67%) conta com mais de 1000 usuários internos. Sendo assim, foram criados dois grupos, sendo o primeiro com as empresas que tenham até 1000 usuários (i.e., sete participantes) e outro com as demais empresas que ultrapassam esse número de usuários. Os resultados demonstraram, conforme consta na Tabela 15, que para ambos os grupos, o mesmo percentual de participantes (86%) afirmou que as empresas não têm a prática de sancionar as condutas que violam a sua política de segurança da informação (i.e., frequência 1 e 2).

Tabela 15.

Relação da aplicação de sanções com o porte da empresa.

Porte da empresa	Frequência de aplicação das sanções				
	1 Nunca	2	3	4	5 Sempre
Até 1000 usuários internos	3	3	1	0	0
Acima de 1000 usuários internos	7	5	1	1	0

Nessa mesma linha, foi verificado se o porte da organização tem alguma relação com a necessidade das empresas investirem em soluções complementares para o controle dos comportamentos dos usuários (i.e., fechamento do cenário) ou com a afirmação de que as violações da política de segurança da informação são usualmente tratadas na esfera técnica o que reduz a percepção de gravidade pelo resto da organização. Como pode ser observado na Tabela 16, em ambos os grupos, o mesmo percentual de participantes (86%) afirmou que houve a necessidade de investir em soluções de segurança da informação complementares para controlar o comportamento dos colaboradores (i.e., grau de concordância 4 e 5). Já em relação à afirmação de que as violações são tratadas prontamente na esfera técnica o que reduz a percepção de gravidade pelo restante da organização, no Grupo 1 (até 1000 usuários internos) 71% dos participantes concordaram com a afirmação e no Grupo 2 (acima de 1000 usuários internos) 57% concordaram com a afirmação (i.e., grau de concordância 4 e 5). Cabe destacar que, em ambos os grupos, os demais participantes foram neutros em relação à afirmação (i.e., grau de concordância 3), mas não houve nenhuma discordância.

Tabela 16.

Relação do porte da empresa com as afirmações acerca da necessidade de investir em soluções complementares para controlar os comportamentos dos colaboradores e do tratamento das violações da PSI prontamente realizado na esfera técnica.

Porte da empresa	Necessidade de investir em soluções complementares [a]					Tratamento das violações da PSI prontamente na esfera técnica [a]				
	1	2	3	4	5	1	2	3	4	5
Até 1000 usuários internos	0	0	1	2	4	0	0	2	3	2
Acima de 1000 usuários internos	0	1	1	2	10	0	0	6	4	4

[a] Escala de respostas de 1 – Discordo plenamente a 5 – Concordo plenamente.

Para avaliar a relação do grau de maturidade na gestão da segurança da informação e a prática de sancionar os comportamentos que violem a PSI, adotou-se como critério de maturidade em gestão de segurança da informação o tempo que a organização tem uma política de segurança da informação formalmente instituída, considerando tratar-se de requisito fundamental para o estabelecimento de um SGSI (ABNT, 2013a, 2013b).

Como pode ser verificado na Tabela 17, 80% dos participantes que representam empresas que tem uma política de segurança da informação formalizada há menos de 10 anos (i.e., 17 participantes), concordam que sanções nunca são aplicadas ou raramente são (i.e., frequência 1 e 2). O mesmo ocorre com os participantes que representam as empresas mais maduras na gestão da segurança da informação, isto é, com uma política de segurança da informação formalizada há mais de 10 anos, três dos quatro participantes afirmaram que aplicação das sanções nunca ocorre (i.e., frequência 1) e um permaneceu neutro (i.e., frequência 3).

Tabela 17.

Relação da aplicação de sanções com a maturidade da empresa na gestão da segurança da informação.

Tempo de PSI formalizada	Frequência de aplicação das sanções				
	1 Nunca	2	3	4	5 Sempre
Menos de 5 anos	3	4	1	0	0
Entre 5 e 10 anos	4	4	0	1	0
Acima de 10 anos	3	0	1	0	0

Quanto à possível relação da maturidade em gestão da segurança da informação na necessidade das empresas investirem em soluções complementares para o controle dos comportamentos dos usuários (i.e., fechamento do cenário), constata-se que no grupo com as empresas que formalizaram a política de segurança da informação há menos de cinco anos, três participantes (38%) não concordaram com a afirmação, isto é, dois foram neutros (i.e., grau de concordância 3) e um discordou (i.e., grau de concordância 2). Nos outros dois grupos, todos os participantes concordaram, em algum grau, com a afirmação (i.e., grau de concordância 4 e 5). Já em relação à afirmação de que as violações da política de segurança da informação são usualmente tratadas na esfera técnica o que reduz a percepção de gravidade pelo resto da organização, constata-se não houve discordância em relação à afirmação em quaisquer um dos grupos (i.e., grau de concordância 1 e 2), conforme consta na Tabela 18.

Tabela 18.

Relação da maturidade em gestão da segurança da informação com as afirmações acerca da necessidade de investir em soluções complementares para controlar os comportamentos dos colaboradores e do tratamento das violações da PSI prontamente realizado na esfera técnica.

Tempo de PSI formalizada	Necessidade de investir em soluções complementares [a]					Tratamento das violações da PSI prontamente na esfera técnica [a]				
	1	2	3	4	5	1	2	3	4	5
Menos de 5 anos	0	1	2	1	4	0	0	3	4	1
Entre 5 e 10 anos	0	0	0	1	8	0	0	3	1	5
Acima de 10 anos	0	0	0	2	2	0	0	2	2	0

[a] Escala de respostas de 1 – Discordo plenamente a 5 – Concordo plenamente.

Discussão

O objetivo do Estudo 3 foi obter uma visão mais abrangente acerca dos resultados da análise comportamental do SGSI estabelecido pela organização participante dos primeiros dois estudos. Nessa esteira, aproximadamente cem diretores de tecnologia da informação foram convidados para responder a um questionário, elaborado com base nos principais achados desses dois estudos, sendo que houve 21 respostas.

Acerca disso, convém ressaltar que a gestão da segurança da informação nas organizações é um tema sensível, e, conforme apontam Kotulic e Clark (2004), as empresas geralmente não estão predispostas a fornecer esse tipo de informação sem maiores garantias. Nesse sentido, os autores sugerem que é mais produtivo ter foco e trabalhar com poucas empresas que tenham confiança nos pesquisadores e na pesquisa a ser realizada. Destarte, conclui-se que a amostra de respostas obtida foi adequada para o alcance dos objetivos traçados no presente estudo.

A partir dos dados levantados, verifica-se que o estudo contou com grande participação de instituições administração pública federal (81%). Entretanto, cabe destacar que a partir da análise

da resposta da única empresa identificada como privada na pesquisa, verificou-se que as principais conclusões do estudo foram corroboradas. Isto é, a empresa não adota a prática de sancionar as condutas que violam a política de segurança da informação, que essas violações são prontamente tratadas na esfera técnica, o que reduz a percepção de gravidade pela empresa, e que foi necessário investir em soluções tecnológicas complementares para impedir a ocorrência dessas condutas. De todo modo, verifica-se que há a necessidade de ampliar a presente pesquisa, em especial com participação do setor privado, com vistas a obter uma visão mais completa acerca do tema.

Acerca disso, impende ressaltar que, no contexto dessa pesquisa, o principal fator diferenciador entre as empresas "públicas" e "privadas" é a relação de trabalho. Pois, conforme exposto, o principal mecanismo de *enforcement* das políticas de segurança da informação é a aplicação de sanções. Logo, um fator relevante a ser considerado é que a relação trabalhista de servidores públicos é regida por lei específica (e.g., Lei 8.112/1990), enquanto para os empregados privados, ou, em alguns casos, públicos, é, usualmente, regulamentada pela Consolidação das Leis do Trabalho – CLT. Assim sendo, os primeiros gozam de algumas prerrogativas, em especial, a de estabilidade no exercício do cargo público, que pode influenciar a aplicação de sanções pelas organizações públicas.

Quanto à maturidade em gestão da segurança da informação, verificou-se que a maioria das empresas possui política de segurança da informação há mais de cinco anos (62%), processo de tratamento de incidentes de segurança da informação definido (70%) e monitoram as atividades de seus colaboradores com vistas a identificar eventuais violações de sua PSI (91%). Constata-se, portanto, que a amostra reúne empresas que estabeleceram um sistema de gestão de segurança da informação, com os elementos mínimos identificados nesse trabalho para tratar a questão comportamental dos colaboradores.

Entretanto, há que se destacar que em relação ao registro e monitoramento das atividades dos usuários, apenas três participantes declararam que a prática é realizada de forma proativa, ou seja, buscando se antecipar à ocorrência dos incidentes de segurança da informação. Acerca disso, convém ressaltar que, assim como foi identificado no Estudo 1, a prática de monitorar as atividades dos colaboradores dificilmente terá função aversiva, no sentido de reduzir a frequência dos comportamentos que violam a PSI, enquanto for executada de forma reativa pelas empresas, pois seus efeitos só serão percebidos naqueles casos em que houver o tratamento do incidente de segurança da informação e, conforme foi apresentado na Tabela 9, a maioria dos participantes (86%) responderam que trataram, nos últimos cinco anos, até 20 violações de sua política de segurança da informação, ou seja, uma média de até quatro violações por ano.

Em relação à frequência de ocorrência dos comportamentos considerados indesejados pelas organizações, destaca-se que os resultados do presente estudo validaram as categorias comportamentais propostas no Estudo 1, pois não houve o apontamento de qualquer conduta que não pudesse ser enquadrada em uma das quatro categorias de padrões comportamentais propostas no primeiro estudo, quais sejam: Compartilhamento de senhas; Uso inadequado dos recursos de TI; Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico); e Descuidos no posto de trabalho.

Quanto à frequência desses comportamentos, convém relembrar que foi solicitado aos participantes para indicar a frequência de sua ocorrência, em uma escala de 1 a 5, sendo 1 para os casos que nunca aconteceram e 5 para os casos que ocorrem muito frequentemente. Fazendo um agrupamento dos dados em dois grupos, sendo o primeiro de comportamentos que raramente aconteceram, frequências 1 e 2, e o segundo de comportamentos que ocorreram com alguma frequência (i.e., frequências de 3 a 5), tem-se a distribuição da frequência de ocorrência das categorias comportamentais, conforme a Figura 24.

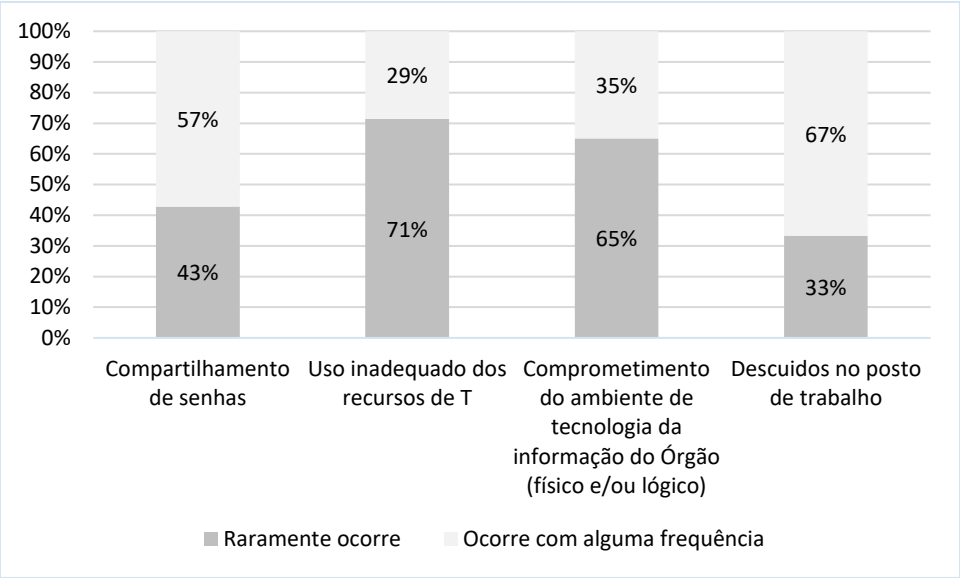


Figura 24. Consolidação da frequência das categorias de padrões comportamentais.

Depreende-se da figura acima, que as condutas que se enquadram nas categorias de padrões comportamentais “Uso inadequado dos recursos de TI” e “Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)” raramente ocorreram, de acordo com os participantes. Por outro lado, a maioria dos participantes responderam que condutas correspondentes às categorias de padrões comportamentais “Compartilhamento de senhas” e “Descuidos no posto de trabalho” ocorreram com alguma frequência.

Acerca disso, cabe destacar que, conforme consta na Tabela 14, a maioria dos participantes (aproximadamente 86%) concordaram com a afirmação de que mesmo com a formalização da PSI houve a necessidade de investimentos adicionais em soluções de segurança da informação para impedir condutas dos usuários que violam seus requisitos de segurança da informação. Verificou-se, também, que aproximadamente 73% dos participantes que responderam que as condutas que se enquadram na categoria de padrões comportamentais “Uso inadequado dos recursos de TI” raramente ocorreram, também informaram que não há monitoramento das atividades dos usuários ou que o monitoramento é feito de forma reativa, isto

é, após a ocorrência do incidentes de segurança da informação. Da mesma forma, em relação à categoria de padrões comportamentais “Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico)”, aproximadamente 61,5% dos participantes que responderam que as condutas dessa categoria raramente ocorreram também informaram que o monitoramento das atividades dos colaboradores é feito de forma reativa, conforme a Tabela 11.

Com base nesses dados, verifica-se que, apesar do comando no questionário consignar que a frequência indicada pelos respondentes deve considerar não só as condutas que foram exitosas (i.e., aquelas que os eventuais mecanismos de controle implementados pela organização não foram suficientes para impedi-las), mas também as condutas mal sucedidas, ou seja, as tentativas sem êxito em decorrência da implementação dos mecanismos de controle implementados pela organização, a realidade apontada pela grande maioria dos participantes, de que as empresas investiram em soluções complementares para controlar o comportamento dos colaboradores, somada à prática de usar os registros das atividades dos usuários apenas de forma reativa (i.e., os registros são usados em atividades de auditoria e/ou para a produção de evidências quando um incidente de segurança da informação está sendo tratado), pode ter relação com as respostas dos participantes acerca da frequência de ocorrência dessas categorias de padrões comportamentais.

Pois, conforme consolida a Tabela 12, os resultados sugerem que a forma como as empresas monitoram a atividade de seus colaboradores tem relação com a percepção da frequência de ocorrências das condutas que violam a PSI. Isto é, os comportamentos até podem ocorrer com uma frequência maior, mas sendo os mecanismos complementares de proteção eficazes e o monitoramento das atividades reativo, a frequência dessas condutas (e.g., tentativa de acesso a um *site* inadequado ou de instalar um programa não licenciado) pode ter sido subestimada.

Por exemplo, para as categorias de padrões comportamentais “Compartilhamento de senhas” e “Descuidos no posto de trabalho”, cujas condutas são mais difíceis de serem controladas por soluções tecnológicas usualmente implementadas pelas organizações (e.g., *antivírus* e soluções de proteção de estação de trabalho) a maioria dos participantes responderam que essas categorias comportamentais ocorreram com alguma frequência, conforme pode ser observado na Figura 24.

Em relação às consequências previstas nas políticas de segurança da informação, impende ressaltar que todos os participantes afirmaram que não há qualquer programa de incentivo para os colaboradores por observarem a política de segurança da informação. Esse resultado corrobora uma premissa fundamental adotada no presente trabalho de que os sistemas de gestão de segurança da informação estão calcados na definição de uma política de segurança da informação e na previsão de sanções em caso de descumprimento. Ou seja, na interpretação aqui proposta, os SGSIs lidam com o macroproblema de exercer o controle coercitivo de comportamentos que violem a sua PSI e tem como consequência condicionada socialmente generalizada (CCSG) a aplicação de sanções.

Quanto às sanções, como foi apresentado na Figura 23, quase 86% dos participantes (i.e., 18 participantes), indicaram o baixo *enforcement* da PSI, ou seja, que a empresa não aplica as sanções previstas no normativo ou raramente o faz. Acerca disso, convém destacar que apenas dois participantes informaram que as empresas buscaram outras formas de sancionar o comportamento não conforme do colaborador, por meio de advertências mais brandas, de caráter educativo, mas consistentemente contingente à conduta, isto é, frequentemente aplicada conforme à sua ocorrência. Constata-se que essas empresas seguiram na mesma direção da proposta feita no Estudo 2, no sentido da organização participante do referido estudo buscar uma gradação de sanções, com vistas a aprimorar o *enforcement* de sua PSI.

Cabe ressaltar que os resultados do estudo também sugerem que a prática de aplicar as sanções previstas nas PSIs não está relacionada ao porte da empresa (i.e., considerando o número de usuários internos) ou à maturidade em gestão da segurança da informação (i.e., considerando o tempo de formalização da política de segurança da informação). Verificou-se que, seja para as empresas com menos de 1000 funcionários ou acima desse número, 86% dos participantes ratificaram que a empresa não adota a prática de aplicar as sanções previstas na PSI. Da mesma forma, conforme ficou demonstrado na Tabela 17, 80% das empresas representadas que tem uma política de segurança da informação formalizada há menos de 10 anos e 75% das empresas representadas que tem PSI formalizada há mais de 10 anos concordaram que as sanções nunca são aplicadas ou raramente são.

Por fim, os resultados deste estudo corroboraram dois importantes achados do Estudo 2, quais sejam: a necessidade de investir em soluções tecnológicas complementares para "fechar o cenário" dos colaboradores; e que a percepção de gravidade dos incidentes de segurança da informação pela organização é prejudicada pela eficiência no tratamento dado a esses incidentes na esfera técnica.

Em relação ao primeiro, a grande maioria dos participantes (85,7%) concordou que houve a necessidade de investir em outras soluções para controlar o comportamento de seus colaboradores. Há que se destacar, que esse percentual praticamente se repetiu quando da separação desses participantes em dois grupos, conforme o porte da empresa que representam (86% em ambos os grupos). Ou seja, constata-se que o porte da organização, nesta amostra, não parece ter relação com a necessidade da organização em investir em soluções complementares para controlar o comportamento dos colaboradores. Quanto à possível relação da maturidade em gestão da segurança da informação, constata-se que todos os três participantes que não concordaram que houve a necessidade de investir em soluções complementares (i.e., um

discordou e dois permaneceram neutros, i.e., grau de concordância 3) representam empresas que têm política de segurança da informação formalizada há menos de cinco anos. Observa-se, portanto, que a necessidade de implementar outras soluções para impedir condutas que violem a PSI pode estar associada ao tempo em que a empresa passou a tratar da questão de segurança da informação, isto é, na medida em que os incidentes vão sendo identificados e tratados, conforme definição da política de segurança da informação, a necessidade de novos investimentos para controlar essas condutas indesejadas parece se intensificar.

Convém ressaltar, que essa necessidade de mecanismos complementares não surpreende, pois, conforme já exposto, as consequências previstas nas políticas de segurança da informação (i.e., sanções), não estão consistentemente contingentes às condutas indesejadas, logo, essas consequências perderam seu efeito aversivo.

Quanto à relação da afirmação de que a eficiência no tratamento dado às violações da PSI na esfera técnica, o que reduz seus impactos e, consequentemente, a percepção de gravidade de sua ocorrência pelo restante da organização, nenhum participante discordou dessa afirmação. Em relação ao porte das empresas, verificou-se que 71% dos participantes que representam empresas com menos de 1000 usuários internos concordaram com a afirmação. Por outro lado, no grupo de empresas com mais de 1000 usuários internos, 43% (i.e., seis participantes) permaneceram neutros (i.e., grau de concordância 3). Acerca disso, há que se verificar em futuros estudos se essa neutralidade está associada à afirmação da percepção de baixa gravidade dos incidentes de segurança da informação pelo restante da organização ou à afirmação acerca da eficiência do processo de tratamento de incidentes de segurança da informação, em especial, considerando que na presente amostra 86% dos participantes declaram que até 20 violações da política de segurança da informação foram tratadas nos últimos cinco anos, ou seja, um número relativamente baixo, especialmente para as organizações de maior porte.

Em relação à maturidade das organizações na gestão da segurança da informação, verificou-se que para os representantes de empresas com PSI formalizada há menos de cinco anos, 38%, ou seja, três participantes permaneceram neutros (i.e., grau de concordância 3); das empresas com PSI formalizada entre cinco e dez anos, 33% permaneceram neutros (i.e., três participantes); e, das empresas com PSI formalizada há mais de dez anos, 50% permaneceram neutros (i.e., dois participantes). Entretanto, cabe destacar que desses oito participantes, seis representam empresas com mais de 1000 usuários internos, ou seja, de maior porte. Observa-se, portanto, que a avaliação dos participantes da afirmação de que a eficiência do tratamento dado às violações da PSI, na esfera técnica, reduz seu efeito aversivo para o restante da organização, parece estar mais associada ao porte da organização do que à maturidade dessas empresas na gestão da segurança da informação.

Outro importante ponto a se destacar, é que a maioria dos participantes do presente estudo representaram órgãos públicos, ou seja, com perfil de risco semelhante ao da organização participante dos estudos 1 e 2. Nesse sentido, verifica-se que com a decisão de "fechar o cenário" para os colaboradores, as unidades técnicas dessas instituições têm um controle mais eficiente desses comportamentos, o que leva a uma maior eficácia no tratamentos dos incidentes de segurança da informação que venham ocorrer, minimizando os impactos e, consequentemente, a percepção de gravidade pelo restante da organização. Portanto, verifica-se que essa visão pode, até certo ponto, ser representativa para o universo de órgãos públicos, entretanto, constata-se a necessidade de replicar esses estudos em empresas de mercados mais competitivos, tipicamente privadas, em que a decisão de "fechar o cenário" não é trivial, pois pode implicar em perdas de oportunidades de negócio, produtividade dos colaboradores e assim por diante.

Do exposto, conclui-se que, apesar das limitações impostas pela amostra de participantes, predominantemente composta por representantes de órgãos públicos, o objetivo traçado para o

terceiro estudo foi alcançado, na medida em que possibilitou complementar a análise de duas importantes premissas factuais relevantes, a probabilidade de ocorrência da conduta indesejada e a potencial eficácia da sanção, bem como investigar possíveis relações entre características das empresas representadas no presente estudo e a adoção da prática de sancionar as condutas que violem seus requisitos de segurança da informação.

Os resultados corroboraram importantes premissas adotadas neste trabalho, reforçando a viabilidade da interpretação analítica-comportamental dos sistemas de gestão de segurança da informação. Também apontaram para a mesma direção que os resultados obtidos nos primeiros dois estudos. Isto é, que o *enforcement* das políticas de segurança da informação está calcado na aplicação de sanções às condutas que não observarem seus requisitos, mas que, apesar dessas políticas preverem a aplicação de sanções, as organizações não adotam essa prática e optam por investimentos adicionais em outros mecanismos de proteção (e.g., *antivírus*, bloqueios de recursos nas estações de trabalho) que dificultam a ocorrência dessas violações. Por fim, que nos casos em que as tentativas de violar a PSI são bem sucedidas, estas são prontamente tratadas pelas unidades de tecnologia da informação, reduzindo a percepção de gravidade pelo restante da organização, contribuindo para que as consequências previstas nas PSIs (i.e., sanções) não sejam consistentemente contingentes à conduta indesejada.

Discussão Geral

Os estudos realizados alcançaram o objetivo desta pesquisa, isto é, por meio da identificação, descrição e análise das contingências planejadas nas políticas de segurança da informação e das contingências vigentes no comportamento dos principais atores que compõem um sistema de gestão da segurança da informação, com base na Análise Comportamental do Direito, verificou-se a viabilidade da interpretação proposta nesta pesquisa, qual seja, a análise comportamental dos sistemas de gestão de segurança da informação.

A partir dos resultados do Estudo 1, obteve-se o primeiro achado de grande relevância para a pesquisa, isto é, que, assim como ocorre com o direito, a política de segurança da informação analisada busca controlar os comportamentos dos colaboradores por meio de sanções. Ou seja, nos termos desta proposta (i.e., a análise comportamental dos sistemas de gestão de segurança da informação), o SGSI da organização lida com o macroproblema de exercer o controle coercitivo de comportamentos que violem a sua PSI e tem como consequência condicionada socialmente generalizada a aplicação de sanções.

Nessa mesma esteira, outro importante componente previsto na Análise Comportamental do Direito foi identificado, que é a relação das contingências planejadas com a meta social do SGSI estabelecido. Ou seja, foi verificado que as contingências planejadas na PSI contribuem para a proteção das informações com vistas a assegurar a continuidade do negócio, mitigar seus riscos, maximizar o retorno sobre os investimentos realizados e ampliar as oportunidades de negócio (ABNT, 2013b). Acerca disso, há que se destacar a relevância deste achado, pois por meio da aplicação do modelo proposto, verificou-se a possiblidade de identificar e reavaliar as contingências que não contribuem para o alcance da meta social do SGSI, promovendo a melhoria do normativo e evitando eventuais consequências indesejadas em decorrência da contingência planejada. Cabe ainda destacar que a análise realizada se revelou útil para verificar o alinhamento das diretrizes de segurança da informação à estratégia da organização. Verificou-se no Estudo 1 que não foi identificado qualquer item da PSI relacionado à meta “Ampliar as oportunidades de negócio”. Ou seja, constata-se que o nível de risco que a organização está disposta a aceitar para implementar sua estratégia não é alto, pois a organização opta por limitar o acesso aos recursos tecnológicos disponíveis ao invés de assumir riscos mais elevados.

Ainda em relação aos riscos, verificou-se que a análise de riscos realizada pela organização participante contribuiu, sobremaneira, para a realização da análise comportamental

da PSI. Na identificação dos riscos, foram destacados o evento suas causas e consequências. A partir desse levantamento, foi possível identificar elementos do estado motivacional e contexto (antecedentes) da ocorrência do padrão comportamental (evento), bem como as consequências para a organização. Cabe destacar que a análise comportamental da PSI também contribuiu para a revisão da análise de riscos realizada pela organização participante. Com a consecução da pesquisa a organização concluiu pela necessidade de rever o grau de eficiência atribuído à sua PSI, enquanto procedimento de controle do comportamento dos seus colaboradores, nos cálculos dos seus riscos residuais (ABNT, 2018).

O Estudo 1, com base na análise funcional dos comportamentos considerados indesejados pela organização, ainda revelou o contexto, estado motivacional e reforços, que mantém esses comportamentos no repertório dos colaboradores. Por exemplo, foi verificado que facilitar a execução das atividades e o uso dos recursos tecnológicos foi um estado motivacional (i.e., operação motivadora) e reforço comum nas quatro categorias comportamentais identificadas. Nesse sentido, o estudo apontou a possibilidade de adoção de medidas gerenciais alternativas que facilitam o uso desses recursos, mantendo os respectivos riscos em níveis aceitáveis, sem a necessidade de aplicação de sanções e de lidar com suas possíveis consequências indesejadas.

O mesmo ocorreu com a identificação dos contextos em que os comportamentos ocorrem. Por meio da análise comportamental da política de segurança da informação, verificou-se que há a previsão do registro e monitoramento da utilização de recursos tecnológicos e a realização de auditorias nos ativos de TI da organização, ou seja, atividades que podem funcionar como estímulos aversivos condicionados e, consequentemente, também controlar o comportamento dos colaboradores. Entretanto, foi identificado que os contextos “possibilidade técnica” e “difícil monitoramento” são os mais frequentes entre as categorias comportamentais. Isto é, para os comportamentos contemplados nessas categorias, o monitoramento das atividades dos

colaboradores e a eventual auditoria da utilização dos recursos de TI dificilmente terão efeito aversivo como planejado na política de segurança da informação. Nesse sentido o estudo aponta a necessidade da organização avaliar medidas alternativas para o controle mais eficiente das condutas que ocorrem nesses contextos.

Constata-se, portanto, que o Estudo 1 demonstrou a viabilidade da análise comportamental das políticas de segurança da informação, mediante a adaptação do modelo proposto pela Análise Comportamental do Direito, no sentido de descrever as contingências planejadas e contribuir para a identificação de falhas, incoerências ou medidas complementares para o controle mais eficaz e eficiente dos comportamentos que violam seus requisitos de segurança da informação.

O Estudo 2 avançou na aplicação do modelo teórico proposto pela Análise Comportamental do Direito e na sua adaptação para a interpretação analítico-comportamental dos sistemas de gestão de segurança da informação. Nesse sentido, foi realizada a análise comportamental da norma de segurança da informação, isto é, a norma social do SGSI estabelecido, enquanto uma rede de padrões comportamentais entrelaçados, conforme proposto por Aguiar (2017) para o direito.

A partir do mapeamento do processo de gestão de incidentes de segurança da informação e do processo disciplinar da organização participante, foi possível identificar os colaboradores que exercem papéis-chaves na aplicação da política de segurança da informação (i.e., o *enforcement* da PSI), bem como os nós que compõem a norma de segurança da informação, a partir dos quais foram identificadas e analisadas as contingências que de fato estão vigentes e controlam comportamentos relevantes para o SGSI.

O principal achado do Estudo 2 foi a constatação de que, apesar de ser prevista na PSI, a organização não adota a prática de sancionar as condutas que violam seus requisitos de segurança

da informação. Acerca disso, convém resgatar que a consequência condicionada socialmente generalizada de um SGSI é aplicação de sanções, conforme disciplinam as principais normas que tratam gestão da segurança da informação nas organizações (e.g., ABNT, 2013a, 2013b). E para que as sanções tenham função aversiva (i.e., diminuir a frequência da resposta que a produziu) devem tornar-se, consistentemente, contingente ao comportamento indesejado. Verificou-se, portanto, que a principal contingência planejada na política de segurança da informação (Estudo 1) não está vigente, o que sugere que a implementação do principal procedimento de controle de segurança da informação, previsto nas boas práticas em gestão da segurança da informação, isto é, a definição de uma política de segurança da informação se mostra pouco eficaz.

Destaca-se que os resultados do Estudo 2, corroboram essa afirmação, pois, conforme descrito anteriormente, a ineficiência da PSI para controlar o comportamento dos colaboradores levou a organização a investir em medidas complementares, no sentido de impedir as condutas que violavam seus requisitos de segurança da informação, ou seja, levou ao "fechamento do cenário" dos colaboradores. Sendo assim, constatou-se que a ineficiência da PSI, pode elevar os custos para a organização, bem como implicar em um aumento de demanda para a unidade de TI.

Nesse sentido, verificou-se no segundo estudo a possibilidade de se adotar medidas alternativas com vistas ao controle dos comportamentos que violam os requisitos de segurança da informação. Por exemplo, através da definição de sanções gradativas (e.g., envio de e-mails com alertas e bloqueios temporários de acesso), conforme a gravidade da conduta, pois essa gradação de sanções, sendo consistentemente contingentes às condutas que violam a PSI, muito provavelmente terá o efeito punitivo almejado pela organização. Acerca disso, destaca-se que o Estudo 3 identificou duas organizações que adotaram medidas nesse sentido.

Acerca dos primeiros dois estudos, constata-se que análise comportamental da política de segurança da informação (Estudo 1) investigou as premissas que sustentam suas regras, ou seja,

avaliou a capacidade dessas regras controlarem os comportamentos de seus destinatários. Já a análise da norma de segurança da informação (i.e., norma social do SGSI) investigou as contingências responsáveis pela ocorrência dos comportamentos relevantes para o SGSI, isto é, aqueles relacionados à aplicação das sanções previstas na política de segurança da informação (Estudo 2). Verifica-se, portanto que os resultados da análise comportamental da política de segurança da informação são premissas da análise comportamental da norma de segurança da informação e vice-versa. Observa-se que os estudos 1 e 2 se complementam e, em até certo ponto, são indissociáveis para a análise comportamental de um sistema de gestão de segurança da informação nos termos proposto neste trabalho. Há que se destacar que isso era esperado, pois uma vez que a pesquisa adotou o arcabouço teórico estabelecido pela Análise Comportamental do Direito, que combina a teoria do comportamento operante com a teoria dos sistemas sociais funcionalmente especializados, essa reciprocidade é característica das ciências que estudam os sistemas sociais funcionalmente especializados, conforme explica Aguiar (2017).

Como pode ser observado, os estudos 1 e 2 demonstraram a viabilidade da interpretação analítico-comportamental dos sistemas de gestão de segurança da informação, por meio da análise comportamental da política de segurança da informação e da norma de segurança da informação (i.e., norma social do SGSI) de uma organização. Entretanto, conforme já exposto, a definição de uma política de segurança da informação e o estabelecimento de um SGSI, normalmente é feito pelas organizações seguindo padrões e boas práticas (Solms, 1999). Nessa esteira, o terceiro estudo buscou complementar as análises realizadas nos primeiros dois estudos e verificar até que ponto os principais achados poderiam ser extrapolados para outras organizações.

O primeiro ponto de destaque no Estudo 3 é a amostra das empresas representadas pelos participantes, que em sua grande maioria (81%) são instituições da administração pública federal. Nessa esteira, verifica-se que os resultados podem até ser representativos para esse segmento,

entretanto, constata-se que há a necessidade de replicar esses estudos em empresas do segmento privado, pois conforme já exposto, uma importante variável para a investigação da prática de sancionar as condutas dos colaboradores são as regras que regem as relações de trabalho.

Quanto aos seus resultados, verificou-se que estes corroboraram os principais achados dos primeiros dois estudos, isto é, que o *enforcement* das políticas de segurança da informação está calcado na aplicação de sanções (i.e., todos os participantes informaram que não há qualquer programa de incentivo para a observação da política de segurança da informação), que as empresas não aplicam ou raramente aplicam essas sanções, apesar de serem previstas nas políticas de segurança da informação, que as empresas realizaram investimentos adicionais em mecanismos de proteção complementares para dificultar a ocorrência de violações de sua PSI (i.e., fechamento do cenário) e que, nos casos em que esses mecanismos não são suficientes para impedi-las, os incidentes de segurança da informação são prontamente tratados pelas unidades de tecnologia da informação, reduzindo a percepção de gravidade pelo restante da organização.

A ineficiência desse modelo, baseado na aplicação de sanções, corrobora a conclusão, frequentemente apontada na literatura, da necessidade de se desenvolver uma "cultura de segurança da informação nas organizações" (e.g. Organisation for Economic Co-operation and Development, 2002; Machado, Cabral, Santos, & Motta, 2009; Vieira, 2009; do Nascimento, 2012). Conforme explicam Aguiar, Oliveira-Castro e Gobbo (2019), as regras podem ser interpretadas como unidade básica da seleção sociocultural. Isto é, na medida em que a sociedade se organiza em sistemas sociais funcionalmente especializados, esses sistemas criam regras de segunda ordem que visam selecionar aquelas regras que são eficientes, no sentido de contribuir para o alcance das metas sociais daquele sistema. Ou seja, na medida em que o comportamento de enunciar uma certa regra deixa de ser reforçado (i.e., não controla o comportamento do destinatário da regra) ele é enfraquecido no repertório comportamental. Nesse sentido, a

ineficácia do comportamento de enunciar a regra revela a ineficiência da regra em si, que pode ser excluída do sistema ou revista e aprimorada.

No contexto da gestão da segurança da informação, os resultados deste trabalho corroboram esta tese. Ou seja, na medida em que as contingências planejadas na PSI não estão vigentes, o comportamento de enunciar as regras que integram a PSI é enfraquecido, fazendo com que as respectivas regras não sejam selecionadas no SGSI (enquanto subsistema social funcionalmente especializado), não contribuindo para o estabelecimento da denominada "cultura de segurança da informação".

Os resultados do Estudo 3 ainda sinalizam que as categorias de padrões comportamentais, propostos no Estudo 1, são adequadas, podendo ser refinadas e/ou ampliadas em trabalhos futuros, mas indicam um bom ponto de partida para a análise comportamental dos SGSIs, pois não houve a indicação de qualquer conduta que não se encaixasse em uma das categorias de padrões comportamentais propostas.

Nessa esteira, o Estudo 3 ainda ratificou outro importante achado do Estudo 1 de que a prática de monitorar as atividades dos colaboradores dificilmente terá função aversiva, no sentido de reduzir a frequência dos comportamentos que violam a PSI. Por ser executada de forma reativa pela maioria das empresas e considerando a estratégia das empresas de "fechar o cenário" dos colaboradores, seus efeitos só serão percebidos naqueles poucos casos em que houver o tratamento do incidente de segurança da informação.

O terceiro estudo corroborou outro relevante achado do Estudo 2, que os incidentes de segurança da informação são usualmente tratados adequadamente na esfera técnica, logo seus impactos são reduzidos, assim como a percepção de sua gravidade pelo restante da organização. Observa-se que esse achado vai ao encontro de um problema apontado com frequência na literatura acerca dos desafios da gestão da segurança da informação nas organizações, isto é, que

a proteção das informações nas organizações ainda é tratada com um problema essencialmente técnico (Solana-González, Vanti & Fontana, 2019), sem um maior envolvimento da alta administração (e.g., AbuSaad, Saeed, Alghathbar & Khan, 2011; Fazenda & Fagundes, 2015).

Acerca disso, convém resgatar que Aguiar (2017) explica que a aversividade de uma conduta delituosa é operação motivadora fundamental para a ocorrência dos comportamentos jurídicos punitivos (i.e., a aplicação de sanções). Contata-se, portanto, que os resultados desta pesquisa reforçam essa afirmação, isto é, na medida em que os incidentes de segurança da informação são vistos como um problema essencialmente técnico, a ocorrência desses incidentes, dificilmente serão fatores causais eficazes para o comportamento das autoridades administrativas responsáveis pela aplicação de sanções.

Ainda em relação à aversividade da conduta, convém destacar que os resultados aqui apresentados se alinham aos da análise comportamental da Lei de Responsabilidade Fiscal realizada por Aguiar e Oliveira-Castro (2020). De acordo com os autores, ao analisar a aversividade da conduta omissiva de deixar de reduzir despesas com pessoal pelos gestores, o dano causado pela conduta omissiva não é imediato e se mostra relativamente abstrato, pois depende de diversas análises econômicas e contábeis. Nesse sentido, os autores apontam que “o delito se aproxima mais de uma conduta que aumenta o risco de certos eventos indesejáveis ocorrerem, do que de uma conduta que causa direta e imediatamente tais eventos” (Aguiar & Oliveira-Castro, 2020, p. 268).

Verifica-se que a conclusão acima se aplica à ocorrência dos incidentes de segurança da informação, isto é, o dano causado, usualmente, não é imediato e depende, muitas vezes, das mais diversas e complexas análises na esfera técnica. Ou seja, a ocorrência de um incidente de segurança da informação, normalmente, não compromete, direta e imediatamente, o alcance da meta social do SGSI, que, em última instância, é a proteção da organização, mas aumenta os

riscos disso ocorrer. Conclui-se, portanto, que esses fatores contribuem para a redução do efeito aversivo da ocorrência dos incidentes de segurança da informação dentro das organizações e ajudam a explicar a ineficácia e ineficiência desse modelo, baseado na aplicação de sanções, adotado para a implementação dos SGSIs.

Considerações Finais

O presente trabalho demonstrou a viabilidade da interpretação analítico-comportamental dos sistemas de gestão de segurança da informação como forma de mitigação dos riscos nas organizações. A partir da releitura dos SGSIs como subsistemas sociais funcionalmente especializados, verificou-se sua semelhança com a interpretação feita por Aguiar (2017) do direito. Isto é, foi possível identificar nos SGSIs os componentes característicos de um sistema social funcionalmente especializado e a semelhança desses componentes com os componentes do sistema jurídico.

A partir dessa adaptação teórica, foram realizados os estudos 1 e 2, com vistas à confirmação empírica de sua aplicabilidade. No Estudo 1, foi realizada a análise comportamental de uma política de segurança da informação, em que se verificou sua capacidade de apontar falhas e inconsistências no normativo, bem como de contribuir com proposições de medidas gerenciais alternativas para a mitigação dos riscos relacionados às condutas dos colaboradores. Já o Estudo 2 avançou na aplicação do modelo, realizando a análise comportamental da norma de segurança da informação, enquanto norma social do SGSI estabelecido. Nessa esteira, o estudo evidenciou a capacidade do modelo proposto de identificar as contingências vigentes no SGSI, bem como de sugerir intervenções no sistema com vistas a aprimorá-lo. Por fim, o terceiro estudo buscou obter uma visão mais abrangente acerca do tema, considerando que os SGSIs, usualmente, são estabelecidos seguindo normas e boas práticas. Os resultados corroboraram os

principais achados dos primeiros dois estudos, reforçando a viabilidade da aplicação do modelo teórico proposto, bem como seu potencial de replicação em outras organizações.

Como principal contribuição desta pesquisa, destaca-se a extensão da aplicação do arcabouço teórico-metodológico proposto pela Análise Comportamental do Direito para o contexto da gestão da segurança da informação nas organizações. Esta proposta propiciou um modelo para a análise comportamental da implementação dos SGSIs nas organizações, enquanto um conjunto de procedimentos para o tratamento dos riscos relacionados às condutas dos seus colaboradores. Entretanto, há que se destacar que os resultados dos estudos realizados vão além da demonstração da viabilidade do modelo proposto, pois apontam um novo caminho, baseado no modelo teórico e metodológico da análise do comportamento, para a realização de estudos passíveis de verificações empíricas (Oliveira-Castro, Oliveira & Aguiar, 2018), se distanciando da forma usual de como a questão comportamental é investigada no contexto da segurança da informação, isto é, baseada em intenções e atitudes (i.e., relatos), ou seja, sem a observação do comportamento de fato executado (e.g., Kim & Kim, 2017; Park & Chai, 2018).

Sob o ponto de vista aplicado, a presente pesquisa também traz relevantes contribuições. Destaca-se a integração da análise comportamental do SGSI com o processo de gestão de riscos. Isto é, conforme exposto, a gestão de riscos realizadas pelas organizações além de contribuir para a análise comportamental do SGSI pode se beneficiar dela, no sentido da análise comportamental dos SGSIs ter se revelado um instrumento importante para verificar se as diretrizes de segurança da informação estão alinhadas à estratégia organizacional, ou seja, a análise comportamental do SGSI pode contribuir para o alinhamento da definição dos requisitos de segurança da informação ao perfil de risco organizacional.

Ainda no campo aplicado, a partir do presente trabalho há a possibilidade de se desenvolver novos estudos aprofundando a análise comportamental dos SGSIs. Isto é, os

resultados aqui expostos poderão servir de referência para futuros estudos, além desses novos estudos poderem aprimorar o modelo aqui proposto, desenvolvendo medidas e variáveis mais precisas relacionadas aos comportamentos relevantes para o *enforcement* das PSIs nas organizações.

Nessa mesma esteira, vislumbra-se novas linhas de pesquisa acerca das condutas dos colaboradores no contexto da segurança da informação nas organizações. Por exemplo, uma linha de pesquisa pode ser os efeitos da implementação de consequência reforçadoras para os comportamentos "seguros" dos colaboradores (i.e., que observam a PSI). Outro campo para a investigação são os efeitos da gradação de sanções, conforme proposto no Estudo 2, e verificada iniciativas nesse sentido em duas empresas no Estudo 3. Outo ponto importante a ser investigado e confirmado empiricamente, são efeitos das relações de trabalho na prática de aplicar sanções pelas organizações, conforme sugerido no Estudo 3.

Além dos aspectos teóricos, metodológicos e empíricos das contribuições dessa pesquisa abordados até aqui, há que se destacar suas implicações práticas na gestão da segurança da informação pelas organizações. Isto é, a simples consignação nas boas práticas ou regulamentos de que é necessário estabelecer um processo sancionatório para as condutas que violam os requisitos de segurança da informação nas organizações (e.g. ABNT, 2013a, 2013b; Decreto n. 9637, 2018), não se revela suficiente. Por exemplo, para o caso dos órgãos da administração pública federal, maior parte da amostra do Estudo 3, foi editada, recentemente, uma instrução normativa dispondo sobre a estrutura de gestão da segurança da informação a ser implementada, que, em termos de estabelecimento de regras de condutas para os colaboradores, se limita a prever a obrigatoriedade de se estabelecer as consequências e as penalidades para os casos violações da PSI ou quebras de segurança, observando ordenamento jurídico relacionado à aplicação de penalidades ao servidor público federal (Instrução Normativa n. 1, 2020).

Constata-se, portanto, que os resultados apresentados nessa pesquisa sugerem que a forma usualmente adotada para a implementação desse modelo sancionatório revela-se pouco eficiente. Ou seja, a partir do modelo teórico-metodológico proposto neste trabalho para a análise comportamental dos SGSIs, bem como das evidências empíricas aqui reunidas, vislumbra-se a possibilidade de aprimorar as orientações constantes das boas práticas, assim como dos regulamentos que definem as diretrizes para a gestão da segurança da informação nas organizações. Ou seja, a revisão desses normativos, com base nos resultados dessa e de futuras pesquisas, pode contribuir para a melhoria da eficácia e eficiência dos SGSIs em um universo mais amplo de organizações.

Por fim, destaca-se, que um SGSI, é um sistema de gestão como vários outros (e.g., qualidade, meio ambiente, segurança e saúde no trabalho). Isto é, trata-se de um sistema que define políticas, objetivos e processos e implementam metodologias para que as etapas desses processos ocorram de forma controlada, monitorada e em constante aprimoramento, para o alcance do objetivo almejado (Neto, da Cunha Tavares & Hoffmann, 2019). Ou seja, há uma outra frente de investigação, que é a viabilidade de aplicação do modelo adotado para a análise comportamental dos SGSIs em outros sistemas de gestão. A consecução desses estudos pode, inclusive, induzir o aprofundamento teórico-conceitual acerca da interpretação de sistemas de gestão específicos como subsistemas sociais. Isto é, sendo uma prática comum às organizações, um caminho plausível é de que seja possível o desenvolvimento de uma tecnologia comportamental a partir da aplicação e evolução do modelo analítico-comportamental nos mais diversos sistemas de gestão.

Referências

AbuSaad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned. https://doi.org/10.4225/75/ 57b52709cd8b2

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp.21-29). New York, NY.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In *Economics of information security* (pp. 165-178). Boston, MA: Springer.

Aguiar, J. C. de (2006). *Análise Comportamental do Direito: Fundamentos para uma abordagem do direito como ciência comportamental aplicada*. Tese de doutorado. Universidade Federal de Santa Catarina.

Aguiar, J. C. (2013). O direito como sistema de contingências sociais. *Revista da Faculdade de Direito da UFG, 37*(2), 164 - 196. https://doi.org/10.5216/rfd.v37i2.23681

Aguiar, J. C. (2014). Análise comportamental do direito: fundamentos para uma abordagem do direito como ciência comportamental aplicada. *Revista do Programa de Pós-Graduação em Direito da UFC, 34(2*), 245–273.

Aguiar, J. C. (2017). *Teoria analítico-comportamental do direito: Para uma abordagem do direito como sistema social funcionalmente especializado*. Porto Alegre, RS: Núria Fabris.

Aguiar, J. C., & Oliveira-Castro, J. M. (2020). *Direito, política e economia na lei de responsabilidade fiscal:* U*ma análise comportamental da lei complementar nº 101, de 4 de maio de 2000*. Brasília, DF: Technopolitik.

Aguiar, J. C., Oliveira-Castro, J. M., & Gobbo, L. (2019). Rules as Basic Units of Sociocultural Selection. *Perspectives on Behavior Science*, *42*(4), 851-868.

Albert, H., & Maluschke, G. (2013). *O direito à luz do racionalismo crítico.* Brasília: Universa/UnB.

Albuquerque, L. C. e Silva, F. M. (2006). Efeitos da exposição a mudanças nas contingências sobre o seguir regras. *Psicologia: Teoria e Pesquisa*, *22*(1), 101-112.

Alqahtani, F. H. (2017). Developing an information security policy: a case study approach. *Procedia Computer Science, 124*, 691-697.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2015). Information security policy: A management practice perspective. In *Australasian Conference on Information Systems, 2015. International Conference on* (Vol. 1, pp. 1-13).

Al-Mayahi I. H., & Mansoor, S., P. (2014). Information security policy development. *Journal of Advanced Management Science, 2*(2), 135-139.

Associação Brasileira de Normas Técnicas. (2013a). *ABNT NBR ISO/IEC 27001 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos*. São Paulo: Autor.

Associação Brasileira de Normas Técnicas. (2013b). *ABNT NBR ISO/IEC 27002 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*. São Paulo: Autor.

Associação Brasileira de Normas Técnicas. (2018). *ABNT NBR ISO/IEC 31000 Gestão de riscos – Diretrizes*. São Paulo: Autor.

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145–159.

Boss, S. R., & Kirsch L. J. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings, 103*. Recuperado em 09/02/2018, de http://aisel.aisnet.org/icis2007/103

Braga, A. (2000). A gestão da informação. *Millenium, 19*. http://hdl.handle.net/10400.19/903

Britto, B. D. S. M., de Oliveira-Castro, J. M., Holanda, A. O., & dos Santos, T. L. (2018). Comportamento do Consumidor: Comparação entre Valor Relatado e Valor Gasto com Cartão de Crédito. *Revista Contabilidade, Gestão e Governança, 21*(3), 402-419.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 476-481). http://dx.doi.org/10.1109/CSE.2009.484

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Campos, V., & Pressler, N. (2018). Gerenciamento da imagem: A influência da comunicação integrada para agregar valor econômico à marca. *Revista Movendo Ideias, 20*(2), 38-44.

Catania, A. C. (1999). *Aprendizagem: comportamento, linguagem e cognição.* Porto Alegre: Artmed.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2012). Cartilha de segurança para internet, versão 4.0/CERT.br. São Paulo, SP: Comitê Gestor da Internet no Brasil. Recuperado em 30/10/2018, de http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. *Computer Standards & Interfaces, 34*(1), 124-134.

Davies, J., Foxall, G. R., & Pallister, J. (2002). Beyond the intention-behaviour mythology: An integrated model of recycling. *Marketing Theory, 2*, 29-113.

Decreto n. 9.637, de 26 de dezembro de 2018 (2018). Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput,inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Diário Oficial da União. Brasília, DF: Presidência da República.

do Nascimento, E. C. L. (2012). Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o Ministério do Desenvolvimento Agrário. *Universitas: Gestão e TI*, *2*(1). https://doi.org/10.5102/un.gti.v2i1.1681

Fazenda, R., & Fagundes, L. (2015). Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro. In *Anais Principais do XI Simpósio Brasileiro de Sistemas de Informação* (pp. 307-314).

Fazio, R. H., & Zanna, M. P. (1981). Direct experience and atitude-behavior consistency. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 14, pp. 161-202). New York, NY: Academic Press.

Flores, E. G., & Amaral, M. M. (2014). Mapeamento de processos utilizando a metodologia BPM: Uma ferramenta de suporte estratégico no desenvolvimento de sistemas em uma instituição federal de ensino superior. *Anais do EATI - Encontro Anual de Tecnologia da Informação e Semana Acadêmica de Tecnologia da Informação, 1,* 325-328.

Foxall, G. R. (1997). *Marketing psychology: The paradigm in the wings*. London, UK: Macmillan.

Foxall, G. R. (1998). Radical behaviorist interpretation: Generating and evaluating an account of consumer behavior. *The Behavior Analyst*, *21*(2), 321-354.

Foxall, G. R. (2002). Marketing's attitude problem – and how to solve it. *Journal of Customer Behaviour, 1*, 19-48.

Foxall, G. R. (2010). Invitation to consumer behavior analysis. *Journal of Organizational Behavior Management*, *30*(2), 92-109.

Foxall, G. R. (2017). *Advanced introduction to consumer behavior analysis*. Cheltenham, UK: Edward Elgar Publishing.

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, *2009* (2), 5-10.

Instrução Normativa n. 1, de 27 de maio de 2020 (2020). Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Diário Oficial da União. Brasília, DF: Gabinete de Segurança Institucional da Presidência da República.

Galizio, M. (1979). Contingency-shaped and rule-governed behavior: Instructional control of human loss avoidance. *Journal of the Experimental Analysis of Behavior, 31*, 53-70.

Hinson, G. (2013). Raising security awareness through marketing: Seven steps to promote your information security brand. *IsecT*. Recuperado em 19/02/2018, de http://www.noticebored.com/Raising_security_awareness_through_marketing.pdf

Holanda, A. O., Oliveira-Castro, J. M., & Silva, T. C. (2018). Análise de conteúdo das justificativas das propostas de emenda à constituição que tratam da maioridade penal. *Revista de Estudos Empíricos em Direito, 5(2),* 43-66.

Höne, K., & Eloff, J.H.P. (2002). Information security policy — what do international information security standards say?. *Computers & Security, 21*(5), 402-409. https://doi.org/10.1016/S0167-4048(02)00504-7

Imoniana, J. O. (2004). Validity of information security policy models. *Transinformação, 16*(3), 263-274.

Kelsen, H., & Knight, M. (1967). *Pure theory of law*. Berkeley, CA: University of California Press.

Kim, K., & Kim, J. (2017). An exploratory research about identifying security practices based on theory of planned behavior. *Far East Journal of Electronics and Communications*, *17*, 531-538.

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security, 70*, 663-674.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with brazilian users. *JISTEM - Journal of Information Systems and Technology Management: Revista de Gestão da Tecnologia e Sistemas de Informação, 13*(3), 479-496. http://dx.doi.org/10.4301/S1807-17752016000300007

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice, 13*(5), 66-80.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Lira, W. S., Cândido, G. A., Araújo, G. M. D., & Barros, M. A. D. (2008). A busca e o uso da informação nas organizações. *Perspectivas em Ciência da Informação, 13*(1), 166-183.

Luhmann, N. (1981). The improbability of communication. *International Social Science Journal, 33*(1), 122-132.

Machado, C. A., Cabral, L. A., Santos, J. P., & Motta, G. H. (2009). Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. In *Anais Principais do V Simpósio Brasileiro de Sistemas de Informação* (pp. 97-108). SBC.

Mann I. (2012). *Hacking the human: Social engineering techniques and security countermeasures.* Aldershot, UK: Gower Publishing.

Martins, A. B., & Santos, C. A. S. (2005). Uma metodologia para implantação de um sistema de gestão de segurança da informação. *JISTEM - Journal of Information Systems and Technology Management, 2*(2), 121-136.

Green, L., & Myerson, J. (2004). A discounting framework for choice with delayed and probabilistic rewards. *Psychological Bulletin, 130*(5), 769–79.

Meadows, D. H., & Wright, D. (2008). *Thinking in systems: A primer.* White River Junction, VT: Chelsea Green.

Michael, J. (2000). Implications and refinements of the establiishing operation concept. *Journal of Applied Behavioral Analysis, 33*(4), 401-410.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing.

Moreira, M. B., & Medeiros, C. A. (2007). *Princípios básicos de análise do comportamento*. Porto Alegre: Artmed.

Neto, J. B. M. R., da Cunha Tavares, J., & Hoffmann, S. C. (2019). *Sistemas de gestão integrados: qualidade, meio ambiente, responsabilidade social, segurança e saúde no trabalho*. São Paulo: Senac.

Oliveira, A. D. (2016). *Comportamento de gestores de recursos públicos: identificação de contingências previstas e vigentes relativas à prestação de contas*. Tese de doutorado. Universidade de Brasília.

Oliveira-Castro, J. M., & Foxall, G. R. (2005). Análise do Comportamento do Consumidor. In *Análise do Comportamento - Pesquisa, Teoria e Aplicação*. Porto Alegre: Artmed.

Oliveira-Castro, J. M., Oliveira, A., & Aguiar, J. C. (2018). Análise comportamental do direito: aplicações de sanções pelo Tribunal de Contas da União a gestores com contas irregulares. *Revista de Estudos Empíricos em Direito, 5(2),* 146-161.

Organisation for Economic Co-operation and Development. (2002). *Guidelines for the security of information systems and networks: towards a culture of security*. Recuperado em 15/10/2020, de http://www.oecd.org/dataoecd/16/22/15582260.pdf

Paracampo, C. C. P., & de Albuquerque, L. C. (2005). Comportamento controlado por regras: revisão crítica de proposições conceituais e resultados experimentais. *Interação em Psicologia, 9(2),* 227-237.

Park, M., & Chai, S. (2018). Internalization of information security policy and information security practice: A comparison with compliance. In *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4ª ed.). Upper Saddle River, NJ: Prentice Hall.

Pimenta, A. M. S., & Quaresma, R. F. C. (2016). A segurança dos sistemas de informação e o comportamento dos usuários. *JISTEM - Journal of Information Systems and Technology Management, 13*(3), 533-552. http://dx.doi.org/10.4301/S1807-17752016000300010

Rachlin, H. (2000). *The science of self-control*. Cambridge, MA: Harvard University Press.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" - a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Schauer, F. (2015). *The force of law*. Cambridge, MA: Harvard University Press.

Sêmola, M. (2014). *Gestão de segurança da informação: Uma visão executiva* (2ª ed.). Rio de Janeiro, RJ: Elsevier Editora Ltda.

Silva, P. (2008). A Imagem de uma Organização como Fator Imprescindível para o Sucesso. In *XXXI Congresso Brasileiro de Ciências da Comunicação. Rigor Proximidade Credibilidade Originalidade Independência Confiança Esforço Diversidade Abertura Espaço de Crítica Formalismo*.

Skinner, B. F. (1953). *Science and human behavior*. New York, NY: Macmillan.

Skinner, B. F. (1969). *Contingencies of reinforcement: A theoretical analysis*. Englewood Cliffs, NJ: Prentice-Hall.

Solana-González, P., Vanti, A. A., & Fontana, K. H. S. (2019). Multicriteria analysis of the compliance for the improvement of information security. *JISTEM-Journal of Information Systems and Technology Management*, *16*.

Solms, R. (1999). Information Security Systems: Why Standards are Important. *Information Management & Computer Security, 46*(8), 91-95.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36* (2), 215-225.

Snyman, D., & Kruger, H. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security, 25*(2), 152-164.

Talbot S., & Woodward A. (2009). Improving an organizations existing information technology policy to increase security. In *Proceedings of the 7th Australian Information Security Management Conference*. Perth, Western Australia.

Todorov, J. C. (2006). Laws and the complex control of behavior. *Behavior and Social Issues, 14*(2), 86-91.

Tribunal de Contas da União. (2012). *Boas práticas em segurança da informação* (4ª ed.). Recuperado em 02/03/2018, de http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 2.

Vieira, P. D. S. (2009). *Cultura de Segurança da informação: Um processo de mudança organizacional na Petrobrás*. Dissertação de Mestrado. RJ: Fundação Getúlio Vargas.

Von Solms, B. (2006). Information security – the fourth wave. *Computers & Security,25*(3), 165-168.

Wicker, A. W. (1969). Attitude versus actions: The relationship of verbal and overt behavioral responses to attitude objects. *Journal of Social Issues, 25*(4), 41-78.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Apêndice A

Análise detalhada de cada item da política de segurança da informação da organização participante selecionado para o escopo do Estudo 1, são eles:

1. É proibido aos usuários compartilhar sua senha de acesso à rede de computadores.
2. O uso não apropriado do acesso à internet e à intranet será passível de apuração de responsabilidade.
3. Os serviços de correio eletrônico corporativo serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.
4. O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.
    a. Por uso não apropriado, considera-se o envio de mensagens de correio eletrônico contendo:
        i. materiais obscenos, ilegais ou antiéticos;
        ii. materiais preconceituosos ou discriminatórios;
        iii. materiais caluniosos ou difamatórios;
        iv. propagandas com objetivos comerciais;
        v. listas de endereços eletrônicos dos usuários do correio eletrônico corporativo;
        vi. vírus ou qualquer outro programa malicioso;
        vii. material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;
        viii. material protegido por leis de propriedade intelectual;

ix. entretenimentos;

x. assuntos ofensivos;

xi. arquivos de áudio, vídeo, imagem ou texto que não sejam de interesse específico do trabalho;

xii. SPAM.

5. É responsabilidade do usuário do correio eletrônico corporativo:
    a. utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais;
    b. não permitir acesso de terceiros ao correio eletrônico por meio de sua senha.
6. Será vedada a cópia, em diretório da rede de computadores, dos seguintes tipos de arquivos:

    i. imagens, músicas e filmes de qualquer formato;

    ii. programas não homologados ou não licenciados;

    iii. programas de conteúdo prejudicial à segurança do ambiente computacional;

    iv. outros arquivos digitais cuja utilização não seja relacionada ao trabalho.

    b. Será autorizado o armazenamento de arquivos elencados no *caput*, desde que expressamente justificado.
7. Será responsabilidade do usuário da rede de computadores:
    a. utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais;

8. É vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.
9. É vedada a instalação e a utilização de programas e aplicativos de computador não homologados ou que descaracterizem os propósitos da organização ou que possam oferecer riscos à segurança dos ativos de informação ou danificar o ambiente tecnológico.
10. É vedada a conexão direta de equipamento ou dispositivo portátil particular na rede de computadores, sem a prévia verificação e autorização da equipe técnica de TI.
11. Os dispositivos portáteis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus e outros programas maliciosos ao serem conectados à rede ou a equipamento pertencente à organização.
12. Durante a execução das suas atividades profissionais, todos os usuários, seja presencialmente, seja em *home office*, devem observar as seguintes recomendações:
    a. guardar em local seguro informações sensíveis ou críticas que estejam armazenadas em papel, mídia eletrônica ou outro meio, especialmente quando o local de trabalho estiver desocupado;
    b. desligar ou hibernar os computadores ao final do expediente;
    c. bloquear os computadores com senha no caso de ausências curtas, por exemplo, para almoço, lanche e reuniões;
    d. utilizar somente equipamentos da própria organização na realização do trabalho presencial.

Item 1 - É proibido aos usuários compartilhar sua senha de acesso à rede de computadores.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Terceiros sem acesso aos recursos de TIC necessários à execução das atividades laborais.	Restrição da empresa na concessão de acessos. Possibilidade técnica de compartilhamento de senhas	Compartilhar senha para acesso à rede de computadores.	Facilitar o trabalho da equipe e maior produtividade.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 1. Descrição da contingência planejada no Item 1.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço de comodidade e produtividade obtida pelo compartilhamento de senhas.	A inobservância das disposições da PSI implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	Redução do compartilhamento de senhas.	Proteção da instituição de acessos não autorizados. Contribui para a responsabilização em caso de comprometimento de informações.

Figura 2. Explicitação das metas sociais relacionadas à contingência planejada no Item 1.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Terceiros sem acesso aos recursos de TIC necessários à execução das atividades laborais.	Restrição da empresa na concessão de acessos. Possibilidade técnica do compartilhamento das senhas.	Compartilhar senha para acesso à rede de computadores.	Reforço para o indivíduo, pois facilita a divisão de tarefas.	Aumenta o risco de exposição de informações de negócio e o risco na responsabilização por eventuais danos.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhar senha para acesso à rede de computadores.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor da aplicação da sanção reduz a probabilidade de compartilhamento de senhas.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Redução da ocorrência de compartilhamento de senhas entre os colaboradores	Maior proteção dos ativos de informação da organização e consequentemente dela própria

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhar senha para acesso à rede de computadores.	Responsabilização administrativa em caso de violação da PSI.	Redução de produtividade e comportamento de contracontrole do colaborador.

Figura 3. Identificação das premissas factuais relevantes (Item 1).

Item 2 - O uso não apropriado do acesso à internet e à intranet será passível de apuração de responsabilidade.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Colaborador privado de acesso a conteúdo reforçador.	Possibilidade técnica de acesso a sítios com conteúdo impróprio. Desconhecimento de riscos no acesso.	Acesso inapropriado à internet e intranet.	Acesso a conteúdo com efeito reforçador para o indivíduo.	A comprovação, por auditoria, do uso não apropriado implicará o bloqueio imediato da internet para o usuário e a comunicação à chefia imediata. A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 4. Descrição da contingência planejada no Item 2.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
O bloqueio da Internet e comunicação à chefia tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o acesso inapropriado.	A comprovação, por auditoria, do uso não apropriado implicará o bloqueio imediato da internet para o usuário e a comunicação à chefia imediata.	Bloqueio da Internet e comunicação à chefia imediata.	Redução de acessos inapropriados à Internet.	Proteção da instituição de mecanismos que possam comprometer a integridade, confidencialidade e disponibilidade de seus serviços de TI.
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o acesso inapropriado.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	Redução de acessos inapropriados à Internet.	Proteção da instituição de mecanismos que possam comprometer a integridade, confidencialidade e disponibilidade de seus serviços de TI.

Figura 5. Explicitação das metas sociais relacionadas à contingência planejada no Item 2.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Colaborador privado de acesso a conteúdo reforçador.	Possibilidade técnica de acesso a sítios com conteúdo impróprio. Desconhecimento de riscos no acesso.	Acesso inapropriado à internet e intranet.	Acesso a conteúdo com efeito reforçador para o indivíduo.	Risco de exposição dos ativos de informação e infraestrutura de TI.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Acesso inapropriado à internet e intranet.	Bloqueio da Internet e comunicação à chefia imediata.	(-) Inconformidade em relação à PSI Efeito punidor que reduz a probabilidade de acessos inapropriados.
	Responsabilização administrativa em caso de violação da PSI.	

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Bloqueio da Internet e comunicação à chefia imediata. Responsabilização administrativa em caso de violação da PSI.	Acesso inapropriado à internet e intranet.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Acesso inapropriado à internet e intranet.	Bloqueio da Internet e comunicação ao responsável pela unidade de lotação do usuário.	Redução de produtividade e comportamento de contracontrole do colaborador. Comportamento de contracontrole do responsável pela unidade.
Acesso inapropriado à internet e intranet.	Responsabilização administrativa em caso de violação da PSI.	Redução de produtividade e comportamento de contracontrole do colaborador.

Figura 6. Identificação das premissas factuais relevantes (Item 2).

Item 3 - Os serviços de correio eletrônico corporativo serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Dificuldade do colaborador em gerir suas mensagens eletrônicas em diversas soluções.	Possibilidade técnica de uso do correio eletrônico para os diversos fins. Grande número de mensagens eletrônicas em soluções diversas. Difícil monitoramento.	Uso do correio eletrônico para assuntos particulares.	Facilidade no gerenciamento e envio de mensagens eletrônicas.	O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade.

Figura 7. Descrição da contingência planejada no Item 3.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o uso inadequado do correio eletrônico.	O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso do correio eletrônico apenas para atividades laborais.	Otimização do uso dos recursos de TI.

Figura 8. Explicitação das metas sociais relacionadas à contingência planejada no Item 3.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Dificuldade do colaborador em gerir suas mensagens eletrônicas em diversas soluções.	Possibilidade técnica de uso do correio eletrônico para os diversos fins. Grande número de mensagens em soluções diversas.	Uso do correio eletrônico para assuntos particulares.	Facilidade no gerenciamento e envio de mensagens eletrônicas.	Possível aumento de demanda infraestrutura de TI para suportar o serviço de correio eletrônico.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso do correio eletrônico para assuntos particulares.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Efeito punidor que reduz a probabilidade de uso do correio eletrônico para assuntos particulares.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso do correio eletrônico para assuntos particulares.	Otimização do uso dos recursos de TI

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso do correio eletrônico para assuntos particulares.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso de serviços de correio eletrônico externos para atividades laborais; Risco de comprometimento da confidencialidade da informação.

Figura 9. Identificação das premissas factuais relevantes (Item 3).

Item 4 - O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Maior esforço do colaborador em encaminhar mensagens eletrônicas a outros colaboradores usando outra solução de e-mail. (Inexistência de catálogo de e-mail com endereços dos colegas)	Possibilidade técnica de uso do correio eletrônico para os diversos fins. Existência de catálogo corporativo com a lista de endereços.	Uso inapropriado do correio eletrônico corporativo.	Maior facilidade no envio de mensagens eletrônicas.	O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.

Figura 10. Descrição da contingência planejada no Item 4.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o uso inadequado do correio eletrônico.	O uso não apropriado do correio eletrônico corporativo é passível de apuração de responsabilidade do usuário.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso do correio eletrônico apenas para atividades laborais.	Otimização do uso dos recursos de TI. Controle de distribuição de conteúdo potencialmente malicioso contribui para a proteção da instituição.

Figura 11. Explicitação das metas sociais relacionadas à contingência planejada no Item 4.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Maior esforço do colaborador em encaminhar mensagens eletrônicas a outros colaboradores usando outra solução de e-mail (Estímulo aversivo).	Possibilidade técnica de uso do correio eletrônico para os diversos fins. Existência de catálogo corporativo com a lista de endereços.	Uso inapropriado do correio eletrônico corporativo.	Maior facilidade no envio de mensagens eletrônicas.	Possível aumento de demanda infraestrutura de TI para suportar o serviço de correio eletrônico. Risco de distribuição de conteúdo malicioso.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso inapropriado do correio eletrônico corporativo.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Efeito punidor que reduz a probabilidade de uso inapropriado do correio eletrônico.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso inapropriado do correio eletrônico corporativo.	Dificulta a distribuição de conteúdo malicioso. Otimização da infraestrutura de TI

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso inapropriado do correio eletrônico corporativo.	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	Uso de serviços de correio eletrônico externos para atividades laborais. Comportamento de contracontrole do colaborador.

Figura 12. Identificação das premissas factuais relevantes (Item 4).

Item 5 - É responsabilidade do usuário do correio eletrônico corporativo: utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais; e não permitir acesso de terceiros ao correio eletrônico por meio de sua senha

Observação: Em relação ao uso para objetivos e funções inerentes às suas atribuições, a análise comportamental da regra foi realizada nos termos da análise feita para a Item 3. Logo, análise da quinta regra restringe-se ao compartilhamento da senha do serviço de correio eletrônico.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Compartilhar a senha do correio eletrônico corporativo.	REFORÇO	SANÇÃO
Membros da equipe sem acesso a mensagens eletrônicas necessárias à execução das atividades da unidade prejudicando a produtividade da equipe.	Possibilidade técnica de compartilhamento da senha. Mensagens corporativas de acesso restrito a alguns colaboradores.		Facilitar o trabalho da equipe e maior produtividade.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 13. Descrição da contingência planejada no Item 5.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL	Responsabilização administrativa em caso de uso inapropriado do correio eletrônico.	IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o compartilhamento da senha de correio eletrônico.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.		Redução do compartilhamento de senhas.	Proteção da instituição de acessos não autorizados. Contribui para a responsabilização em caso de comprometimento de informações.

Figura 14. Explicitação das metas sociais relacionadas à contingência planejada no Item 5.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Membros da equipe sem acesso a mensagens eletrônicas necessárias à execução das atividades da unidade prejudicando a produtividade da equipe.	Possibilidade técnica de compartilhamento da senha. Mensagens corporativas de acesso restrito a alguns colaboradores.	Compartilhar a senha do correio eletrônico corporativo.	Facilitar o trabalho da equipe e maior produtividade.	Aumenta o risco de exposição de informações de negócio e o risco na responsabilização por eventuais danos.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhar a senha do correio eletrônico corporativo.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor reduz a probabilidade de compartilhamento de senhas.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Redução da ocorrência de compartilhamento de senhas entre os colaboradores	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Compartilhar a senha do correio eletrônico corporativo.	Responsabilização administrativa em caso de violação da PSI.	Redução de produtividade e comportamento de contracontrole dos colaboradores.

Figura 15. Identificação das premissas factuais relevantes (Item 5).

Item 6 - Será vedada a cópia, em diretório da rede de computadores, dos seguintes tipos de arquivos.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Necessidade de compartilhar arquivos. Necessidade de realizar cópia de segurança de arquivos pessoais	Possibilidade técnica de usar diretório de rede. Rotinas automáticas de cópias de segurança dos serviços de diretório.	Uso inadequado dos diretórios da rede de computadores.	Maior facilidade no compartilhamento de arquivos. Menor esforço para a realização de cópias de segurança dos arquivos.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 16. Descrição da contingência planejada no Item 6.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o uso inadequado do diretório de rede.	A inobservância deste normativo implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	Menor demanda para o serviço e necessidade de investimentos em infraestrutura de TI. No caso de programas não licenciados, reduz ações de pirataria e eventual responsabilização da organização. No caso de programas maliciosos, a contingência dificulta sua propagação.	Controle de distribuição de programas maliciosos contribui para a proteção da instituição. Otimização do uso dos recursos de TI

Figura 17. Explicitação das metas sociais relacionadas à contingência planejada no Item 6.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Necessidade de compartilhar arquivos. Necessidade de realizar cópia de segurança de arquivos pessoais	Possibilidade técnica de usar diretório de rede. Facilidade de uso do diretório.	Uso inadequado dos diretórios da rede de computadores.	Maior facilidade no compartilhamento de arquivos. Menor custo para cópias de segurança dos arquivos.	Possível aumento de demanda infraestrutura de TI para suportar o serviço de diretório de rede. Risco de facilitar a distribuição de programas maliciosos. Risco de responsabilização da empresa por pirataria.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso inadequado dos diretórios da rede de computadores.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor que reduz a probabilidade de uso inapropriado do diretório de rede.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Uso inapropriado do diretório de rede.	Dificulta a distribuição de conteúdo malicioso. Otimização da infraestrutura de TI

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Uso inapropriado do diretório de rede.	Responsabilização administrativa em caso de violação da PSI.	Uso excessivo de serviços de armazenamento em nuvem para o compartilhamento de arquivos.

Figura 18. Identificação das premissas factuais relevantes (Item 6).

Item 7 - Será responsabilidade do usuário da rede de computadores utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Usabilidade limitada em outros serviços como de armazenamento em nuvem ou e-mail. Necessidade de cópia de segurança.	Possibilidade técnica de uso do diretório de rede. Difícil monitoramento.	Armazenamento de arquivos particulares nos diretórios de rede.	Facilidade no gerenciamento dos arquivos. Obtenção de cópia de segurança.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 19. Descrição da contingência planejada no Item 7.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com o armazenamento de arquivos particulares nos diretórios de rede.	Art. 86. A inobservância das disposições deste Ato implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	Uso do diretório de rede apenas para armazenar arquivos referentes às atividades laborais implica em menor demanda para o serviço e, logo, necessidade de investimentos.	Otimização do uso dos recursos de TI.

Figura 20. Explicitação das metas sociais relacionadas à contingência planejada no Item 7.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Armazenamento de arquivos particulares nos diretórios de rede.	COLABORADOR	ORGANIZAÇÃO
Usabilidade limitada em outros serviços como de armazenamento em nuvem ou e-mail. Necessidade de cópia de segurança.	Possibilidade técnica de uso do diretório de rede.		Facilidade no gerenciamento dos arquivos. Obtenção de cópia de segurança.	Possível aumento de demanda infraestrutura de TI para suportar o serviço de diretório de rede.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Armazenamento de arquivos particulares nos diretórios de rede.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor que reduz a probabilidade de uso do diretório de rede para armazenagem de arquivos particulares.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Armazenamento de arquivos particulares nos diretórios de rede.	Otimização da infraestrutura de TI

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Armazenamento de arquivos particulares nos diretórios de rede.	Responsabilização administrativa em caso de violação da PSI.	Comportamento de contracontrole; Uso de serviços de armazenamento em nuvem com potencial para o vazamento de informações por descuido.

Figura 21. Identificação das premissas factuais relevantes (Item 7).

Item 8 - É vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Programas disponibilizados não atendem às necessidades particulares dos usuários.	Possibilidade técnica de instalação do programa. Disponibilidade do programa para instalação	Instalação de programas não licenciados.	Acesso a recursos até então indisponíveis.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 22. Descrição da contingência planejada no Item 8.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com a instalação irregular de programas.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	Redução das tentativas de instalação irregular de programas.	Otimização do uso dos recursos de TI. Proteção da imagem da instituição (Responsabilização da organização por uso ilegal de programas).

Figura 23. Explicitação das metas sociais relacionadas à contingência planejada no Item 8.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Programas contratados/disponibilizados pela instituição não atendem às necessidades particulares dos usuários.	Possibilidade técnica de instalação do programa. Disponibilidade do programa para instalação.	Instalação de programas não licenciados.	Acesso a recursos até então indisponíveis.	Possível aumento de demanda infraestrutura de TI para suportar os novos programas. Custos para regularização. Responsabilização por pirataria

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Instalação de programas não licenciados.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor que reduz a probabilidade da instalação irregular de programas.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Instalação de programas não licenciados.	Otimização do uso dos recursos de TI. Proteção da imagem da organização.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Instalação de programas não licenciados.	Responsabilização administrativa em caso de violação da PSI.	Comportamento de contracontrole;

Figura 24. Identificação das premissas factuais relevantes (Item 8).

Item 9 - É vedada a instalação e a utilização de programas e aplicativos de computador não homologados ou que descaracterizem os propósitos da organização ou que possam oferecer riscos à segurança dos ativos de informação ou danificar o ambiente tecnológico.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Programas disponibilizados não atendem às necessidades particulares dos usuários.	Possibilidade técnica de instalação do programa. Disponibilidade do programa para instalação	Instalação de programas não homologados.	Acesso a recursos até então indisponíveis.	O usuário será responsabilizado pela instalação ou pela execução não autorizada de programa não homologado, considerando-se a possibilidade de dano à organização.

Figura 25. Descrição da contingência planejada no Item 9.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com a instalação irregular de programas.	O usuário será responsabilizado pela instalação ou pela execução não autorizada de programa não homologado, considerando-se a possibilidade de dano à organização.	Responsabilização administrativa em caso de instalação ou execução não autorizada de programa não homologado.	Redução da probabilidade de instalação de programas com potencial de danificar as instalações de TI.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

Figura 26. Explicitação das metas sociais relacionadas à contingência planejada no Item 9.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Programas disponibilizados não atendem às necessidades particulares dos usuários.	Possibilidade técnica de instalação do programa. Disponibilidade do programa para instalação	Instalação de programas não homologados.	Acesso a recursos até então indisponíveis.	Possível aumento de demanda infraestrutura de TI para suportar os novos programas. Risco de uso de programas com potencial danoso para a organização.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Instalação de programas não homologados.	Responsabilização administrativa em caso de instalação ou execução não autorizada de programa não homologado.	Efeito punidor que reduz a probabilidade da instalação irregular de programas.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de instalação ou execução não autorizada de programa não homologado.	Instalação de programas não homologados.	Maior proteção dos ativos de informação da organização e consequentemente dela própria. Otimização do uso dos recursos de TI.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Instalação de programas não homologados.	Responsabilização administrativa em caso de instalação ou execução não autorizada de programa não homologado.	Comportamento de contracontrole dos colaboradores.

Figura 27. Identificação das premissas factuais relevantes (Item 9).

Item 10 - É vedada a conexão direta de equipamento ou dispositivo portátil particular na rede de computadores, sem a prévia verificação e autorização da equipe técnica de TI.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Programas disponibilizados nos computadores do órgão não atendem às necessidades particulares dos usuários. Restrições (bloqueios de recursos) nos equipamentos do órgão.	Possibilidade técnica de conexão à rede de computadores.	Conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Acesso a recursos indisponíveis. Comodidade na execução de tarefas.	A não observância desse dispositivo implicará a responsabilizaçã o do usuário que efetuar a conexão

Figura 28. Descrição da contingência planejada no Item 10.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido com uso de equipamento pessoal.	A não observância desse dispositivo implicará a responsabilização do usuário que efetuar a conexão	Responsabilização administrativa em caso de conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Redução da probabilidade conexão de dispositivos potencialmente danosos à rede de computadores.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

Figura 29. Explicitação das metas sociais relacionadas à contingência planejada no Item 10.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		COLABORADOR	ORGANIZAÇÃO
Programas disponibilizados nos computadores do órgão não atendem às necessidades particulares dos usuários. Restrições (bloqueios de recursos) nos equipamentos do órgão.	Possibilidade técnica de conexão à rede de computadores.	Conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Acesso a recursos indisponíveis. Comodidade na execução de tarefas.	Risco de vazamento das informações organizacionais e de comprometimento da disponibilidade dos recursos de TI.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Responsabilização administrativa em caso de conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Efeito punidor que reduz a probabilidade de conexão de dispositivos particulares.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Maior proteção da rede de computadores e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Responsabilização administrativa em caso de conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores.	Comportamento de contracontrole: Instalação de programas não autorizados em equipamentos do órgão; instalação de programas para contornar controles estabelecidos.

Figura 30. Identificação das premissas factuais relevantes (Item 10).

Item 11 - Os dispositivos portáteis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus e outros programas maliciosos ao serem conectados à rede ou a equipamento pertencente à organização.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO		REFORÇO	SANÇÃO
Estímulo aversivo – demora para realizar a verificação.	Possibilidade técnica de não verificar.	Não verificação de existência de programas maliciosos em dispositivos portáteis de armazenamento.	Agilidade na execução da tarefa.	A não observância deste dispositivo implicará a responsabilizaçã o do usuário que efetuar a conexão

Figura 31. Descrição da contingência planejada no Item 11.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao reforço obtido pela agilidade na execução da tarefa.	A não observância deste dispositivo implicará a responsabilização do usuário que efetuar a conexão	Responsabilização administrativa caso não seja verificada a existência de programas maliciosos em dispositivos portáteis de armazenamento.	Redução da probabilidade de uso de dispositivos de armazenamento móveis sem prévia verificação.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

Figura 32. Explicitação das metas sociais relacionadas à contingência planejada no Item 11.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Não verificação de existência de programas maliciosos em dispositivos portáteis de armazenamento.	COLABORADOR	ORGANIZAÇÃO
Estímulo aversivo – demora para realizar a verificação.	Possibilidade técnica de não verificar.		Agilidade na execução da tarefa.	Risco de introdução de programas maliciosos na rede corporativa.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Não verificação de existência de programas maliciosos em dispositivos portáteis de armazenamento.	Responsabilização administrativa caso não seja verificada a existência de programas maliciosos em dispositivos portáteis de armazenamento.	Efeito punidor que reduz a probabilidade de uso de dispositivos de armazenamento móveis sem prévia verificação.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa caso não seja verificada a existência de programas maliciosos em dispositivos portáteis de armazenamento.	Não verificação de existência de programas maliciosos em dispositivos portáteis de armazenamento.	Maior proteção da rede de computadores da organização e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Não verificação de existência de programas maliciosos em dispositivos portáteis de armazenamento.	Responsabilização administrativa caso não seja verificada a existência de programas maliciosos em dispositivos portáteis de armazenamento.	Comportamento de contracontrole: Uso de outras soluções de armazenamento (e.g., serviços em nuvem) sem a exigência de verificação.

Figura 33. Identificação das premissas factuais relevantes (Item 11).

Item 12 Durante a execução das suas atividades profissionais, todos os usuários, seja presencialmente, seja em *home office*, devem observar as seguintes recomendações.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Expor informações sensíveis através do acesso físico ao posto de trabalho.	REFORÇO	SANÇÃO
Estímulo aversivo – procedimentos atrasam as atividades rotineiras.	Possibilidade de não realizar. Difícil monitoramento e auditoria.		Menos esforço na realização de atividades rotineiras.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.

Figura 34. Descrição da contingência planejada no Item 12.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL	Responsabilização administrativa em caso de violação da PSI.	IMEDIATA	MEDIATA
A eventual responsabilização administrativa tende a ter efeito aversivo de maior magnitude quando comparado ao custo dos cuidados indicados.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.		Redução da probabilidade de descuido na manipulação de informações sensíveis no posto de trabalho.	Maior proteção dos ativos de informação da organização e consequentemente dela própria.

Figura 35. Explicitação das metas sociais relacionadas à contingência planejada no Item 12.

PROBABILIDADE DE OCORRÊNCIA DO COMPORTAMENTO INDESEJADO

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Expor informações sensíveis através do acesso físico ao posto de trabalho.	COLABORADOR	ORGANIZAÇÃO
Estímulo aversivo – procedimentos atrasam as atividades rotineiras.	Possibilidade de não realizar. Difícil monitoramento e auditoria.		Menos esforço na realização de atividades rotineiras.	Risco de divulgação de informações sensíveis.

POTENCIAL EFICÁCIA DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Expor informações sensíveis através do acesso físico ao posto de trabalho.	Responsabilização administrativa em caso de violação da PSI.	Efeito punidor que reduz a probabilidade de descuido no posto de trabalho.

NEXO CAUSAL ENTRE A CONDUTA SANCIONADA E A META SOCIAL MEDIATA

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Responsabilização administrativa em caso de violação da PSI.	Expor informações sensíveis através do acesso físico ao posto de trabalho.	Maior proteção das informações organizacionais e consequentemente dela própria.

POSSÍVEIS CONSEQUÊNCIAS SOCIAIS INDESEJÁVEIS DA APLICAÇÃO DA SANÇÃO

ANTECEDENTES	PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS
Expor informações sensíveis através do acesso físico ao posto de trabalho.	Responsabilização administrativa em caso de violação da PSI.	Comportamento de contracontrole.

Figura 36. Identificação das premissas factuais relevantes (Item 12).

Apêndice B

Roteiro de entrevista com os coordenadores.

1. Quais os critérios adotados para notificar uma suspeita de incidente de segurança da informação?

2. Como os incidentes de segurança da informação são tratados no âmbito da organização?

3. As violações da política de segurança da informação (PSI) que são identificadas são usualmente tratadas como incidentes de segurança da informação?

4. Quais são as consequências típicas quando constatado um incidente de segurança da informação?

Roteiro de entrevista com o supervisor da Seção de Gestão de Segurança da Informação.

1. Quais os critérios adotados para a convocação da Equipe de Resposta e Tratamento de Incidentes de Segurança da Informação (ETIR)? Houve alguma reversão de decisão de não convocação da ETIR?

2. Quais requisitos para que as eventuais violações da PSI sejam tratadas como incidentes de segurança da informação?

3. Quais os principais argumentos debatidos no CGSI para proposição de aplicação ou não de sanções às condutas desconformes à PSI?

4. Como são tratados os incidentes de segurança da informação no âmbito da organização?

5. Existe processo de gestão de incidentes de segurança da informação formalmente instituído?

6. As violações da política de segurança da informação (PSI) que são identificadas são todas tratadas como incidentes de segurança da informação?

7. O processo de gestão de incidentes de segurança da informação pode deflagrar um processo disciplinar, isto é, a responsabilização administrativa? Como é a interação desses processos?

8. Qual o papel do Comitê Gestor de Segurança da Informação (CGSI) no tratamento dos incidentes de SI?

9. Todos os incidentes de segurança da informação são submetidos ao CGSI?

10. A partir de quando os incidentes de segurança da informação passaram a ter um tratamento padronizado? Quantos incidentes foram registrados e qual o tratamento dado?

11. Mesmo que não tratadas como incidentes, quais tipos de violações da PSI ocorrem com mais frequência? É possível quantificar (existe na base de dados de chamados)?

12. Quais sanções já foram aplicadas em decorrência de violações da PSI (Não há necessidade de identificar o colaborador responsabilizado)? Quantas sanções foram aplicadas?

13. Quais as violações mais sancionadas?

14. Quantos processos disciplinares foram instaurados ou sindicâncias instaladas para apurar violações da PSI?

Apêndice C

Efeitos de procedimentos de controles de segurança da informação sobre a conduta de colaboradores: Uma análise comportamental

Por favor, forneça abaixo seu e-mail corporativo.

* Required

Email address *

Your email

Termo de Consentimento Livre e Esclarecido. *

O(a) Senhor(a) está sendo convidado(a) a participar do projeto de pesquisa "Efeitos de procedimentos de controles de segurança da informação sobre a conduta de colaboradores: Uma análise comportamental", sob a responsabilidade do pesquisador Rafael Almeida de Paula, aluno de doutorado do curso de Pós-Graduação em Ciências do Comportamento do Departamento de Processos Psicológicos Básicos - Instituto de Psicologia da Universidade de Brasília, sob a orientação do Prof. Jorge Mendes de Oliveira-Castro Neto. A pesquisa destina-se a investigar a eficiência dos procedimentos que usualmente são adotados pelas organizações para tratar questões comportamentais dos colaboradores no contexto da gestão da segurança da informação. Nessa esteira, a presente pesquisa adota um arcabouço teórico sistemático para a análise dessas questões comportamentais e objetiva, em última instância, a mitigação dos riscos organizacionais. Solicitamos sua autorização para que suas respostas possam ser incluídas na base de dados da presente pesquisa. Esclarecemos que sua participação é voluntária e asseguramos que, ao longo da pesquisa, bem como na publicação dos seus resultados, será mantido o sigilo sobre a sua identidade e da organização que representa. Os resultados da pesquisa serão divulgados na Universidade de Brasília podendo ser publicados posteriormente. Os dados e materiais serão utilizados somente para esta pesquisa e ficarão sob a guarda do pesquisador por um período de cinco anos, e serão destruídos após esse prazo. Se o(a) Senhor(a) tiver qualquer dúvida em relação à pesquisa, por favor contate o pesquisador responsável, Rafael Almeida de Paula, por meio do telefone (61) 9 9968-3536 ou através do e-mail rafael.paula@gmail.com. Este projeto foi aprovado pelo Comitê de Ética em Pesquisa em Ciências Humanas e Sociais (CEP/CHS) da Universidade de Brasília. O CEP é composto por profissionais de diferentes áreas cuja função é defender os interesses dos participantes da pesquisa em sua integridade e dignidade e contribuir no desenvolvimento da pesquisa dentro de padrões éticos. As dúvidas com relação à concordância do TCLE ou aos direitos do participante da pesquisa podem ser esclarecidos pelo telefone (61) 3107-1592 ou do e-mail cep_chs@unb.br, no horário de atendimento de 14:00hs às 20:00hs, de segunda a sexta-feira. Caso concorde com a participação, pedimos que assinale abaixo a sua concordância.

□ Sim, eu autorizo a inclusão das minhas respostas na base de dados da pesquisa, uma vez que está assegurado meu anonimato e da minha instituição.

□ Não, eu não autorizo a inclusão das minhas respostas na base de dados desta pesquisa.

Dados da organização

A empresa conta, aproximadamente, com quantos usuários internos de TI (Ex.: colaboradores da organização, terceirizados e estagiários)?

- Menos de 500 usuários internos
- Entre 500 e 1000 usuários internos
- Acima de 1000 usuários internos

Há quantos anos a empresa tem uma política de segurança da informação formalizada?

- Menos de 5 anos
- Entre 5 e 10 anos
- Mais de 10 anos

A empresa adota a prática de registrar e monitorar as atividades de seus usuários internos com vistas à detectar e evidenciar eventuais violações de sua política de segurança da informação.

- Não
- Sim, ocorre o registro e monitoramento das atividades dos usuários internos.
- Sim, ocorre o registro e o monitoramento das atividades e a prática está prevista na própria política de segurança da informação.

Caso afirmativo, qual opção abaixo se aproxima mais da forma como os registros das atividades dos usuários internos são usados na identificação e tratamento das violações da PSI?

Considere apenas violações causadas pelos usuários internos e tratadas no sentido de aplicar as consequências previstas nos normativos da organização.

De forma geral, os registros são usados em atividades de auditoria e/ou para a produção de evidências quando um incidente de segurança da informação está sendo tratado.

- 1
- 2
- 3
- 4
- 5

De forma pró-ativa. Os registros das atividades frequentemente dão início ao processo de tratamento das violações da PSI.

Existe processo definido para o tratamento dos incidentes de segurança da informação?

Obs.: O processo não precisa estar necessariamente formalizado, mas os atores sabem seus papéis e responsabilidades.

- Sim
- Não

Caso afirmativo, explique em linhas gerais seu funcionamento, em especial quanto às possíveis consequências para os colaboradores por eventuais violações da política de segurança da informação.

A aplicação da política de segurança da informação no âmbito da organização

Existe alguma iniciativa da organização em premiar os colaboradores por observarem a política de segurança da informação?

□ Sim
□ Não

Caso afirmativo, explique em linhas gerais como funciona essa premiação.

Em termos de categorias de comportamentos indesejados pela organização, por favor indique nas questões abaixo a frequência de sua ocorrência, considerando os últimos cinco anos.

A frequência indicada deve considerar as condutas que foram exitosas, ou seja, os eventuais mecanismos de controle implementados pela organização não foram suficientes para impedi-las, bem como as condutas mal sucedidas, ou seja, as tentativas sem êxito em decorrência da implementação dos mecanismos de controle implementados pela organização.

Compartilhamento de senhas: colaborador compartilhar senha de acesso aos recursos informatizados com terceiros.

Exemplos: compartilhamento de senhas de correio eletrônico, sistemas corporativos, rede corporativa, dentre outros.

Nunca
□ 1
□ 2
□ 3
□ 4
□ 5
Muito frequentemente

Uso inadequado dos recursos de TI: utilização dos recursos disponibilizados com fins particulares, em atividades ilegais ou que possam comprometer a segurança das informações do Órgão.

Exemplos: acessos (ou tentativas de acessos) a sites com conteúdo proibido; uso do e-mail corporativo para atividades particulares ou de forma inapropriada, como envio de materiais obscenos, ilegais, preconceituosos, etc; cópia de arquivos na rede corporativa não relacionados ao trabalho como filmes, fotos, programas não homologados ou licenciados ou de conteúdo prejudicial à segurança da ambiente computacional.

Nunca
□ 1
□ 2
□ 3
□ 4
□ 5
Muito frequentemente

Comprometimento do ambiente de tecnologia da informação do Órgão (físico e/ou lógico): condutas que possam comprometer a integridade do ambiente de TI, seja por intervenções físicas (e.g., uso de equipamentos que não são do órgão) ou lógicas (e.g., instalação de programas não homologados e uso de dispositivos móveis para manipulação de arquivos).

Exemplos: conexão de notebook particular na rede corporativa, uso de pendrive sem verificação de antivírus/solução de proteção de desktop, instalação de programas não licenciados ou não homologados pela organização

Nunca
□ 1
□ 2
□ 3
□ 4
□ 5
Muito frequentemente

Descuidos no posto de trabalho: ações que possam comprometer a segurança das informações organizacionais mediante acesso físico ao posto de trabalho do colaborador.

Exemplo: informações sigilosas impressas na mesa do colaborador "política de mesa limpa", estação de trabalho "destravada" ao se ausentar do posto de trabalho, etc...

Nunca
□ 1
□ 2
□ 3
□ 4
□ 5
Muito frequentemente

Caso existam condutas que não se encaixam em uma das quatro categorias comportamentais sugeridas no questionário, por favor descreva-as abaixo e indique a sua frequência (1 a 5).

Nos últimos cinco anos, quais tipos de sanções foram aplicadas com mais frequência nas ocorrências de violações da política de segurança da informação da organização?

Considere sanção qualquer tipo de consequência que possa ser percebida como sancionatória ou corretiva pelo usuário que violou a política de segurança da informação.

	Não ocorreu	Raramente	Frequentemente	Sempre
Advertência	□	□	□	□
Suspensão	□	□	□	□
Demissão	□	□	□	□
Outra(s)	□	□	□	□

Caso tenha assinalado na questão anterior algum outro tipo de sanção, por favor, explique abaixo.

Quantas violações da PSI foram tratadas nos últimos cinco anos?
Considere apenas violações causadas pelos usuários internos e tratadas no sentido de aplicar as consequências previstas nos normativos da organização.

- Nenhuma
- Até 20
- Entre 21 e 50
- Acima de 50 violações.

A organização tem a prática de aplicar sanções aos colaboradores que violam a PSI?

Nunca

- 1
- 2
- 3
- 4
- 5

Sempre

Nos últimos cinco anos, quais as principais condutas dos usuários internos sancionadas com maior frequência?
Trata-se de condutas que violaram a PSI e sofreram as consequências previstas nos normativos internos da organização.

Em relação às afirmações abaixo, indique seu grau de concordância, sendo 1 para "discordo plenamente" e 5 para "concordo plenamente".
Mesmo com a formalização da PSI houve a necessidade de investimentos em soluções de segurança da informação para impedir condutas dos usuários que violam os requisitos de segurança da informação da organização.
Exemplos: soluções de filtro de conteúdo; soluções que bloqueiam recursos nas estações de trabalho, como USB e permissão para instalação de aplicativos; filtros de e-mail, etc. Obs.: Entenda investimentos como também de tempo e recursos humanos, por exemplo, na implantação de soluções baseada em software livre (sem custos).

- 1
- 2
- 3
- 4
- 5

As violações da política de segurança da informação, usualmente, são prontamente tratadas na esfera técnica, fato que reduz seus impactos e contribui para a percepção de baixa gravidade pela organização.

- 1
- 2
- 3
- 4
- 5

Muito obrigado!

Agradecemos a sua participação! Por favor indique abaixo se deseja receber os resultados consolidados dessa pesquisa.

- Sim, desejo receber os resultados consolidados desta pesquisa.