Disponível em
http://www.desafioonline.ufms.br
Desafio Online, Campo Grande, v.9, n.1, Jan./Abr. 2021

ANÁLISE COMPORTAMENTAL DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO – UM ESTUDO DE CASO

BEHAVIORAL ANALYSIS OF INFORMATION SECURITY POLICIES - A CASE STUDY

Rafael Almeida de Paula
Universidade de Brasília, DF, Brasil
rafael.paula@gmail.com
https://orcid.org/0000-0001-7424-1171

Jorge Mendes de Oliveira-Castro
Universidade de Brasília
jorge.oliveiracastro@gmail.com
https://orcid.org/0000-0002-5438-7330

Resumo

Um dos grandes desafios na gestão da segurança da informação nas organizações é o tratamento dos riscos relacionados ao comportamento de seus colaboradores. A principal medida adotada é a definição de políticas de segurança da informação, cuja maioria dos estudos na literatura restringe-se aos aspectos formais de sua elaboração ou aborda as ações de conscientização como instrumentos de sua implantação. Nesse trabalho, propõe-se um novo modelo para tratar esses riscos, mediante adoção do arcabouço teórico estabelecido pela análise do comportamento, em especial, a teoria analítico-comportamental do direito. Para a sua consecução, foram identificados, descritos e analisados três exemplos de contingências planejadas na política de segurança da informação de um órgão da administração pública federal e demonstrada a viabilidade da adaptação proposta. Os resultados evidenciam a necessidade de uma análise funcional dos comportamentos considerados indesejados pelas organizações quando da definição da política de segurança da informação e sugerem um novo caminho baseado na análise comportamental das políticas de segurança da informação, bem como dos sistemas de gestão de segurança da informação para a mitigação dos riscos organizacionais.

Peer Review under the responsibility of Escola de Administração e Negócios da Universidade Federal do Mato Grosso do Sul ESAN/UFMS.

Palavras-chave: política; segurança; informação; comportamento; usuário.

Abstract

One of the major challenges in managing information security in organizations is the treatment of risks related to the behavior of their employees. The main measure adopted by organizations to address the risks that involves employee's behavior is the definition of information security policies. However, it occurs that most of the studies in the literature are restricted to the formal aspects of the elaboration of the policies or approached the awareness programs as instruments of its implantation. In this work, a new model is proposed to deal with these risks, by adopting the theoretical framework established by the behavior analysis, especially the theory presented by the Behavior Analysis of Law. To achieve this, three examples of planned contingencies in the information security policy of a federal public administration agency were identified, described and analyzed, demonstrating the feasibility of the proposed adaptation. The results highlights the need for a functional analysis of behaviors considered unwanted by the organizations when defining it´s information security policy and suggests a new path based on behavioral analysis of information security policies, as well as of information security management systems for mitigating organizational risks.

Keywords: *policy; information; security; behavior; user.*

1. Introdução

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 (Associação Brasileira de Normas Técnicas [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 (PSI) 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).

Acerca disso, há que se destacar que boa parte dos estudos na literatura concentram-se na forma de se definir uma PSI e seu conteúdo (e.g., Höne & Eloff, 2002; Talbot & Woodward, 2009; Al-Mayahi & Mansoor, 2014) e indicam que existe certa semelhança entre elas por observarem os padrões e as boas práticas (Imoniana, 2004). Esses estudos também apontam a necessidade de realizar ações de conscientização (i.e., a divulgação de informações acerca dos cuidados necessários para a proteção da organização) como mecanismo para a implementação das PSIs, ou seja, como forma de controlar o comportamento de seus colaboradores e assegurar a observação da PSI estabelecida.

Vários estudos destacam a importância das ações de conscientização para a implantação de uma PSI nas organizações (e.g., Hinson, 2013; Klein & Luciano, 2016; Snyman & Kruger, 2017). Entretanto, as conclusões desses estudos baseiam-se nas declarações dos participantes, logo, necessitam de uma confirmação empírica tendo em vista que o comportamento declarado pode não coincidir com o comportamento executado (Davies, Foxall & Pallsiter, 2002; Foxall, 2002; Oliveira-Castro & Foxall, 2005). Convém destacar que 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 executado. Ou seja, os usuários demonstram preocupação com a questão de segurança da informação, mas não se comportam de forma segura quando necessário (Acquisti & Grossklags, 2004).

Acerca disso, ressalta-se que a predição de comportamentos com base em declarações deve ser vista com cautela, pois a premissa de que há consistência entre o comportamento

declarado (dizer) e o comportamento executado (fazer) é questionada com base na revisão de vários estudos, cujos resultados indicam baixa correlação entre eles (Wicker, 1969). Por exemplo, na análise comportamental do consumidor os resultados indicam que comportamentos declarados não se mostram consistentes ou bons preditores do comportamento de consumo observado (Foxall, 1997).

Como pode ser visto, o tratamento dos riscos relacionados ao comportamento dos colaboradores carece de um modelo estruturado para aferir a eficácia e eficiência das ações empreendidas. Nesse sentido, a interlocução com a psicologia parece promissora, em especial, com a abordagem conhecida como análise do comportamento, que disponibiliza um sólido arcabouço teórico e metodológico desenvolvido para investigar as variáveis que influenciam o comportamento dos indivíduos (e.g., Skinner, 1953, 1957; Todorov, 2004, 2005). Nessa perspectiva, a proposta deste trabalho se afasta da avaliação típica de aspectos formais que envolvem a elaboração das políticas de segurança da informação ou das ações de conscientização deflagradas pelas organizações.

Nesse contexto, convém ressaltar 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, para aferir a eficácia e eficiência de uma PSI, como instrumento para controlar o comportamento dos colaboradores, propõe-se a adaptação da teoria proposta pela Análise Comportamental do Direito (Aguiar, 2017), para realizar a análise comportamental das regras que compõem uma PSI, isto é, identificar as contingências planejadas no normativo, ou seja, as condutas, suas sanções ou, menos comum, seus reforços (Oliveira, 2016). Neste artigo, buscou-se identificar, descrever e analisar três exemplos de contingências planejadas na política de segurança da informação estabelecida em uma organização da Administração Pública Federal, que optou por não ser identificada, e assim demonstrar a viabilidade da adaptação proposta.

2. Método

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 das regras jurídicas em que se denomina a relação causal entre a contingência coercitiva e o estado desejável das coisas de premissas factuais relevantes, o estado desejável das coisas como meta social e a contingência coercitiva estabelecida entre o comportamento indesejável e a sanção de contingência jurídica.

O modelo exposto pode ser resumido 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 quatro etapas:

1. Identificação das regras na política de segurança da informação que tratam do comportamento esperado dos colaboradores;
2. Descrição das contingências planejadas na política de segurança da informação, a partir das regras identificadas na primeira etapa;
3. Explicitação das metas sociais relacionadas às contingências planejadas;
4. Identificação das premissas factuais relevantes considerando as quatro categorias básicas propostas pela Análise Comportamental do Direito, são elas: a probabilidade de ocorrência do comportamento indesejado; 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.

A primeira etapa consiste na definição do escopo da análise a ser realizada. Isto é, trata-se da seleção das regras da PSI que versam sobre o comportamento esperado dos colaboradores (e.g., não instalar programas sem licenciamento) e das possíveis consequências a depender de suas condutas (e.g., bloqueio da Internet nos casos de acessos impróprios). A segunda etapa é a descrição das contingências planejadas na PSI, a partir da análise de riscos realizada pela organização participante, em termos de antecedentes (i.e., contexto e estado motivacional), padrão comportamental e sua consequência, conforme proposto por Aguiar (2017). Em seguida passa-se à terceira etapa, onde para cada contingência descrita é

identificada a respectiva meta social do SGSI à qual está relacionada, ou seja, verifica-se se a contingência planejada contribui para a proteção da informação dos diversos tipos de ameaças, de forma a assegurar a continuidade do negócio, mitigar os riscos e maximizar o retorno sobre os investimentos realizados e ampliar as oportunidades de negócio (ABNT, 2013b).

Por fim, avalia-se as premissas factuais relevantes que sustentam a contingência planejada em análise. A primeira categoria, probabilidade de ocorrência do comportamento indesejado, visa identificar quais consequências reforçadoras mantém aquela conduta no repertório comportamental dos colaboradores. Já a segunda, potencial eficácia da sanção, avalia se a sanção prevista na PSI, tende a ter efeito de maior magnitude se comparada aos reforços identificados na primeira categoria. A terceira categoria, nexo causal entre a conduta sancionada e a meta social mediata, visa identificar se a conduta, de fato, aumenta os riscos para a organização. Por último, são avaliadas as possíveis consequências indesejadas em decorrência da aplicação da sanção para determinada conduta, ou seja, avalia-se os possíveis efeitos, não previstos, da aplicação da sanção que possam prejudicar a organização.

Convém ressaltar que a análise da política de segurança da informação em tela, além de seus artigos, parágrafos e incisos, também contemplou 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.

3. Resultados

Uma política de segurança da informação define as diretrizes para a gestão da segurança da informação como um todo, nesse sentido, 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 outros elementos. 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, na primeira etapa do estudo, o objetivo foi definir o escopo da análise a ser realizada, excluindo regras 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").

A fim de exemplificar a análise realizada, das doze regras avaliadas, selecionou-se três regras para apresentação neste artigo, são elas:

1. É proibido aos usuários compartilhar sua senha de acesso à rede de computadores.
2. Os serviços de correio eletrônico corporativo serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.
3. 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 às regras acima, cumpre ressaltar que a numeração dos artigos, parágrafos e incisos foi substituída, bem como o texto sofreu pequenas mudanças, sem alteração de conteúdo, visando 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.

Para a análise das três regras selecionadas, foram descritas as contingências planejadas nas respectivas regras, 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 divida 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 1 a descrição da contingência planejada na Regra 1, qual seja: 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 da PSI implicará em responsabilidade administrativa na forma da lei.

Figura 1. Descrição da contingência planejada na Regra 1.

Como pode ser observado, a análise funcional da contingência planejada na Regra 1 indica que o compartilhamento de senhas ocorre no âmbito da organização para facilitar o trabalho e busca a maior produtividade da equipe (i.e., o reforço para o indivíduo que compartilha a senha), já que existem acessos necessários para a realização das atividades laborais que não são concedidos (i.e., estado motivacional - privação de acesso aos recursos necessários). Ou seja, há que se avaliar a contingência planejada pela organização, pois esta prevê a punição para uma conduta cujo reforço, em princípio, contribui para o sucesso da organização. Isto é, da análise da contingência planejada, verifica-se a oportunidade da adoção de medidas alternativas como a revisão de sua política de concessão de acessos às informações.

As contingências planejadas em uma PSI devem contribuir para o alcance da meta social do SGSI, ou seja, contribuir 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 ampliar as oportunidades de negócio (ABNT, 2013b), isto é, em última instância, proteger a organização. Nesses termos, verifica-se na Figura 2, a descrição da contribuição da Regra 1 para o alcance a da meta social do SGSI estabelecido pela organização.

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 na Regra 1.

Depreende-se da Figura 2, que sancionar o compartilhamento de senhas de acesso à rede de computadores contribui para o alcance da meta social do SGSI, pois a redução da ocorrência do compartilhamento de senhas (i.e., meta social imediata – redução da frequência do comportamento indesejado) contribui para a mitigação do risco de acessos não autorizados, preservando a confidencialidade e a integridade das informações organizacionais, bem como contribui para eventuais processos de responsabilização em caso de comprometimento das informações (meta social mediata).

Por último, 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 teoria analítico-comportamental do direito, essa identificação foi feita em quatro categorias básicas considerando a probabilidade de ocorrência do comportamento indesejado (i.e., identificar os possíveis reforços que mantém o comportamento indesejado no repertório comportamental do colaborador), a potencial eficácia da sanção, o nexo causal entre a conduta sancionada e a meta social mediata (i.e.,

meta social do SGSI) e as possíveis consequências indesejadas em decorrência da aplicação da sanção, conforme a Figura 3.

PROBABILIDADE DE OCORRÊNCIA DA CONDUTA

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 de 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 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 (Regra 1).

Depreende-se das premissas factuais relevantes identificadas, que a contingência planejada na Regra 1 contribui para a proteção da instituição (i.e., a redução do compartilhamento de senhas contribuí para a proteção da organização), logo justifica a sua definição. Entretanto, verificou-se que uma das consequências indesejadas da aplicação da sanção é o comportamento de contracontrole (Catania, 1999; Moreira & Medeiros, 2007) dos colaboradores, o que pode comprometer a eficácia da contingência. Acerca disso, convém

relembrar 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. Nesse sentido, reitera-se que 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 regra consigna que o serviço de correio eletrônico corporativo é destinado ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares. Nesses termos, a contingência planejada foi descrita conforme a Figura 4.

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.	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 4. Descrição da contingência planejada na Regra 2.

Da análise da Figura 4, verifica-se que o que mantém o comportamento de usar o correio eletrônico corporativo para fins particulares é a facilidade no gerenciamento das mensagens eletrônicas em uma solução única.

Em relação ao alcance da meta social do SGSI, verifica-se, conforme a Figura 5, a contribuição para a otimização do uso dos recursos TI, isto é, a contingência planejada contribui para a maximização do retorno sobre os investimentos realizados pela organização.

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 5. Explicitação das metas sociais relacionadas à contingência planejada na Regra 2.

Em relação às premissas factuais relevantes, identificadas na Figura 6, há necessidade de destacar as possíveis consequências indesejadas da aplicação da sanção. Verificou-se, conforme a Figura 5, que a contingência planejada contribui para a otimização do uso dos recursos de TI, essa é a meta social mediata alcançada. Entretanto, da aplicação da sanção nesses casos, verificou-se a possibilidade de uso de serviços de correio eletrônico externos para atividades laborais, já que o reforço do comportamento aqui analisado é a facilidade na gestão das mensagens eletrônicas. Constata-se, portanto a necessidade de uma análise pela organização dessas possíveis consequências indesejadas e avaliar se o impacto da possível exposição de informações organizacionais, mediante uso de correio eletrônico externo para o trabalho, é maior para a organização do que o eventual uso inapropriado dos recursos de TI. O resultado dessa análise pode levar à adoção de medidas alternativas, como a limitação do tamanho das caixas postais, 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.

PROBABILIDADE DE OCORRÊNCIA DA CONDUTA

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS	
ESTADO MOTIVACIONAL	CONTEXTO	Uso do correio eletrônico para assuntos particulares.	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.		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 6. Identificação das premissas factuais relevantes (Regra 2).

Por último, passa-se a análise da terceira regra que 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 foi descrita conforme a Figura 7.

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

Figura 7. Descrição da contingência planejada na Regra 3.

Observa-se na figura acima, que as recomendações contidas na PSI têm efeito aversivo para o colaborador, já que não observar as recomendações implica em menor esforço na realização das atividades rotineiras, em que pese a contingência planejada contribuir para o alcance da meta social do SGSI da organização, conforme a Figura 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 custo dos cuidados indicados.	A inobservância das disposições deste normativo implicará responsabilidade administrativa na forma da lei.	Responsabilização administrativa em caso de violação da PSI.	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 8. Explicitação das metas sociais relacionadas à contingência planejada na regra 11.

Em relação às premissas factuais relevantes, merece destaque o contexto em que o comportamento ocorre. Isto é, a dificuldade de aferir se as recomendações da PSI estão sendo cumpridas, conforme exposto na Figura 9.

PROBABILIDADE DE OCORRÊNCIA DA CONDUTA

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 9. Identificação das premissas factuais relevantes (Regra 3).

Acerca dessa última contingência, a dificuldade de aferir se as recomendações da PSI estão sendo observadas tem impacto direto na potencial eficácia da sanção, em que se espera que o seu efeito seja de maior magnitude quando comparado ao reforço para o colaborador (i.e., menor esforço na realização de suas atividades). Essa dificuldade certamente reduz a eficácia da contingência planejada, logo, verifica-se que a organização deve avaliar outras medidas para assegurar o comportamento que considera adequado.

4. Discussão

O objetivo do presente estudo foi identificar e descrever as principais contingências planejadas na política de segurança da informação de uma organização com base na adaptação da teoria analítica-comportamental do Direito (Aguiar, 2017).

Da análise da política de segurança da informação instituída pela organização participante, foram extraídas 12 regras que tratam do comportamento esperado dos colaboradores ou daqueles que são considerados inadequados pela organização, sendo três delas analisadas, a título de exemplo, no presente artigo. Acerca do cumprimento dessas regras, verificou-se que as contingências planejadas pela política de segurança da informação preveem 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.

Outro ponto importante da descrição das contingências planejadas em uma PSI é a identificação da relação dessas contingências com a meta social do sistema de gestão de segurança da informação da organização, isto é, se as contingências planejadas contribuem para a proteção das informações, asseguram a continuidade do negócio, mitigam riscos, maximizam o retorno sobre os investimentos realizados e ampliam as oportunidades de negócio (ABNT, 2013b). Nesses termos, verificou-se que as contingências planejadas na PSI ora analisada 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, essas contingências visam, em última instância, a proteção da instituição.

Acerca disso, impende 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.

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. Nos exemplos destacados neste artigo, verificou-se na Regra 1 a proibição do compartilhamento de senhas para acesso à rede de computadores. Da descrição da contingência planejada nesta regra (Figura 1), foi identificada como contexto da ocorrência do comportamento a restrição da organização na concessão de alguns acessos. Observa-se, portanto, que uma revisão da política de classificação das informações da organização (i.e., revisão dos requisitos para a concessão de acessos considerando as atividades dos colaboradores) pode revelar-se mais eficaz que a contingência planejada na política de segurança da informação. Quanto à Regra 2, destaca-se a possível consequência indesejada da contingência planejada, isto é, o uso de soluções de correio eletrônico externas para atividades laborais. Constata-se que as restrições de uso impostas na PSI podem levar à exposição das informações organizacionais, portanto, cabe à organização avaliar se esses riscos não são maiores que o uso inadequado dos seus recursos de tecnologia e eventualmente propor medidas alternativas como limitar o tamanho da caixa de mensagens eletrônicas, ou mesmo investir em infraestrutura de TI com vistas à reduzir o risco de exposição de suas informações. Por fim, em relação às recomendações contidas na terceira regra, que visam reduzir o risco de exposição de informações sensíveis por meio de acesso ao posto de trabalho do colaborador, na descrição da contingência (Figura 7), o contexto em que o comportamento de descuido ocorre contempla a dificuldade da organização em registrar e monitorar o cumprimento das recomendações. 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.

5. Conclusões

Do exposto, verificou-se no presente estudo que a aplicação da teoria analítica-comportamental do direito para a descrição e análise das contingências planejadas em uma política de segurança da informação de um SGSI, pode contribuir para a mitigação dos riscos organizacionais e, consequentemente, para a proteção das organizações. A interpretação aqui proposta evidencia a necessidade de uma análise funcional dos comportamentos indesejados quando da definição da PSI, pois as sanções previstas no normativo devem ter efeitos com magnitude maiores que os reforçadores dos comportamentos indesejados (Holanda, Oliveira-Castro & Silva, 2018).

Acerca disso, impende ressaltar que 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. Da mesma forma, as sanções previstas 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).

Nessa esteira, há necessidade de avançar na aplicação do modelo proposto para a Análise Comportamental do Direto na análise comportamental de um SGSI, pois esta análise também deve contemplar a análise das contingências que, de fato, estão vigentes, e por vezes não são planejadas pela organização, e influenciam os comportamentos que compõem a norma social, enquanto uma rede de comportamentos entrelaçados (Aguiar, 2017), de um sistema de gestão de segurança da informação (i.e., a rede de comportamentos entrelaçados que visam aumentar ou diminuir a probabilidade de aplicação de uma sanção quando da violação da PSI).

A análise da norma social do SGSI deve identificar os principais atores no processo de gestão de incidentes de segurança da informação da organização e descrever e analisar as contingências vigentes em cada nó, que compõe referida a norma social, no que diz respeito ao tratamento dado a esses incidentes (i.e., violações da política de segurança da informação). Essa análise permitirá, além da identificação das contingências vigentes nos principais nós que compõem a norma social do SGSI, aferir o grau de aplicação (i.e., *enforcement*) da

política de segurança da informação na organização participante, isto é, avaliar o quanto a PSI é eficaz enquanto procedimento de controle do comportamento dos colaboradores.

Concluindo, o presente trabalho propôs um novo método para a análise comportamental das políticas de segurança da informação nas organizações, mediante adoção do arcabouço teórico proposto pela análise do comportamento, em especial a Análise Comportamental do Direito. Nessa esteira, este artigo aponta um novo caminho para tratar os riscos que envolvem o comportamento dos colaboradores nas organizações, por meio da adoção e extensão da teoria analítica-comportamental do direito, podendo contribuir para o seu aprimoramento mediante a sua aplicação em outro contexto.

Referências

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. (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.

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

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.

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

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

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

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

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

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.

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

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.

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.

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

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.

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

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

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

Skinner, B. F. (1957). *Verbal behavior*. Englewood Cliffs, NJ: Prentice-Hall.

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. (2004). Da Aplysia à Constituição: evolução dos conceitos na análise do comportamento. *Psicologia: Reflexão e Crítica, 17*(2), 151-156.

Todorov, J. C. (2005). Laws and the complex control of behavior. *Behavior and social issues, 14*, 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

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.