ACTA COMPORTAMENTALIA
Vol. 31, Núm. 1, pp. 99-119

Sistemas de gestão de segurança da informação – uma análise comportamental

(Information security management systems – a behavioral analysis)

Rafael Almeida de Paula[1] y Jorge Mendes de Oliveira-Castro

Universidade de Brasília

(Brasil)

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 estabelecido pela análise do comportamento, em especial, a teoria analítico-comportamental do direito, mediante a sua aplicação em um órgão da administração pública federal. A pesquisa foi divida em duas fases, sendo a primeira a análise comportamental da política de segurança da informação, que contempla a descrição e análise das contingências planejadas no normativo, e a segunda a análise comportamental da norma de segurança da informação, enquanto um conjunto de padrões comportamentais entrelaçados que visam o controle coercitivo dos comportamentos indesejados. Os resultados apontam um novo caminho baseado na análise comportamental dos sistemas de gestão de segurança da informação para a mitigação dos riscos organizacionais, por meio da identificação de falhas, incoerências e a proposição de novas medidas com vistas ao aprimoramento desses sistemas de gestão.

Palavras-chave: gestão, segurança, informação, comportamento, usuário.

1 Endereço para correspondência: Rafael Almeida de Paula. Instituto de Psicologia - Departamento de Processos Psicológicos Básicos - Programa de pós-graduação em ciências do comportamento. Brasil. SQNW, 108 Bloco G, Apt. 611, Brasília – DF. Brasil. CEP: 70686-185. E-mail: rafael.paula@gmail.com.

ABSTRACT

The treatment of risks related to the behavior of employees in organizations represents a major challenge in the implementation of information security management systems. The main measure adopted by the organizations is the definition of information security policies. It occurs that the majority of the studies in the literature is restricted to the formal aspects of their elaboration or approached the awareness programs as instruments of their implantation. In this work, a new model is proposed to deal with these risks, based on the theoretical framework established by the behavior analysis, especially the theory presented by the Behavior Analysis of Law, which proposes an interpretation of the legal system that combines the theory of operant behavior with the theory of functionally specialized social systems. This research was divided into two phases, the first being the behavioral analysis of an information security policy, which includes the description and analysis of the contingencies planned in the normative, and the second the behavioral analysis of an information security norm, while a set of interlocked behavioral patterns aimed at coercive control of unwanted behaviors. Through its application in a Brazilian government agency, the results pointed to a new path based on the behavioral analysis of information security management systems for risk mitigation in organizations, by identifying flaws, inconsistencies and proposing new measures, based on principles of behavior analysis, subject to empirical verification, aiming at the improvement of these management systems.

Keywords: manage, information, security, behavior, user.

A informação tornou-se um dos ativos mais importantes de qualquer organização moderna (e.g., Braga, 2000; 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, assim como ampliar as oportunidades de negócio (ABNT, 2013b).

A implantação de um sistema de gestão de segurança da informação (SGSI) busca o estabelecimento dos processos de segurança da informação (e.g., gestão de incidentes, de riscos e de continuidade), baseada em uma abordagem de riscos para o negócio (ABNT, 2018), em um ciclo de melhoria contínua. Ou seja, 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; Von Solms, 2006; 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 PSI 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 de senhas e regras de uso de correio eletrônico), define responsabilidades e prevê as consequências de sua violação (ABNT, 2013b).

Acerca disso, verifica-se que boa parte dos estudos na literatura concentra-se na forma de se definir uma PSI, seu conteúdo (e.g., Talbot & Woodward, 2009; Al-Mayahi & Mansoor, 2014) e sugerem certa semelhança entre elas já que não poderiam ser plenamente implementadas distantes dos padrões e das boas práticas (Imoniana, 2004). Na mesma esteira, há estudos que sinalizam a necessidade de se estabelecer uma "cultura de segurança", mediante a realização de ações de conscientização como mecanismo para a implementação das PSIs (e.g., 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 (e.g., Wicker, 1969; Foxall, 1997; Davies, Foxall & Pallsiter, 2002; Foxall, 2002; Oliveira-Castro & Foxall, 2005). Acquisti e Grossklags (2004) destacam 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.

Como pode ser visto, o tratamento dos riscos que envolvem a questão humana dentro dos SGSIs está relacionado ao comportamento dos colaboradores. Ou seja, o diálogo com a psicologia parece oportuno e, nos casos de pesquisas empíricas, em especial, com a análise do comportamento, que propicia 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). Nesse contexto, destaca-se a Análise Comportamental do Direito (Aguiar, 2017), que propõe uma interpretação do Direito compatível com uma teoria operante do comportamento (Oliveira-Castro, Oliveira & Aguiar, 2018). Neste artigo, será demonstrado como a sua adaptação para a avaliação e tratamento dos riscos relativos ao comportamento dos colaboradores na implementação de um SGSI, isto é, uma análise comportamental dos SGSIs, pode possibilitar a definição de um modelo sistemático e estruturado para aferir a eficácia e eficiência das ações empreendidas para controlar o comportamento dos colaboradores.

Análise comportamental do direito

A Análise Comportamental do Direito (ACD) é uma interpretação do Direito que combina a teoria do comportamento operante com a teoria dos sistemas sociais funcionalmente especializados (Aguiar, 2017; Oliveira-Castro & Aguiar, 2020), que, enquanto sistema, tem a função social de reduzir a ocorrência de comportamentos considerados indesejados, predominantemente por meio da coerção. A organização da sociedade em sistemas sociais funcionalmente especializados ocorre quando práticas de grupos de pessoas são selecionadas por aumentarem a probabilidade de

sobrevivência, reprodução e bem-estar daquele grupo (Oliveira-Castro, Oliveira & Aguiar, 2018). De acordo com Aguiar (2017), dois dos principais elementos dos sistemas sociais funcionalmente especializados são a normas e regras sociais.

A norma social é definida como padrões comportamentais entrelaçados que controlam o comportamento dos indivíduos por meio de consequências reforçadoras e punitivas (cf. Skinner, 1953). Nesses termos, a norma jurídica é uma norma social especializada no controle coercitivo de comportamentos considerados indesejáveis, cujos padrões comportamentais entrelaçados (i.e., comportamentos jurídicos) podem ser classificados como punitivos (i.e., são influenciados pelo aumento da probabilidade de aplicação ou magnitude de sanções jurídicas) ou defensivos (i.e., são influenciados pela redução da probabilidade de aplicação ou magnitude de sanções jurídicas). Esse conjunto de padrões comportamentais entrelaçados (i.e., norma jurídica) forma uma rede de comportamentos jurídicos, cujos nós são compostos 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 (Aguiar & Oliveira-Castro, 2020).

Um comportamento comum e relevante nas normas jurídicas é o comportamento verbal de enunciação de regras jurídicas, isto é, das regras sociais do sistema jurídico (Aguiar, 2017). A ACD adota um conceito funcional de regras, pois as define como padrões comportamentais verbais cuja probabilidade de ocorrência depende de sua capacidade de alterar o comportamento de outros indivíduos (Aguiar, 2014). Por exemplo, um advogado de defesa quando cita textos da jurisprudência de tribunais superiores em sua petição, ele enuncia regras jurídicas. Esse comportamento é reforçado ou não pela redução da probabilidade de aplicação de uma sanção pelo juiz. O texto da jurisprudência tem função de estímulo discriminativo, pois sinaliza ao juiz um possível aumento na probabilidade de uma consequência aversiva, por exemplo, a sentença ser reformada em instâncias superiores.

A ACD propõe um modelo de análise comportamental das regras jurídicas em que a relação causal entre a contingência coercitiva e o estado desejável das coisas, de acordo com o conhecimento advindo das ciências, é denominada de premissa factual relevante; o estado desejável das coisas como meta social, que pode ser imediata (i.e., a redução do comportamento indesejado) ou mediata (i.e., efeito consequente da punição do comportamento); e a contingência coercitiva estabelecida entre o comportamento indesejável e a sanção de contingência jurídica (Aguiar & Oliveira-Castro, 2020).

Nessa esteira, a ACD provê um arcabouço teórico que pode ser aplicado às mais diversas pesquisas empíricas que investigam as relações das normas jurídicas e o comportamento dos seus destinatários e daqueles que atuam no sistema jurídico (e.g., advogados, magistrados e promotores). O presente trabalhou buscou mostrar como essa teoria pode contribuir para avaliar a implementação dos SGSIs nas organizações, no que tange ao controle dos riscos relacionados ao comportamento dos colaboradores. Essa proposta, a Análise Comportamental dos SGSIs, se afasta da avaliação típica dos aspectos formais que envolvem a elaboração das PSIs ou da avaliação das ações de conscientização e foca no comportamento dos indivíduos,

mediante a investigação das contingências planejadas e das contingências de fato vigentes que influenciam comportamentos relevantes de um SGSI.

Análise comportamental dos sistemas de gestão da segurança da informação

A definição de uma PSI é uma das principais medidas adotadas pelas organizações no estabelecimento de um SGSI. Trata-se de uma norma de cumprimento obrigatório que visa, dentre outras coisas, controlar o comportamento de seus colaboradores visando proteger as informações organizacionais. Constata-se, portanto, sua semelhança com o Direito, pois, conforme explica Aguiar (2014), as leis também são estabelecidas com a função de controlar os padrões comportamentais considerados indesejáveis pela sociedade. Nessa esteira, verifica-se a viabilidade da adaptação do modelo proposto pela ACD para aferir a eficácia e eficiência de uma PSI enquanto instrumento para controlar o comportamento dos colaboradores. Trata-se de uma adaptação que permite a análise comportamental das PSIs, ou seja, um modelo que permite identificar as contingências planejadas no normativo, isto é, as condutas, suas sanções ou, menos comum, seus reforços (Oliveira, 2016).

Entretanto, o planejamento dessas contingências não assegura que estas estejam de fato vigentes. Galizio (1979) aponta que quando as contingências planejadas (regras) e as vigentes são compatíveis, o comportamento de observar a regra se mantém, 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 (e.g., Albuquerque & Silva, 2006).

No contexto de um SGSI, o tratamento de eventuais violações da PSI 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). Novamente, constata-se a semelhança entre o SGSI e o Direito, pois ambos estabelecem processos que disciplinam como as eventuais violações de seus normativos devem ser tratadas. Ou seja, assim como ocorre no Direito, em um SGSI também há uma norma social, enquanto uma rede de comportamentos entrelaçados (Aguiar, 2017), que lida com o problema de sancionar ou não condutas que violem a PSI da organização. A adaptação da teoria analítico-comportamental do direito permite descrever e analisar a norma social de um SGSI, neste trabalho chamado 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). Por meio da aplicação deste modelo teórico em um SGSI é possível identificar as contingências vigentes nos principais nós que compõem a norma de segurança da informação da organização e aferir a eficácia e eficiência desse sistema no controle dos comportamentos dos colaboradores nas organizações.

Depreende-se do exposto, que a interpretação analítico-comportamental dos SGSIs, por meio da aplicação do modelo teórico proposto pela ACD, 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).

METODOLOGIA

Esta pesquisa foi realizada em um órgão da Administração Pública Federal, que optou por não ser identificado, que possui em torno de 3.000 (três mil) colaboradores e PSI formalmente estabelecida há mais de 10 (dez) anos. Participaram da pesquisa o gestor responsável pela gestão da segurança da informação e os principais atores no processo de gestão de incidentes de segurança da informação. Para a sua consecução, foram consultados o regulamento geral do órgão; a PSI, suas normas complementares e a documentação relativa à análise de riscos que a embasou; e a norma que estabeleceu o processo de gestão de incidentes de segurança da informação. 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.

A aplicação do modelo teórico proposto pela ACD no SGSI estabelecido pela organização participante foi dividida em duas fases, sendo a primeira a análise comportamental da PSI e a segunda a análise comportamental da norma de segurança da informação (NSI), no tocante ao processo de gestão de incidentes de SI, que disciplina como as violações da PSI devem ser tratadas.

A Fase 1 da pesquisa foi divida em 5 etapas, são elas: 1) Identificação dos itens na PSI que tratam do comportamento esperado dos colaboradores; 2) Classificação dos comportamentos identificados na primeira etapa em categorias; 3) Descrição das contingências planejadas na PSI, a partir das categorias identificadas na segunda etapa; 4) Explicitação das metas sociais relacionadas às contingências planejadas; e 5) Identificação das premissas factuais relevantes considerando as quatro categorias básicas propostas pela ACD e adaptadas no presente estudo.

Já a Fase 2 foi divida 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 NSI; e 3) Descrição e análise das contingências em cada nó.

Na Fase 1, a análise comportamental da PSI, a primeira etapa consistiu na definição do seu escopo, ou seja, foram extraídos os dispositivos da PSI que versavam sobre o comportamento esperado dos colaboradores, excluindo os itens que, por exemplo, tratavam da definição de procedimentos (e.g., como solicitar a troca de senhas) ou de responsabilidades (e.g., a unidade de TIC deverá bloquear contas de acesso não utilizadas há mais de 60 dias).

Em seguida, Etapa 2, os itens selecionados foram agrupados em categorias comportamentais, a partir da sua análise funcional, isto é, das possíveis variáveis que influenciam a ocorrência do comportamento e das possíveis consequências. Por exemplo, na PSI analisada, as regras "É proibido aos usuários compartilhar sua senha de acesso à rede de computadores" e "É responsabilidade do usuário

do correio eletrônico corporativo não permitir acesso de terceiros por meio de sua senha", foram agrupadas em uma única categoria comportamental por serem funcionalmente equivalentes.

Na Etapa 3 foram descritas as contingências planejadas naquele conjunto de 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, estas foram divididas em reforçadoras, pois, caso não houvesse reforço o comportamento não se manteria no repertório comportamental do colaborador; e em sanções, isto é, consequências punitivas, previstas na PSI, com vistas a reduzir a frequência de ocorrência do comportamento indesejado (Catania, 1999).

A título de exemplo, passa-se à análise realizada para a categoria "Compartilhamento de senhas" em que a contingência planejada foi descrita conforme a Figura 1.

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. Difícil monitoramento.	Compartilhar senhas.	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

Uma vez descritas as contingências, na Etapa 4 foi verificado se essas contingências contribuem para o alcance da meta social do SGSI, isto é, se contribuem 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).

Seguindo com a análise aqui exemplificada, depreende-se da Figura 2, 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.

ANTECEDENTES		PADRÃO COMPORTAMENTAL	CONSEQUÊNCIAS (META SOCIAL)	
PREMISSAS FACTUAIS RELEVANTES	AUTORIZAÇÃO LEGAL		IMEDIATA	MEDIATA
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 2. Explicitação das metas sociais

Por fim, na Etapa 5 foram identificadas as premissas factuais relevantes que embasaram a instituição da contingência, isto é, as condições ou circunstâncias que se assumem como verdadeiras, conforme o conhecimento advindo das ciências. Com base na adaptação da teoria analítico-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.

Nesse sentido, no exemplo de análise realizada na Fase 1, conforme a Figura 3, 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 PSI, 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 repetiu, 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.

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. 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	Maior proteção dos ativos de informação da organização

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 3. Identificação das premissas factuais relevantes

Ainda em relação à análise dessas premissas, conforme o exemplo aqui apresentado, 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, logo, conclui-se do exemplo da análise realizada, 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 fase da pesquisa buscou identificar os principais atores no processo de gestão de incidentes de segurança da informação da organização e então descrever e analisar a norma de segurança da informação (NSI). Nessa análise, foram identificadas as contingências vigentes nos principais nós, bem como foram levantados dados secundários que revelaram o grau de aplicação (i.e., enforcement) da PSI na organização participante.

Na Etapa 1, para o mapeamento do processo de gestão de incidentes de segurança da informação, foi utilizado o programa Bizagi Modeler – versão 3.4, compatível com o padrão BPMN – Business Process Model and Notation, disponível gratuitamente na Internet, em que foi possível identificar os colaboradores que

exercem papéis-chaves na aplicação das regras contidas na PSI, conforme resumido na Figura 4.

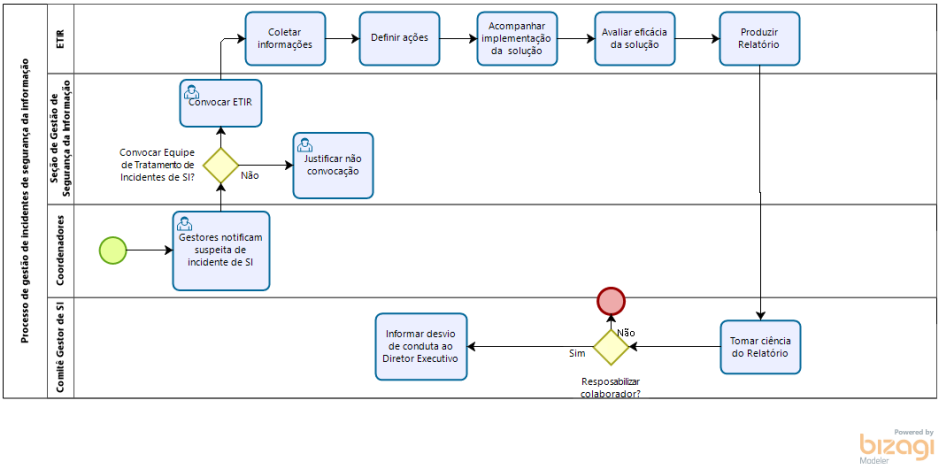

Figura 4. Processo de gestão de incidentes de segurança da informação

Uma vez mapeado o processo de gestão de incidentes, passou-se a identificação dos principais nós da NSI, Etapa 2 desta fase. Como pode ser observado na Figura 4, o primeiro nó é composto pelos padrões comportamentais: notificação da suspeita de incidente de SI; e a convocação, ou não, da equipe de tratamento de incidentes de segurança da informação (ETIR).

A Etapa 3, isto é, a descrição e análise das contingências em cada nó, foi realizada por meio de entrevistas com os colaboradores que exercem papéis-chaves dentro do processo de gestão de incidentes de segurança da informação, bem como análise dos relatórios de incidentes de SI produzidos nos últimos cinco anos e das atas das reuniões do CGSI. Cumpre ressaltar que o escopo deste trabalho restringiu-se aos incidentes ocorridos nos últimos cinco anos, período em que passaram a ter um tratamento padronizado pela organização. Nessa etapa, foram descritas e analisadas as contingências vigentes nos principais nós que formam a NSI da organização também nos termos da contingência de quatro termos (i.e., padrão comportamental, consequência, contexto e estado motivacional), conforme proposto pela ACD e apresentado na próxima seção.

RESULTADOS

O escopo deste trabalho contemplou 13 itens da PSI por tratarem do comportamento esperado dos colaboradores. Esses itens foram agrupados em quatro categorias comportamentais, a partir da análise funcional de cada comportamento identificado em cada um dos itens, conforme consolidado na Tabela 1.

Tabela 1. Categorias comportamentais identificadas na PSI da organização participante

Categoria	Descrição	Nº de itens da PSI
Compartilhamento de senhas.	Colaborador compartilhar senhas de acesso aos recursos informatizados com terceiros.	2.
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.	6.
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 equipamento particular) ou lógicas (e.g., instalação de programas não homologados).	4.
Descuidos no posto de trabalho.	Ações que possam comprometer a segurança das informações organizacionais mediante acesso físico ao posto de trabalho do colaborador.	1.

Acerca do cumprimento dessas regras, verificou-se que a PSI 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 estabelecida pela organização visa controlar os comportamentos dos colaboradores por meio de sanções. Acerca disso, impende ressaltar que as eventuais sanções podem ter ou não função punitiva. 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 PSI prevê outras duas atividades que também podem funcionar como estímulos aversivos condicionados, são elas: a previsão de monitoramento da utilização de recursos tecnológicos, com vistas a detectar e evidenciar incidentes (passíveis de responsabilização); e a realização de auditorias nos ativos de TI, visando avaliar a conformidade técnica com os normativos aplicáveis e a apuração de eventos que possam expor os ativos de informação.

Um importante ponto na descrição das contingências planejadas na PSI é a identificação da relação dessas contingências com a meta social do SGSI, isto é, identificar se essas contingências 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). Nesses termos, conforme pode ser observado na Tabela 2, todos os itens analisados contribuíram para o alcance de pelo menos uma meta social do SGSI estabelecido. Entretanto, em relação à meta "Ampliar as oportunidades de negócio" não foi identificado qualquer item na PSI que contribuísse para o seu alcance.

Tabela 2. Relação das contingências planejadas com a meta social do SGSI da organização

Meta Social do SGSI	Nº de itens da PSI
Assegurar a continuidade do negócio.	10.
Mitigar riscos.	12.
Maximizar o retorno sobre os investimentos.	10.
Ampliar as oportunidades de negócio.	0.

Outro importante ponto da análise realizada foi a identificação do estado motivacional e as consequências reforçadoras que mantém os comportamentos considerados indesejados pela organização, conforme a Tabela 3.

Tabela 3. 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 TI 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). 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). 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.
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 a 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.

Nessa esteira, a compreensão dos contextos em que os comportamentos ocorrem também é relevante para o planejamento adequado das contingências (i.e., regras na PSI). A partir da análise comportamental da PSI foram identificados quatro contextos, sendo os contextos "possibilidade técnica" e "difícil monitoramento" os mais frequentes entre as categorias comportamentais, conforme pode ser observado na Tabela 4.

Tabela 4. 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.

Uma vez concluída a análise comportamental da PSI, passou-se à segunda fase da pesquisa, a análise comportamental da NSI. A partir do mapeamento do processo de gestão de incidentes de SI foi possível identificar seus principais atores e os nós que compõem a norma.

Como pode ser observado na Figura 4, o primeiro nó 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). A partir das entrevistas realizadas com os responsáveis, verificou-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. Observa-se, portanto, que o comportamento de "Registrar a suspeita dos incidentes de SI", além de estar sob o controle de uma contingência planejada (i.e., previsão normativa que atribui aos coordenadores esta responsabilidade), é reforçado negativamente pela redução da probabilidade dos riscos associados àquela suspeita virem a concretizar. Constata-se, portanto que o conhecimento da suspeita e dos possíveis impactos associados a ela funciona como contexto para o comportamento de registrá-la, e que a redução dos riscos para a organização é o estado motivacional dos coordenadores. Quanto à convocação ou não da ETIR, foi esclarecido que para todas as suspeitas de incidente que eventualmente possam comprometer a confidencialidade, integridade e/ou disponibilidade das informações da organização a ETIR é convocada e que não houve casos de não

convocação no período analisado nesta pesquisa. Sendo assim, o primeiro nó da NSI foi descrito conforme a Figura 5.

NO #1				
PADRÕES COMPORTAMENTAIS	CONTINGÊNCIAS	ANTECEDENTES		CONSEQUÊNCIAS
		CONTEXTO	ESTADO MOTIVACIONAL	
Registro da suspeita de incidente.	Norma institucional atribui aos coordenadores a responsabilidade pela notificação de qualquer suspeita que aponte para um incidente de SI. Dever de tratar adequadamente os riscos organizacionais.	Previsão normativa do dever de notificar qualquer suspeita de incidentes. Conhecimento da atividade suspeita e dos riscos associados.	Reduzir a probabilidade de concretização do risco associado a suspeita. 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 de concretização do risco associado a suspeita. 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 5. Descrição do primeiro nó da norma de segurança de informação

Uma vez convocada a ETIR, o incidente é tratado e um relatório submetido ao CGSI a quem caberá decidir pela apuração ou não de responsabilidade pelo evento ocorrido, trata-se do segundo nó na NSI. Novamente, por meio das entrevistas realizadas, verificou-se que o tratamento de incidentes de SI é prioridade no âmbito da unidade de TI, diante do conhecimento dos riscos associados. Quanto à apuração ou não de responsabilidade, foi verificado que o CGSI adota dois critérios para a tomada de decisão, a reincidência e a gravidade. Em relação à reincidência foi ve-

rificado que não houve casos nos últimos anos e quanto à gravidade constatou-se que, como os incidentes, usualmente, são tratados e prontamente solucionados na esfera técnica, os impactos são bem reduzidos, logo a percepção de gravidade 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 aplicação de sanções ao colaborador que viole os requisitos de segurança da informação da organização, de acordo com os relatos, os membros do CGSI não percebem a violação da PSI como sendo um risco significativo para a organização, logo, não veem necessidade de mobilizar outras áreas da organização na apuração de responsabilidade, pois os incidentes usualmente são tratados de uma forma satisfatória pela equipe técnica e os impactos mitigados. Isto posto, verificou-se que não houve a ocorrência de apuração de responsabilidade dos colaboradores que deram causa a incidentes de SI nos últimos cinco anos. Nesses termos, as contingências vigentes no segundo nó foram descritas conforme a Figura 6.

NO #2				
PADRÕES COMPORTAMENTAIS	CONTINGÊNCIAS	ANTECEDENTES		CONSEQUÊNCIAS
		CONTEXTO	ESTADO MOTIVACIONAL	
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.	Dever de tratar os incidentes de SI, conforme previsão normativa; Convocação da ETIR pela SSEGI; Incidente de SI triado para tratamento.	Reduzir a probabilidade de concretização do risco associado a suspeita. Evitar responder por eventuais danos causados pelo incidente de SI. Reduzir a probabilidade de recorrência de eventos semelhante.	Mitigação dos riscos associados ao incidente (Reforço negativo para a ETIR e Coordenadores). O aprimoramento dos mecanismos de proteção evita incidentes similares no futuro, aumentando a proteção da organização (Reforço positivo para ETIR e equipe técnica)
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 6. Descrição do segundo nó da norma de segurança de informação

Apesar da constatação de que não houve casos de apuração de responsabilidades e punição de colaboradores que violaram a PSI restringir a análise deste nó e encerrar a análise da NSI, trata-se de um nó crítico para o tratamento da questão comportamental no âmbito do SGSI, pois é um ponto de alavancagem desse sistema (Aguiar, 2017), no qual pequenas mudanças causam grandes alterações comportamentais.

CONCLUSÃO

O objetivo deste trabalho foi demonstrar a viabilidade da adaptação da teoria analítica-comportamental do direito (Aguiar, 2017) no tratamento dos riscos de segurança da informação relacionados ao comportamento dos colaboradores nas organizações. Isto é, a Análise Comportamental dos SGSIs, mediante a sua aplicação em um órgão da Administração Pública Federal.

Da análise comportamental da PSI, verificou-se que as contingências planejadas contribuem para o alcance de pelo menos uma das metas sociais do SGSI, à exceção da meta "Ampliar as oportunidades de negócio", em que não foi identificado qualquer item na PSI que contribua para o seu alcance. Constata-se, portanto, que a análise comportamental da PSI sugere 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. A partir da análise funcional dos itens da PSI, verificou-se que 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 PSI nas organizações pode ser útil no sentido de verificar se há alinhamento das diretrizes de segurança da informação à estratégia da organização.

A primeira fase deste trabalho também permitiu identificar algumas variáveis, à luz da teoria analítico-comportamental, que contribuem para a ocorrência de condutas consideradas inadequadas pela organização. Isto é, foram identificados o estado motivacional e contexto no qual esses comportamentos ocorrem, bem como suas consequências reforçadoras. Dessa análise, verificou-se que para as quatro categorias comportamentais 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, mantenham os riscos da organização em níveis aceitáveis, pode ser mais eficiente que a contingência planejada na PSI. Por exemplo, a descrição da contingência planejada na primeira categoria comportamental, isto é, a proibição do compartilhamento de senhas (Figura 1), aponta que 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 PSI, pois atenderá à necessidade do colaborador que compartilha sua senha (i.e., estado motivacional) sem incorrer na violação dos requisitos de segurança da organização. Da mesma forma, a análise dos contextos revelou que a "possibilidade técnica" e o "difícil monitoramento" foram os mais frequentes entre as categorias comportamentais. Acerca disso, convém resgatar que a PSI 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 4, 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 PSI.

A segunda fase deste trabalho buscou descrever e analisar a norma de segurança da informação, ou seja, descrever 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, verificou-se que a organização não tem a prática de sancionar o comportamento de seus colaboradores quando da violação de sua PSI. Foi constatado que nos últimos cinco anos foram registrados e tratados dez incidentes, para os quais não foram instaurados processos para apuração de responsabilidade, logo, também não houve a aplicação de sanções. Como a aplicação de sanções é a contingência planejada na PSI, verifica-se que esta dificilmente terá função aversiva, pois a consequência prevista não é consistentemente contingente aos comportamentos considerados indesejados pela organização (Aguiar, 2017). Constata-se, portanto, que apesar da PSI e do processo de gestão de incidentes de segurança da informação da organização estarem conforme as boas práticas (ABNT, 2013a; ABNT, 2013b), à luz da teoria analítico-comportamental, em especial a Análise Comportamental do Direito, o SGSI estabelecido dificilmente tratará os riscos de segurança da informação relacionados aos comportamentos dos colaboradores.

No entanto, apesar dos resultados sugerirem que o SGSI não se revela 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 de um dos entrevistados, 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 dos colaboradores, em termos de contexto para a ocorrência dos comportamentos, 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. Por exemplo, ao acessar a Internet, as únicas opções disponíveis para

o colaborador são aquelas categorias de sítios eletrônicos 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 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 PSI (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.

A análise comportamental da norma de segurança da informação é relevante, pois contribui para a identificação de falhas e proposição de medidas alternativas e/ou complementares com vistas ao aprimoramento do SGSI estabelecido na organização. Por exemplo, 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 deve avaliar uma possível gradação de sanções, como o envio de notificações, alertas às chefias, bloqueios temporários de acesso e, eventualmente, a responsabilização do colaborador. Essa gradação de sanções, sendo consistentemente contingentes às condutas que violam a PSI, muito provavelmente terá o efeito punitivo almejado pela organização.

Conclui-se, portanto, que a adaptação do modelo proposto pela Análise Comportamental do Direito além de ser aplicável para a descrição e análise das contingências planejadas nas PSIs, também pode ser utilizada para a descrição e análise das contingências vigentes em um SGSI (i.e., da norma de segurança da informação) viabilizando a análise comportamental dos SGSIs. Essa proposta contribui para a mitigação dos riscos organizacionais e, consequentemente, para a proteção das organizações, por meio da identificação de falhas, incoerências e a proposição de medidas alternativas e/ou complementares com vistas à, de fato, controlar os comportamentos indesejados dos colaboradores e aprimorar os SGSIs.

Nesse sentido, constata-se que essa intepretação aponta um novo caminho para tratar os riscos que envolvem o comportamento dos colaboradores nas organizações e revela a possibilidade de novas pesquisas empíricas, por meio da intervenção em um SGSI, a partir de sua análise comportamental. Por exemplo, o estudo dos efeitos da implementação de consequências reforçadoras para os comportamentos "seguros" dos colaboradores (i.e., que observam a PSI) ou dos efeitos da gradação de sanções, conforme proposto neste trabalho. Outro ponto importante a ser investigado e confirmado empiricamente, que configura a principal limitação desta pesquisa, são os efeitos das relações de trabalho na prática de aplicar sanções pelas organizações. Trata-se de um fator relevante a ser considerado, pois a relação trabalhista de servidores públicos federais é regida por lei específica (e.g., Lei n. 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.

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 implementa 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). Logo, outra promissora frente de investigação 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

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In Economics of information security (pp. 165-178). Boston, MA: Springer. http://dx.doi.org/10.1007/1-4020-8090-5_13

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.

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

Alqahtani, F. H. (2017). Developing an information security policy: a case study approach. Procedia Computer Science, 124, 691-697. http://dx.doi.org/10.1016/j.procs.2017.12.206

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

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

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

Al-Mayahi I. H., & Mansoor, S., P. (2014). Information security policy development. Journal of Advanced Management Science, 2(2), 135-139. http://dx.doi.org/10.12720/joams.2.2.135-139

Braga, A. (2000). A gestão da informação. Millenium, 19.

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. http://dx.doi.org/10.21714/1984-3925_2018v21n3a6

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. https://doi.org/10.1177/1470593102002001645

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. http://dx.doi.org/10.1362/147539202323071263

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.

Imoniana, J. O. (2004). Validity of information security policy models. Transinformação, 16(3), 263-274. http://dx.doi.org/10.1590/S0103-37862004000300006

Lei n. 8.112, de 11 de dezembro de 1990. (1990). Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Brasília. 1990.

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.

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.

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

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., & de Aguiar, J. C. (2020). Behavioral Analysis of Law: An Operant Interpretation of Legal Systems. Perspectivas em Análise do Comportamento, 11(1), 92-113. http://dx.doi.org/10.18761/PAC.2020.v11.n1.08

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. http://dx.doi.org/10.19092/reed.v5i2.245

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

Snyman, D., & Kruger, H. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. Information & Computer Security, 25(2), 152-164. http://dx.doi.org/10.1108/ICS-03-2017-0015

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

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

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. http://dx.doi.org/10.1590/S0102-79722004000200003

Todorov, J. C. (2005). Laws and the complex control of behavior. Behavior and social issues, 14, 86-91. http://dx.doi.org/10.5210/bsi.v14i2.360

Von Solms, B. (2006). Information security – the fourth wave. Computers & Security,25(3), 165-168. http://dx.doi.org/10.1016/j.cose.2006.03.004

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. https://doi.org/10.1111/j.1540-4560.1969.tb00619.x

(Received: March 31, 2022; Accepted: July 27, 2022)