relato de pesquisa

RELAÇÕES ÀS VIOLAÇÕES INDIVIDUAIS DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

RELATIONSHIP TO INDIVIDUAL INFORMATION SECURITY POLICY VIOLATIONS

Alexandre Cappellozza [1]
0000-0002-1539-1230
Camila Bernardo da Silva [2]
Luciana Arantes Medeiros [3]
Gustavo Hermínio Salati Marcondes de Moraes [4]
0000-0001-5238-0314
Gilberto Perez [5]
0000-0002-6624-0643

RESUMO
Não há dúvidas de que a Tecnologia da Informação e Comunicação é fundamental para o desempenho das organizações e que atinge também a produtividade dos colaboradores. Entretanto, o uso indevido da tecnologia pode provocar problemas irreversíveis às organizações, tais como a violação das políticas da segurança da informação. O objetivo deste estudo é investigar os antecedentes que possam impactar no mau uso dos sistemas de informação, em particular, aqueles específicos que possam causar a violação das políticas de segurança da informação. Para tanto, o trabalho foi conduzido por meio de uma pesquisa quantitativa com 456 usuários de tecnologias organizacionais. Para os testes de hipóteses do estudo, foi realizada a análise de equações estruturais, ao modelo de pesquisa proposto. Confirmou-se que o Desengajamento Moral teve efeito positivo na Intenção de Violação de Política Organizacional de Segurança da Informação, sendo a dimensão Justificativa Moral com manifestação de maior efeito, seguido da dimensão Eufemismo. A Habilidade Tecnológica e a Liderança Autêntica não foram confirmadas como fatores que influenciam na Violação de Políticas de Segurança da Informação.
Palavras-Chave: Desengajamento moral. Habilidade tecnológica. Segurança da informação. Violação de políticas. Liderança autêntica. Penalidades.

Artigo submetido em 03/03/2021 e aceito para publicação em 30/09/2021.

[1] Professor do Núcleo Docente Permanente do Programa de Pós-Graduação em Administração de Empresas da Atitus Educação e coordenador do Programa de Mestrado Profissional em Administração do Desenvolvimento de Negócios da Universidade Presbiteriana Mackenzie. Lattes: http://lattes.cnpq.br/8358857348226421. E-mail: alexandre.cappellozza@mackenzie.br.
[2] Professora de Pós Graduação da Universidade de São Caetano, Estácio de Sá e Faculdade Phorte. Professora de Ensino Presencial da Escola de Negócios e Hospitalidade do Centro Universitário Faculdades Metropolitanas Unidas (FMU). Mestre em Administração pela Universidade Metodista de São Paulo. Lattes: http://lattes.cnpq.br/3907101981722570. E-mail: camis.log@gmail.com.
[3] Mestre em administração pela Universidade Metodista de São Paulo. Lattes: http://lattes.cnpq.br/9325288590585544. E-mail: luarantesmedeiros@gmail.com.
[4] Professor Associado (MS 5.1) da Faculdade de Ciências Aplicadas (FCA) da UNICAMP desde 2015. Livre Docente na área de Administração pela UNICAMP (2021). Doutor (2013). Lattes: http://lattes.cnpq.br/4643990060392832. E-mail: gustavo.salati@fca.unicamp.br.
[5] Professor Adjunto I na Universidade Presbiteriana Mackenzie (UPM), atuando na Pós-Graduação Stricto Sensu em Administração (PPGA). Lattes: http://lattes.cnpq.br/8699394703578756. E-mail: gilberto.perez@mackenzie.br.

ABSTRACT
There is no doubt that Information and Communication Technology is essential for organizations' performance and that it also affects the productivity of employees. However, the improper use of technology can cause irreversible problems for organizations, such as violating information security policies. This study aims to investigate the antecedents that may impact the misuse of information systems, particularly those that may cause the violation of information security policies. To this end, the work was conducted through a quantitative survey with 456 users of organizational technologies. For the study's hypothesis tests, the analysis of structural equations was performed, according to the proposed research model. It was confirmed that Moral Disengagement had a positive effect on the Intention to Violate Organizational Information Security Policy, with the Moral Justification dimension showing the most significant effect, followed by the Euphemism dimension. Technological Skill and Authentic Leadership have not been confirmed as factors that influence the Violation of Information Security Policies.

Keywords: *Moral disengagement. Technological skill. Information security. Policy violation. Authentic leadership. Penalties.*

1 INTRODUÇÃO

A infraestrutura dos sistemas de informações e o volume crescente de dados nas organizações exigem controle e proteção dos conteúdos dos dados armazenados com o objetivo de mitigar os acessos não autorizados, cópias indevidas e outros riscos à segurança das informações (MANÃS, 2014). O desafio de proteção dessas informações sigilosas (STONE-ROMERO; STONE; HYATT, 2003) se associa a ocorrência frequente de eventos de violação de segurança da informação nas organizações (McCANDLESS; EVANS, 2021).

A sociedade moderna se tornou dependente de sistemas de tecnologia da informação de uma forma geral (SAFA et al., 2018) e demanda por constante inovação (SILVA; DAMIAN; VALENTIM, 2020). As organizações, sejam elas de classe econômica, política, militar e/ou legal, tornam-se cada vez mais globais e interligadas, e o uso das Tecnologias de Informação se faz necessário como ferramenta de gerenciamento eficaz e confiável, aumentando produtividade e garantindo agilidade na troca das informações (FLOWERDAY; TUYIKEZE, 2016).

No entanto, junto com a dependência dos sistemas de informação nas instituições se potencializa a vulnerabilidade das informações confidenciais dessas organizações, uma vez que a disponibilidade dos recursos adequados

para assegurar a privacidade das informações pode não estar garantida (WARKENTIN; WILLISON, 2009).

Segundo D'Arcy et al., (2009), a preocupação com a privacidade de informações surgiu na década de 1970 e, desde então, essa preocupação aumentou dada a proporção do uso desses artefatos nas organizações. É necessário buscar um equilíbrio entre a privacidade e a utilidade dos dados, levando em conta que a proteção da privacidade é fundamental atualmente (AFFONSO; OLIVEIRA; SANT'ANNA, 2017). Nas últimas décadas ocorreram desvios de comportamentos éticos e morais dentro das mais diversas organizações, sejam públicas, privadas ou até mesmo a do terceiro setor, e a fim de mudar este cenário, muitas revisaram suas políticas internas com o objetivo de evidenciar perante acionistas, clientes e colaboradores, o compromisso com a ética e a moral (AVOLIO; GARDER, 2005).

A segurança da informação envolve controles específicos desenvolvidos para proteger as informações de cópias não autorizadas, perdas, destruição, venda ou até mesmo o uso indevido dos dados (BÉLANGER et al., 2017). As políticas de segurança contêm diretrizes detalhadas para o uso adequado e recursos organizacionais de segurança da informação. As Políticas Organizacionais de Segurança da Informação propõem diretrizes e protocolos para assegurar a inviolabilidade das normas de conduta desejáveis, fundamentais para estabelecer a segurança da informação necessária à proteção dos dados (LOGAN, 2010).

Respectivamente, as políticas de segurança contam com o mesmo mecanismo subjacente que as leis da sociedade: fornecer conhecimento sobre conduta inaceitável, e a ameaça de punição por práticas e comportamentos ilícitos (D'ARCY et al., 2009).

As organizações dedicam recursos significativos para implementar medidas de segurança, e desenvolvem políticas, apoiadas pela educação e treinamento, além de manter atualizada as tecnologias de segurança, que apenas se tornam efetiva quando há o engajamento de funcionários no cumprimento das políticas e procedimentos de segurança estabelecidos, em geral, quando há efetividade na verticalidade dessa política, em que a alta direção participa ativamente deste processo.

Entretanto, alguns estudos sugerem que tais requisitos podem ter o efeito oposto, ou seja, trazer um comportamento inverso ao pretendido devido às exigências, que elas impõem aos funcionários, tais como tempo, esforço e frustração (PAHNILA; SIPONEN; MAHMOOD, 2007).

Além disso, sabe-se que em algumas organizações, há a falta de conscientização sobre políticas de segurança e que podem ocasionar a negligência aos sistemas de informação, a resistência às normas internas, apatia e malícia são as causas possíveis de violação do sistema de segurança da informação por parte dos colaboradores nas organizações (SAFA et al., 2018).

A baixa confiança na organização prejudica os benefícios percebidos de *compliance* e acresce os riscos percebido de perda de privacidade dos dados pelos colaboradores (SANTOS, CAPPELLOZZA, ALBERTIN, 2018), assim como a falta de conhecimento dos usuários também é apresentada como risco à segurança de informação das organizações, ou seja, o funcionário se torna ameaça de violação dada a sua pouca instrução. A falta de instrução pode levar os colaboradores a ações imprudentes, por falta de conhecimento, o que deixa a segurança de informação vulnerável (SIPONEN, 2005).

Em um ambiente de pressão, o estresse, as penalidades das infrações às políticas organizacionais entre outros fatores de tensão, fazem com que os colaboradores estejam sujeitos a se comportarem de forma contrária às regras organizacionais, cuja consequência é a criação de mecanismos subjetivos, como o desengajamento moral, que aliviam as tensões, e justificam o comportamento inadequado, racionalizam os danos e fazendo-os parecer moralmente justificáveis (BANDURA, 2002).

A Teoria do Desengajamento Moral tem sido usada para explicar por que os indivíduos se envolvem em comportamentos inadequados, quando eles entendem que é errado fazê-lo (BANDURA, 1996). Segundo Moore (2015), o Desengajamento Moral refere-se a um conjunto de mecanismos cognitivos que desacoplam os padrões morais internos de suas ações, que justificam ou facilitam o comportamento antiético das pessoas perante a sociedade em que convive.

O ambiente de trabalho pode provocar e/ou induzir comportamentos imorais dos colaboradores, quando postos em situações desfavoráveis, comportamentos como: improdutividade, descumprimento de políticas,

maquiavelismo e desvio de condutas. Os funcionários podem racionalizar ou justificar seu comportamento imoral com base nas condições de trabalho dispostas pela empresa (BANDURA et al., 2000; D'ARCY et al., 2014; MEDEIROS et al., 2018).

À luz da governança corporativa, quando não há influência positiva da liderança, pode haver desvio comportamental por partes dos colaboradores (MOORE, 2015). A potencial vulnerabilidade na conduta de gestores e colaboradores e a falta de confiança na alta gestão em empresas de diversos segmentos, tamanhos ou localizações, estimula a ascensão de um outro modelo de liderança: a Liderança Autêntica com objetivo de restaurar a confiança em todos os níveis de gestão das organizações (LUTHANS; AVOLIO, 2003; AVOLIO; GARDNER, 2005; WALUMBWA et al.,2008). Avolio e Gardner (2005) argumentaram que a liderança autêntica inclui uma perspectiva moral caracterizada por elevados padrões éticos que orientam a tomada de decisões e o comportamento dos colaboradores.

A liderança é considerada um fenômeno fundamental na criação de valor nas empresas, tanto no desenho de processos, quanto no comportamento dos colaboradores pois, por meio da influência, é possível fazer com que os funcionários executem, de forma eficaz, as políticas e estratégias definidas pela organização, sempre com o objetivo de trazer bons resultados à organização (FONSECA et al., 2015).

À luz das competências individuais, alguns colaboradores possuem habilidades distintas na compreensão e uso dos recursos tecnológicos. Esses indivíduos possuem alto nível de conhecimento, informação e habilidade relacionada às tecnologias da informação e comunicação (TICs), e, portanto, têm a capacidade de se adaptarem rapidamente às mudanças tecnológicas, e conseguem lidar melhor com o estresse atribuído ao tempo de aprendizagem desses recursos (YE, 2018). É compreensível, por tanto, que possa haver fatores que antecedem a violação das políticas de segurança da informação, entre os quais o desengajamento moral e habilidade tecnológica, sendo estes fatores apontados como dimensões significativas para a ocorrência desse fenômeno.

Assim, formula-se a seguinte questão de pesquisa: Qual o efeito das habilidades tecnológicas, penalidades organizacionais, desengajamento moral e

da liderança autêntica no comportamento de violação de políticas de segurança da informação? Dado que os conceitos de Desengajamento Moral e Liderança podem contribuir com violações de Segurança de Informação, o objetivo desse artigo consiste na investigação desses fatores antecedentes associados aos comportamentos que podem tornar vulneráveis os sistemas de informação organizacionais.

2 REFERENCIAL TEÓRICO

A proteção das informações, por meio das tecnologias da informação, está se tornando uma questão mais séria no mundo, conforme tem aumentado a quantidade de compartilhamento de conhecimento e transações *on-line* entre indivíduos e organizações (BARLOW et al., 2013).

O uso indevido de informações organizacionais pelos colaboradores pode ocasionar problemas relevantes de segurança da informação e levar as empresas à perda de credibilidade e danos monetários (CHUA; WONG; LOW; CHANG, 2018). O roubo de grandes somas de dinheiro, por meio do uso indevidos de tecnologias, no local de trabalho, também se soma aos riscos para segurança. Outra grande ameaça são aqueles colaboradores que passam informações da companhia a fraudadores externos, especialmente, ex-funcionários (BARLOW et al., 2013).

Para que essas ameaças não se tornem problemáticas aos sistemas organizacionais, e que não haja nenhum tipo de violação à segurança de informação nas empresas, designa-se aos colaboradores das organizações utilizar as ferramentas de proteção para mitigar os riscos de violação de políticas eminentes (AURIGEMMA; PANKO, 2012; FLOWERDAY; TUYIKEZE, 2016). Para incentivar o uso adequado de sistemas de segurança organizacional, as empresas criam e implementam políticas de segurança da informação (BÉLANGER et al., 2017).

Uma política de segurança da informação de uma organização define um conjunto de regras e políticas relacionadas ao acesso dos funcionários e uso de ativos de informação (YAZDANMEHR; WANG, 2016). Essas políticas de segurança da informação (PSI) estabelecem funções e responsabilidades aos colaboradores usuários, ao descreverem questões específicas voltadas à

segurança, textos que estabelecem proteção de recursos de informação nas organizações (AURIGEMMA; PANKO, 2012).

A norma ABNT NBR ISO/IEC 27002 releva a importância da organização interna para que as organizações definam alguns aspectos tais como: As responsabilidades pela proteção de cada ativo e o cumprimento de processos de segurança da informação; As responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e, em particular, pela aceitação dos riscos residuais; As responsabilidades sejam complementadas, quando necessário, com orientações mais detalhadas para locais específicos e recursos de processamento da informação (ABNT 27002, 2013).

A segurança da informação se caracteriza pelo controle da informação, de forma que ela esteja disponível e íntegra, estritamente para quem precisa delas. Para se obter este controle, é necessário lançar mão de uma série de ações capazes de evitar os riscos de que elas possam ficar indisponíveis, sem confiança ou compartilháveis de forma indesejada (SANTOS; CAPPELLOZZA; ALBERTIN, 2018).

A gestão da política de segurança da informação é cada vez mais necessária nas organizações, haja visto a incidência cada vez maior de crimes cibernéticos. Deve-se lidar com estes aspectos a fim de se cumprir com as políticas, tarefa que deve ser de muita responsabilidade em todo o ambiente organizacional. Algumas organizações têm a responsabilidade legal de proteger as informações que estão sob a sua guarda, evitando o acesso não autorizado desses ativos, além de cuidar para que a partilha de informações com terceiros siga todas as medidas de segurança com o zelo correspondente ao grau de criticidade deste acesso (SOLOVE, 2007).

Quando uma organização depende de sistemas baseados em TI para permanecer viável, a segurança das informações e a disciplina de gerenciamento de riscos devem se tornar parte integrante da base econômica para a tomada de decisões de negócios. Essas decisões são baseadas em *trade-offs* entre os custos da aplicação de controles do sistema de informações e os benefícios do uso de sistemas seguros e disponíveis. Em geral, as políticas organizacionais de segurança da informação são implementadas por meio de comitês de segurança, compostos por indivíduos de diferentes segmentos da organização; entretanto, tais aceites são protocolares e, eventualmente, as

organizações podem não ter o controle necessário para verificar se tais políticas são efetivas, além de eventuais ocorrências de violações das políticas de segurança pelos usuários dos sistemas de informações, sejam eles empregados ou clientes dessas empresas (VON SOLMS, 2006).

2.1 Violação de Política de Segurança de Informação

Embora os profissionais de segurança estejam trabalhando ativamente para melhorar os sistemas empresariais, existe a crescente necessidade de usuários, que podem não, necessariamente, ser especialistas em tecnologia da informação, executarem ações específicas nos sistemas como abrir ou não e-mails suspeitos e usar senhas complexas (BARLOW et al., 2013). Os colaboradores e usuários de sistemas das companhias se tornaram uma das ameaças mais citadas, segundo estudos, na violação dos sistemas de informação (SIPONEN, 2005; FLOWERDAY; TUYIKEZE, 2016; YAZDANMEHR; WANG, 2016; CHUA et al., 2018).

As violações das políticas representam as quebras de acordo, portanto, consistem nos eventos de não conformidade com a política organizacional de segurança da informação, de forma espontânea ou intencional. Para tratar as violações elas podem ser categorizadas de algumas formas: 1) violam as regras conscientemente (os funcionários violam as políticas de segurança que eles sabem que existem); 2) são voluntárias (as ações não são forçadas por outras partes, por exemplo, supervisores); 3) são intencionais (empregados tomam decisões conscientes para se engajar na ação); e 4) não maliciosos (os funcionários não estão tentando causar danos) (GUO, YUAN, 2012).

Os colaboradores que podem violar os sistemas de informações das organizações, mal-intencionados ou não, podem ser: auditores financeiros, clientes, funcionários permanentes ou temporários, ex-funcionários e/ou fornecedores, o que tornam as informações das organizações vulneráveis e faz com que o desenvolvimento de sistemas de segurança tenha que considerar todos tipos de ameaças oriundas de seus próprios atores (FLOWERDAY;TUYIKEZE, 2016; YAZDANMEHR; WANG, 2016; CHANG et al., 2018, SAFA et al., 2018).

Muitos colaboradores têm acesso fácil às informações da companhia, o que não se faz necessário gastar tanto tempo e esforço para acessar as informações almejadas em comparação com os invasores externos (SAFA et al., 2018). A pesquisa apresentada por Barlow et al., (2013) indica que 80% dos diretores que administram áreas relacionadas a sistemas de segurança da informação acreditam que funcionários e contratados apresentam uma ameaça maior aos seus dados do que os hackers externos. Segundo Bélanger et al., (2017), os empresários e gestores também apresentam atitudes de vulnerabilidade no controle de suas senhas, um estudo de 2.500 pequenos empresários, nos EUA, em 2014, revelou que 74,2% mantêm registros escritos de senhas e 63% reutilizam a mesma senha para muitos sistemas, o que expõe os sistemas de informação a suscetíveis ataques ou violação de segurança, devido à falta de parâmetros de segurança por meio do uso indevido de senhas.

No entanto, a distinção entre grandes e pequenas violações, nem sempre são claras, por exemplo, o compartilhamento de uma senha pode parecer uma pequena violação, porém compartilhar senha com um colega mal-intencionado pode ter grandes consequências (BARLOW et al., 2013). Diariamente, inúmeros dados de clientes passam pelas mãos de funcionários que podem ver, compartilhar e usar todas essas informações. As violações de dados podem acontecer devido à divulgação maliciosa e proposital de informações em troca de benefícios, ou não intencionais (CHUA et al., 2018)

Há colaboradores que indicam comportamentos totalmente avessos à garantia de segurança de informações, por meio de comportamentos, que infringem a privacidade, quando os usuários são apresentados a situações em que podem levar algum tipo de vantagem ao expor suas informações que detêm, e essas informações são confidenciais, muitos usuários repassam informações acreditando que obterão benefícios com essas ações transgressoras (MILTGEN; SMITH, 2015).

Há um desafio por parte das organizações na implantação das políticas de segurança da informação, desenvolver e implementar essas normas não é tarefa fácil, são necessárias muitas análises e estudos baseados em requisitos de regulação, averiguar as complexidades das novas tecnologias e ameaças externas e internas na realidade da empresa (FLOWERDAY; TUYIKEZE, 2016). O desafio para as organizações é saber como transformar usuários da maior

ameaça da segurança da informação ao principal recurso de defesa em conformidade de política e segurança das informações (AURIGEMMA; PANKO, 2012).

Alguns estudos apontam que o comportamento não ético dos colaboradores e ou usuários podem ter sido desenvolvidos, ainda no processo de formação acadêmica, em experiências relacionadas à participação desses indivíduos em grupos, pelos quais se expõem a outros tipos de valores (TANIGUCHI; SANCHEZ; CAPPELLOZZA; FILENGA, 2011).

Um dos motivos que podem levar os colaboradores a violarem os sistemas de informação, é a racionalização de senha. A maioria das empresas implementaram algum sistema de tecnologia da informação, com a racionalização de senha, por parte das empresas, os usuários usam como meio de justificar suas ações errôneas de violação, mesmo quando fortes punições organizacionais constam nas políticas para violações. Ao racionalizar as senhas, os funcionários tentam reduzir sua culpa ou vergonha por ter a intenção de violar as políticas de TI. Já a neutralização da “defesa da necessidade” é usada quando um indivíduo pretende violar uma política que a ação foi necessária, dado que a escolha não dependia apenas do usuário sob a forma de desengajamento moral (BARLOW et al., 2013).

2.2 Desengajamento Moral

O comportamento dos colaboradores é motivo de preocupação constante na gestão de pessoas que busca modelos que possam prever tais comportamentos, adequá-los ao perfil requerido a fim de se atender as necessidades da organização, bem como criar harmonia entre as características individuais e objetivos organizacionais (KRISTOF, 1996).

As organizações demandam algumas decisões que podem envolver conflitos de valores e estão sujeitas a comportamentos dos decisores que podem ser influenciados a partir de aspectos subjetivos, éticos e do contexto da situação em questão. O comportamento ético é aquele consistente com os princípios, as normas e os padrões das práticas de negócios devidamente acordadas com a sociedade, sendo que os dilemas éticos existentes nos negócios são totalmente previsíveis (TREVIÑO; NELSON, 2011).

Agentes estressantes predizem comportamentos indesejáveis dos colaboradores, como improdutividade e desvios de conduta moral. A racionalização por parte dos colaboradores pode ser explicada pela teoria cognitiva social e pela teoria do desengajamento moral, sendo este último composto por mecanismos cognitivos que desativam o processo de autocontrole no indivíduo para que ele possa agir de maneira diferente, e inadequada, da sua própria atitude natural, formada por valores éticos e morais que o caracteriza (BANDURA, 1990).

Há vários mecanismos antecedentes que podem efetivar este comportamento, entre eles, o deslocamento de responsabilidade, em que o indivíduo se desvia da responsabilidade de um ato direcionando-o a outro, ou a difusão da responsabilidade em que a atribuição do ato é diluída entre o grupo, ou redução do efeito dos atos, a partir da negação da existência de problemas ou de suas consequências (DETERT et al., 2008).

Os escândalos organizacionais exibidos, nos mais diversos canais de comunicação, pressupõem questionamento sobre o porquê de as pessoas agirem de forma transgressora, e muitas teorias buscam justificar tais comportamentos, inclusive as que associam o desengajamento moral como causa dessas ações (REYNOLDS; DANG; YAM; LEAVITT, 2013).

Em comparação com outros famosos modelos cognitivos de tomada de decisões morais, a Teoria Cognitiva Social se baseia nos indivíduos que podem se desvincular de seus próprios padrões morais, cometendo atos imorais (REYNOLDS et al., 2013). O Desengajamento Moral é uma construção central da Teoria Cognitiva Social do pensamento e ação moral, desenvolvida por Albert Bandura, em seu primeiro livro seminal sobre Teoria do cognitivo social em 1991 (KAVUSSANU; HATZIGEORGIADI; ELBE; RING, 2016).

Segundo Bandura (1991), a Teoria Cognitiva Social do Desengajamento Moral propõe que os indivíduos desenvolvam padrões morais que regulem comportamentos durante a socialização, seja no convívio familiar, ou profissional, por meio de autoavaliação. As pessoas se abstêm de agir de maneira correta, a fim de violarem seus padrões morais, pois se desafiam a agir ao que está errado, segundo seus preceitos (BANDURA, 1991).

Os padrões morais não funcionam como reguladores da conduta, pois existem manobras psicossociais pelas quais as ações morais podem ser,

seletivamente, desprendidas de conduta maléfica e alguns dos mecanismos cognitivos de desengajamento moral centram-se na reconstrução dessa conduta. As violações podem ser desvinculadas das atitudes negativas, por meio do uso de mecanismos cognitivos de desengajamento, que permitem diferentes comportamentos por parte dos indivíduos com os mesmos padrões morais (KAVUSSANU et al., 2016).

Tais mecanismos cognitivos buscam minimizar, justificar ou obscurecer a ação do transgressor no dano causado seja a algo ou alguém, desconsiderando ou distorcendo as consequências prejudiciais do comportamento ou/e desumanizando ou culpando a pessoa transgressora passando-a à vítima (BANDURA, 1991). Os mecanismos cognitivos desenvolvidos por Bandura foram classificados por Kavussanu et al., (2016) em grupos. No Quadro 1, é possível identificar alguns desses grupos.

Quadro 1 - Mecanismos Cognitivos de Desengajamento Moral

Mecanismo Cognitivo	**Definições**
Justificativa moral	Implica a reestruturação cognitiva de um comportamento prejudicial (ruim) em um louvável (bom), fazendo parecer aquilo que é moralmente não aceitavel pela sociendade, pareça aceitavel.
Eufemismo	Envolve o uso da linguagem para disfarçar o comportamento erroneo, afim de torná-lo menos prejudicial.
Distorção das consequências	Ocorre quando há a tentativa de minimizar, esconder e/ou evitar para a sociedade as consequências de erros dos indivíduos.

Fonte: Adaptado de BANDURA (1991) e KAVUSSANU et al*.,* (2016)

Alguns aspectos específicos relacionados ao ambiente de SI podem causar pressão aos colaboradores e estimulam emoções negativas. Sob este aspecto, o desengajamento moral pode ser compreendido como uma forma de se reduzir as tensões e restaurar a estabilidade emocional, ou seja, uma função de enfrentamento instrumental capaz de fazer como que os colaboradores possam recuperar um certo grau de controle psicológico. O desengajamento moral aparece de forma multifacetada, e entre estas manifestações estão: a folga social que se caracteriza pela diminuição intencional de esforço individual de um colaborador quando ele é submetido a uma atividade em grupo, o enfraquecimento de colegas, a trapaça e *hacking* de computadores (D'ARCY; HERATH; SHOSS, 2014).

O ataque e violações às políticas organizacionais de segurança da informação podem ter várias motivações, mas o desengajamento moral de colaboradores aparenta ser um fator significativo, tendo em vista as suas características e ainda por cima, difíceis de serem detectados pois são vistos como integrantes do time, onde menos se espera eventuais rupturas morais (D'ARCY, HERATH; SHOSS, 2014).

Esta abordagem pode ser aprofundada a partir do conhecimento de que os colaboradores possam ter maior conhecimento acerca das tecnologias, percepção da importância dos dados corporativos com os quais manipulam de forma direta ou indiretamente. Assim, elabora-se a primeira hipótese desse estudo:

Hipótese 1 (H1): O desengajamento moral influencia positivamente a violação de política organizacional de segurança da informação

Além dos aspectos relacionados ao agenciamento humano, a Era da Informação proporciona uma dinâmica única aos indivíduos que precisam se adaptar rapidamente às mudanças em curso. Sem dúvidas, as mudanças envolvem adaptações tecnológicas que, embora tenham por objetivo geral reduzir custos e diminuir tempo dos processos, podem, eventualmente, impactar nas instruções de trabalhos de forma a torná-las mais elaboradas, paradoxalmente (LIPNACK, STAMPS 1999).

Num ambiente corporativo, tais mudanças não são, necessariamente, bem-vindas. Há todo um processo de implantação de novas tecnologias que enfrentam resistência na cultura organizacional, de forma que elas são efetuadas de cima para baixo, para que a alta direção possa determinar um ritmo capaz de enfrentar as resistências que certamente virão com um certo grau de sucesso (HENDERSON, RUIKAR 2010).

Para enfrentar os desafios, em particular, aqueles relacionados ao uso adequado de novas tecnologias da informação e comunicação, surge a figura do indivíduo habilidoso tecnologicamente ou, no idioma inglês, *Techno-savvy*. O termo refere-se a um indivíduo que possui um diferencial em compreender os alcances de uma determinada tecnologia e adaptá-la para os mais diversos usos, aos mais diversos ambientes e aos mais variados graus de habilidades

existentes em um determinado ambiente. Com isso, este indivíduo se torna essencial para tornar simples algo aparentemente complexo (BROWN, MURPHY, NANNY, 2003).

2.3 Habilidade Tecnológica

Quando a Internet ainda estava se popularizando e tornando-se acessível ao público, já se havia alguma ideia de que algumas profissões iriam usufruir desta tecnologia, tanto do ponto de vista profissional quanto acadêmico. Advogados, e profissionais de direito poderiam, por exemplo, poderiam se comunicar com clientes, alunos independentemente do seu local de trabalho por meio de fibras óticas (VANDAGRIFF, 1995).

Nesta época, as possibilidades aos profissionais da nutrição ligados a tecnologia, se multiplicavam, desde o estudo de práticas de dieta que consideravam o projeto Genoma Humano em que os marcadores genotípicos auxiliavam uma possível resposta de um paciente a uma dada intervenção dietética, ou da telemedicina, levando programas de alimentação saudável aos lugares mais remotos, ou ainda na escolha de softwares de análise de nutrientes (MONSEN, 1999).

Alguns estudos mostram a efetividade deste tipo de indivíduo. Nas microempresas domésticas, em sua grande parte com poucos ou quase nenhum recurso, a adoção e difusão das tecnologias da informação e comunicação mostram o uso intensivo de internet, e-mail e celular para as atividades de negócio em níveis escalares de crescimento (regional, nacional internacional), sendo isso possível a partir do momento em que os sócios proprietários dessas microempresas tem o perfil de *Techno-savvy* (CLARK, DOUGLAS, 2011).

Entretanto, as facilidades advindas com as tecnologias da informação e comunicação também consistem em alguns problemas aos indivíduos *Techno-savvy*. Uma pesquisa qualquer no site de informações Google possui uma imensa variedade de respostas, ordenadas por um critério estipulado em popularidade das mesmas, sendo que a imensa maioria das pessoas possuem dificuldades em filtrar quais delas realmente são relevantes, até porque a popularidade das páginas sugeridas pelo mecanismo se baseia em mapas de

hiperlinks alimentados pela subjetividade dos seus visitantes (BRIN, PAGE, 1998).

As habilidades de um *Techno-savvy* parecem estar acima de um alfabetizado em tecnologia, mas há limites. Elas não incluem especificidades relacionadas a aplicação em si. Um estudo mostrou que estudantes universitários que simplesmente possuem certa facilidade em buscar informações acadêmicas para apoiar suas atividades acadêmicas não possuem certos cuidados que um especialista em pesquisa de informação possui as quais incluem, o planejamento necessário para determinar a natureza da informação necessária, acessá-la de forma eficaz e eficiente, a análise crítica das informações e fontes, utilização da informação de forma eficaz para um propósito e compreensão das questões econômicas, jurídicas e sociais acerca do uso de informações para o uso ético e legal (BROWN, MURPHY E NANNY, 2003).

Por este aspecto, um *Techno-savvy* aparenta ter um perfil que irá ajudá-lo em sua ação, por ser um entusiasta natural do uso de tecnologia, entretanto, como um *Techno-savvy* tem uma noção do que este ataque irá proporcionar, do ponto de vista das consequências desastrosas para a organização e do uso negativo de tecnologia. Portanto formula-se a seguinte hipótese:

Hipótese 2 (H2): A Habilidade Tecnológica influencia negativamente a violação de política de segurança.

A alta gestão das companhias está menos tolerante quanto à leviandade relacionada aos princípios, valores e condutas inferidas e recomendam aos seus líderes que operem em total integridade, o que pode influenciar, positivamente, o comportamento dos colaboradores (WALUMBWA et al., 2008). Assim, o líder tem papel fundamental para equilibrar o que está estabelecido no código de ética, nas políticas e na conduta moral com a conduta profissional e ética de seus colaboradores (SANTOS; GUEVARA; AMORIM; FERRAZ-NETO, 2012).

Em meio ao surgimento de novos cenários competitivos, dada a velocidade das mudanças tecnológicas, há a necessidade de se manter a credibilidade dos líderes para com seus liderados e uma relação de confiança entre todos os colaboradores dentro das empresas. Nesta direção emerge a

Liderança Autêntica que possui componente ético nas ações desses líderes (LUTHANS; AVOLIO, 2003).

2.4 Liderança Autêntica

Um líder autêntico é definido como aquele que baseia suas próprias experiências pessoais, sejam pensamentos, emoções, necessidades, desejos, preferências ou crenças. Consiste “em quem” age de acordo sua verdade, expressando-se de maneira consistente, sem perder valor ditos como positivo pela sociedade (AVOLIO; GARDNER, 2005; WALUMBWA et al., 2008; WEISS et al., 2017)

Cabe ao líder autêntico empenho, tanto no cumprimento da regra, quanto nas ações de conscientização, prevalecer a ética, por meio de ações baseadas em pilares comportamentais éticos e morais, o que o torna admirado pelos seus liderados (SANTOS; GUEVARA; AMORIM; FERRAZ-NETO, 2012)

Kernis e Goldman (2006) definem autenticidade como o encontro de suas características, por meio do resultado de um exercício na identificação pessoal. Para que os indivíduos reconheçam sua autenticidade, é necessário conhecimento de suas necessidades, valores, sentimentos e aspectos de personalidade.

Os líderes autênticos motivam e inspiram seus funcionários baseado em princípios como bom comportamento, moralidade, verdade e transparência, a prestarem um bom serviço ao cliente, não apenas para cumprirem o padrão, mas sim a fim de agregar valor à companhia, aos acionistas e, assim, construírem organizações duradouras. O líder autêntico apresenta a capacidade de planejar, analisar, comunicar e tomar decisões firmadas em seus dilemas éticos (AVOLIO; GARDNER, 2005). Em relação à promoção dessas capacidades do líder autêntico Walumbwa et al. (2008) acrescentaram alguns atributos à Liderança Autêntica em relação às suas ações do líder ante a seus liderados, atributos esses que convergiram a quatro dimensões subjacentes, nomeadas de capacidades psicológicas positivas. São elas: Autoconsciência, Perspectiva moral interna, Processamento equilibrado e Transparência relacional

A autoconsciência é uma das capacidades, psicologia positiva definida como o autoconhecimento e a autoconfiança de um líder, baseados em suas

crenças, sentimentos, pontos fortes e fracos, anseios e a autocompreensão do quanto seu comportamento impacta nas outras pessoas (WALUMBWA et al., 2008). Segundo Fidalgo (2018, p.55) “a autoconsciência não só ajuda os líderes autênticos a conhecerem-se a si mesmos, mas também ajuda a mostrar aos seus seguidores a autenticidade da sua liderança”.

A Transparência Relacional é definida como o comportamento que demonstra por meio de discursos, conversas abertas e compartilhamento de seus verdadeiros pensamentos e sentimentos, minimizando as exibições de emoções inadequadas, transparecendo os pensamentos e sentimentos verdadeiros (WALUMBWA et al., 2008).

A Perspectiva Moral Interna trata da demonstração e autorregulação dos valores éticos e morais de um líder, independentemente da situação, organização, experiências; seus verdadeiros valores e padrões internalizados são demonstrados mesmo sob pressões organizacionais, grupais e sociais (AVOLIO; GARDNER, 2005; WALUMBWA et al., 2008).

O Processamento Equilibrado refere-se aos líderes que mostram e analisam, objetivamente todos os dados relevantes antes de sua tomada de decisão, lidam com as considerações dos outros sobre as informações e reflexões mais profundas do líder (AVOLIO; GARDNER, 2005; WALUMBWA et al, 2008). Segundo Fidalgo (2018), esse conceito se caracteriza pela ausência de distorções interpretativas no processamento das informações recebidas pelo líder com o suporte de opiniões externas como uma maneira de ampliar a sua visão sobre a questão em análise.

Os líderes que demonstram comportamentos antiéticos incentivam o desvio de comportamento de seus subordinados, já os líderes que têm seu comportamento e sua gestão baseada na ética, na moral e nos cumprimentos das políticas internas inspiraram a boa conduta de seus liderados, logo, a liderança autêntica pode comedir o desvio de conduta dos colaboradores (MOORE, 2015; WEISS et al., 2017).

Quando os funcionários entendem que seu líder é um profissional honesto, tem uma gestão transparente e ética, cresce a confiança dos funcionários, o que evidencia a autenticidade e o bom comportamento da equipe, o que pode influenciar que colaborador não desempenhe mal comportamento,

dado o bom exemplo de seu líder (LUTHANS; AVOLIO, 2003; MOORE, 2015; PECK; HOGUE, 2017; WEISS et al., 2017).

Quanto maior for a conexão entre o líder autêntico e sua equipe, maior será o seu poder de persuadir ou motivá-los, tais líderes têm a facilidade de inspirar seus liderados, dada sua gestão transparente, discutir abertamente suas vulnerabilidades e as dos colaboradores, políticas internas, metas e resultados esperados pela empresa, enfatizando constantemente o engajamento entre líder e seus liderados (AVOLIO et al., 2004).

Segundo Avolio et al. (2004), o líder autêntico tem a capacidade de influenciar seus liderados, quando ambos se associam aos mesmos propósitos. Sendo um dos principais desafios do líder autêntico, identificar os pontos fortes dos colaboradores e ajudar a direcionar e construir comportamentos alinhados ao propósito politicamente correto da corporação ao qual estão inseridos. Desta forma, elabora-se a seguinte hipótese:

Hipótese 3: A Liderança Autêntica influencia negativamente a violação de políticas de Segurança da Informação.

2.5 Penalidade Percebida

Estudos que utilizaram a teoria geral de dissuasão (TGD) indicam que quanto maior for a certeza e a severidade das penalidades aplicáveis em função de um ato ilícito praticado, mais os indivíduos tendem a ser dissuadidos de praticar esse ato (GIBBS, 1975; NAGIN; POGARSKY, 2001). Neste aspecto, a certeza de penalidades refere-se à alta probabilidade de um indivíduo ser punido, enquanto a severidade das penalidades está ligada ao grau de punição associada a cometer um ato ilícito.

Os indivíduos com alto comprometimento com a moral, geralmente são muito sensíveis com relação à certeza das punições a que estão sujeitos, uma vez que, não importa qual seja a penalidade prevista, eles considerariam muito desagradável serem acusados de um ato considerável socialmente indesejável (D'ARCY; HOVAV; GALLETTA, 2009). Já os indivíduos com baixo comprometimento moral estão mais preocupados com a penalidade que lhes seriam imputadas decorrentes do seu comportamento.

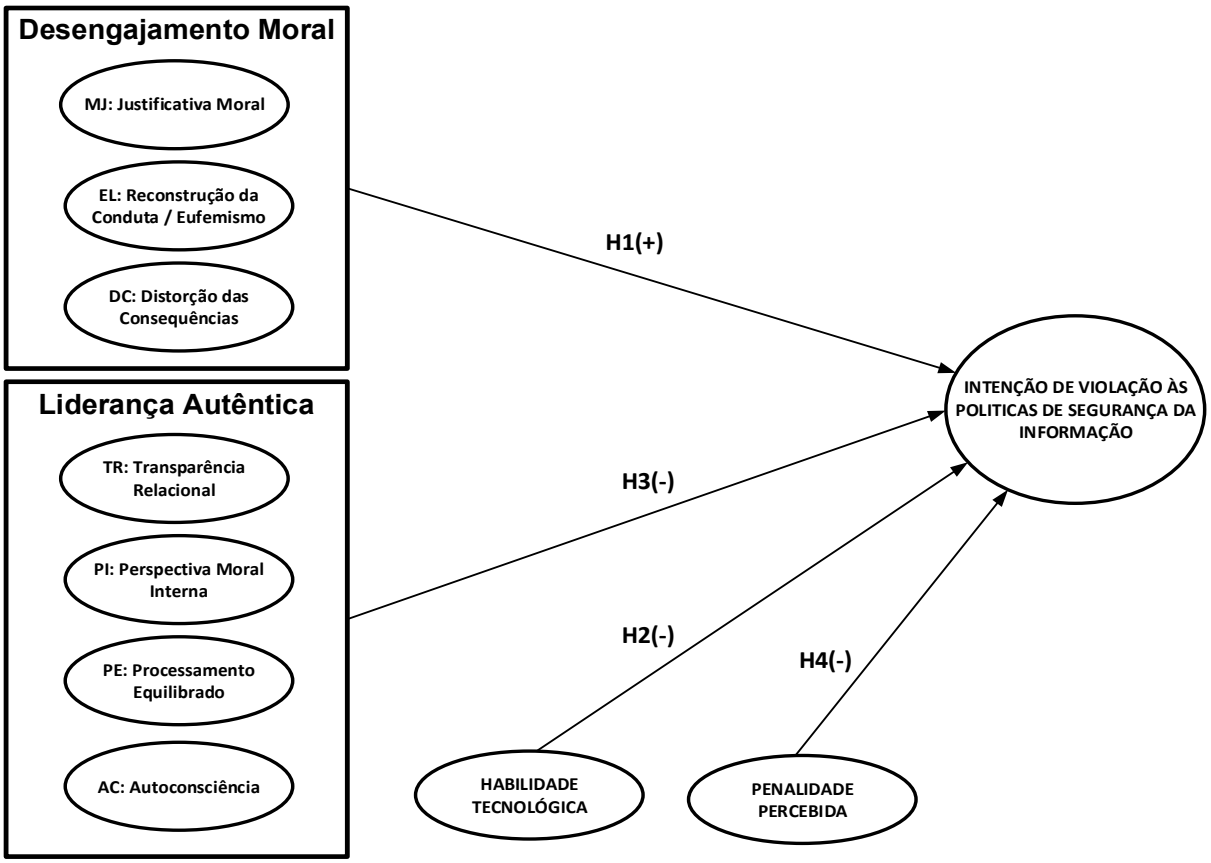
Em termos de segurança da informação, os possíveis efeitos da aplicação de severas penalidades, as fortes pressões organizacionais, e a eficácia percebida das ações punitivas aos infratores, fazem com que os funcionários tenham um mais claro entendimento e aumentem seu comprometimento com as políticas de segurança da informação implantadas em suas organizações (HERATH; RAO, 2009). Para os autores, as pressões exercidas por normas subjetivas e atitude dos colegas de trabalho influenciam os comportamentos com relação à segurança da informação, por parte dos funcionários. Em seu estudo, ao analisar as penalidades aplicáveis a atos ilícitos, a certeza de que ocorreria a detecção, e consequente punição desses atos foram consideradas significativas (HERATH; RAO, 2009).

Guo e Yuan (2012) propuseram e testaram empiricamente um modelo de mediação com o intuito de examinar os efeitos das sanções multiníveis na prevenção de violações de segurança da informação no local de trabalho. Os resultados do experimento indicaram que as auto-sanções pessoais e as sanções do grupo de trabalho têm efeitos dissuasivos significativos sobre as tentativas de violações de segurança por parte funcionário (GUO; YUAN, 2012). Constataram também que os efeitos das sanções organizacionais se tornam praticamente insignificantes quando os outros dois tipos de sanções são levados em consideração, ou seja, as auto-sanções pessoais e sanções informais do grupo de trabalho (GUO; YUAN, 2012), o que os levaram a concluir que a estratégia de influenciar pode ser mais eficaz do que fazer cumprir uma estratégia de gestão de segurança da informação

Hipótese 4: A Penalidade Percebida influencia negativamente a violação de políticas de Segurança da Informação.

Portanto, a partir das quatro hipóteses formuladas previamente, a Figura 1 apresenta o modelo conceitual de pesquisa proposto.

Figura 1 - Modelo conceitual



Fonte: elaborado pelos autores

3 PROCEDIMENTOS METODOLÓGICOS

Neste estudo adota-se uma abordagem metodológica quantitativa e de corte transversal, pois os dados foram coletados em um só ponto no tempo e sintetizados estaticamente. Os dados podem ser considerados primários, pois foram coletados, especificamente, para completar o projeto de pesquisa (HAIR et al., 2005). O método quantitativo parte da quantificação, tanto na coleta quanto no tratamento das informações e faz uso de técnicas estatísticas, com o objetivo de evitar possíveis distorções de análise e interpretação nos resultados (DALFOVO, 2008).

Já o propósito da análise confirmatória foca o estudo na análise das relações entre os indicadores e variáveis observadas, partindo da pontuação dos itens nas escalas utilizadas, originárias dos instrumentos de medida (LEÓN, 2011). Os cálculos e validações dos testes estatísticos foram desenvolvidos por meio da técnica de análise multivariada de Modelagem por Equações Estruturais

por Mínimos Quadrados Parciais (MEE-MQP), com o software SmartPLS 3.0M3 (RINGLE; WENDE; BECKER, 2015).

A abordagem MEE-MQP foi escolhida devido à sua capacidade de examinar a previsão e explicação dos construtos, também fornecendo um ponto comum entre a análise confirmatória e a modelagem de caminho (Hair et al., 2019). A utilização do MEE-MQP justifica-se também pela utilização de duas variáveis latentes hierárquicas (construtos de 2ª ordem) (Ringle et al., 2018). Os construtos de primeira ordem são reflexivos, enquanto os construtos de segunda ordem são formativos. Além disso, o PLS-SEM supera a aparente dicotomia entre explicação e previsão, que é a base para o desenvolvimento de implicações gerenciais (Hair et al., 2019).

O instrumento de coleta de dados utilizado na pesquisa foi um questionário composto por perguntas fechadas, que abordam cinco dimensões: Intenção de Violação de Política de Segurança da Informação, Desengajamento Moral, Liderança Autêntica, Penalidade Percebida e Habilidade Tecnológica. Neste estudo foram utilizadas escalas internacionais traduzidas do idioma inglês para o português e avaliadas por três professores doutores pesquisadores da área de Administração e atuantes em programas Stricto-Sensu.

Para testar as quatro hipóteses propostas no modelo conceitual da pesquisa, utilizou-se de escalas validadas do tipo Likert. As escalas são de 5 pontos onde (1) representa que o respondente “Discordo totalmente” e (5) “Concordo totalmente” sobre cada afirmativa. O Quadro 2 apresenta os construtos originais e seus autores, que serviram de base para a elaboração do instrumento de medida.

Quadro 2. Instrumento de Medida.

Dimensões	Subdimensões	Referências
Intenção de Violação de Política de Segurança de Informação Penalidade Percebida		D’arcy, Hovav, Galletta (2009).
Desengajamento Moral	- Justificativa Moral - Eufemismo - Distorção das Consequências	Bandura, Barbaranelli, Caprara, Pastorelli (1996).

Habilidade Tecnológica *(Techno-Savvy)*	- Transparência Relacional - Perspectiva Moral Interna - Processamento Equilibrado - Autoconsciência	Ye (2018).
Liderança Autêntica	- Transparência Relacional - Perspectiva Moral Interna - Processamento Equilibrado - Autoconsciência	Rego, Sousa, Marques, Cunha (2012).

Fonte: elaborado pelos autores

A coleta de dados dessa pesquisa ocorreu por meio de uma aplicação de questionário presencial. Foram aplicados 534 questionários sendo, deste total, considerados 456 questionários completos como válidos. Todos os respondentes atuavam com sistemas de informação em suas empresas no momento da coleta. Considerou-se o tamanho da amostra coletado como adequado, pois o tamanho mínimo da amostra calculado foi igual a 85 participantes de acordo com software G*Power 3.1.5. (FAUL; ERDFELDER; LANG; BUCHNER, 2007; FAUL; ERDFELDER; BUCHNER; LANG, 2009).

Quanto ao gênero, 47,4% dos respondentes eram mulheres e a idade média calculada dos respondentes foi igual a 25,5 anos e o tempo médio de experiência na empresa atual foi igual cinco anos, o que nos possibilita a inferir que os respondentes devem ter vivenciado situações que envolvem as políticas de segurança das empresas que atuam.

3.1 Avaliação do modelo de mensuração e estrutural

A avaliação do modelo conceitual foi realizada por meio da avaliação do modelo de mensuração e do modelo estrutural. O modelo apresenta dois construtos de segunda ordem formativos (desengajamento moral e liderança autêntica) e três construtos de primeira ordem reflexivos (habilidade tecnológica, penalidade percebida e intenção de violação às políticas de segurança da informação). Para estimar os parâmetros do modelo, a abordagem em dois estágios foi escolhida (BECKER; KLEIN; WETZELS, 2012; HAIR et al., 2019).

A avaliação do modelo da segunda etapa iniciou-se com a avaliação do modelo reflexivo. A consistência interna, confiabilidade composta, validade convergente e validade discriminante dos construtos reflexivos foram avaliados (HAIR et al., 2019). A Tabela 1 apresenta os indicadores necessários para a

avaliação de construtos reflexivos e, depois de alguns ajustes com exclusão de indicadores dos construtos habilidade tecnológica, transparência relacional, perspectiva moral interna e processamento equilibrado, no modelo ajustado todos os valores estão dentro do estabelecido por Hair et al. (2019).

Tabela 1 - Sumário da Avaliação dos Modelos de Mensuração – Construtos de 1ª Ordem

Constructos	INT	LA-AC	LA-PE	LA-PMI	LA-TR	OC-DC	PS	RC-EL	RC-MJ	TSV
INT	**0.954**									
LA-AC	-0.038	**0.872**								
LA-PE	-0.048	0.696	**0.867**							
LA-PMI	0.087	0.329	0.331	**0.776**						
LA-TR	0.105	0.483	0.461	0.398	**0.719**					
OC-DC	0.528	0.004	-0.073	0.000	0.079	**0.886**				
PS	-0.605	0.090	0.129	0.028	-0.004	-0.382	**0.874**			
RC-EL	0.594	-0.091	-0.125	0.010	0.030	0.694	-0.495	**0.830**		
RC-MJ	0.582	0.011	-0.059	0.043	0.094	0.802	-0.416	0.718	**0.887**	
TSV	0.120	0.100	0.090	0.085	0.093	0.134	-0.070	0.092	0.141	**0.706**
Alha de Cronbach	0.900	0.901	0.719	0.547	0.740	0.863	0.896	0.771	0.865	0.748
Confiabilidade Composta	0.953	0.927	0.856	0.728	0.807	0.916	0.928	0.868	0.917	0.792
Variância Média Extraída	0.909	0.760	0.752	0.603	0.517	0.785	0.764	0.688	0.787	0.500

Nota: INT: intenção de violação; LA-AC: autoconsciência; LA-PE: processamento equilibrado; LA-PMI: perspectiva moral interna; LA-TR: transparência relacional; OC-DC: distorção das consequências; PS: penalidade percebida; RC-EL: reconstrução da conduta; RC-MJ: justificativa moral; RC-MJ: justificativa moral; TSV: habilidade tecnológica
Fonte: elaborado pelos autores

Após a validação no modelo no primeiro estágio, os escores das variáveis latentes dos construtos foram obtidos do modelo que não considerou os construtos do nível de segunda ordem. Na segunda etapa, as pontuações das variáveis latentes obtidas na primeira etapa foram utilizadas como indicadores (BECKER; KLEIN; WETZELS, 2012) para os construtos desengajamento moral e liderança autêntica.

No segundo estágio, a validade convergente, a colinearidade e a significância estatística e a relevância dos construtos formativos foram avaliadas. A validade convergente foi estimada a partir do valor do coeficiente de caminho do construto formativo. Valores de coeficiente de caminho maiores que 0,8 fornecem suporte para a validade convergente do construto formativo (HAIR et al., 2019). O valor do coeficiente de caminho do construto de nível de segunda ordem desengajamento moral foi de 0,955 e da liderança autêntica foi de 0,853, apoiando a validade convergente dos construtos. O valor do fator inflado da

variância (VIF) foi usado para avaliar a colinearidade do construto, e verificou-se que todos os valores estavam abaixo de 5 (HAIR et al., 2019). Para avaliar a significância estatística dos construtos, foi utilizada a técnica de *bootstrapping*. Seguindo as recomendações de Hair et al. (2019), todos os itens foram mantidos no modelo.

Para os construtos reflexivos, os mesmos indicadores foram avaliados. A Tabela 2 apresenta os indicadores necessários para a avaliação de construtos reflexivos no segundo estágio de avaliação, e todos os valores estão dentro do estabelecido por Hair et al. (2019). Nenhum novo indicador teve que ser excluído nessa etapa.

Tabela 2 - Sumário da Avaliação dos Modelos de Mensuração – 2º Estágio

Construtos	DM	INT	LA	PS	TSV
DM	FORMATIVE				
INT	0,635	**0,954**			
LA	0,142	0,173	FORMATIVE		
PS	-0,493	-0,605	-0,098	**0,874**	
TSV	0,126	0,120	0,030	-0,070	**0,706**
Alpha deCronbach	FORMATIVE	0,900	FORMATIVE	0,896	0,748
Composta	FORMATIVE	0,953	FORMATIVE	0,928	0,792
Variância Média Extraída	FORMATIVE	0,909	FORMATIVE	0,764	0,500

Nota 1: INT: intenção de violação; PS: penalidade percebida; TSV: habilidade tecnológica; DM: desengajamento moral; LA: liderança autêntica.
Nota 2: Na diagonal em negrito é apresentada a raiz quadrada de AVE.
Fonte: elaborado pelos autores

Na sequência, para avaliação do modelo estrutural, os critérios utilizados foram: colinearidade, cargas fatoriais significativas, coeficientes estruturais e coeficiente de determinação do modelo (R^2) (HAIR et al., 2019). Os valores das cargas fatoriais significativas e dos coeficientes estruturais foram obtidos pela técnica de *bootstrapping*. Na análise da colinearidade, os valores do fator de inflação da variância entre os relacionamentos do modelo foram analisados e constatou-se que estavam abaixo de cinco, conforme o estabelecido por Hair et al. (2019). A Tabela 3 apresenta os coeficientes do modelo estrutural entre os construtos. De acordo com os resultados, apenas os relacionamentos entre desengajamento moral e intenção e penalidade percebida e intenção são significantes.

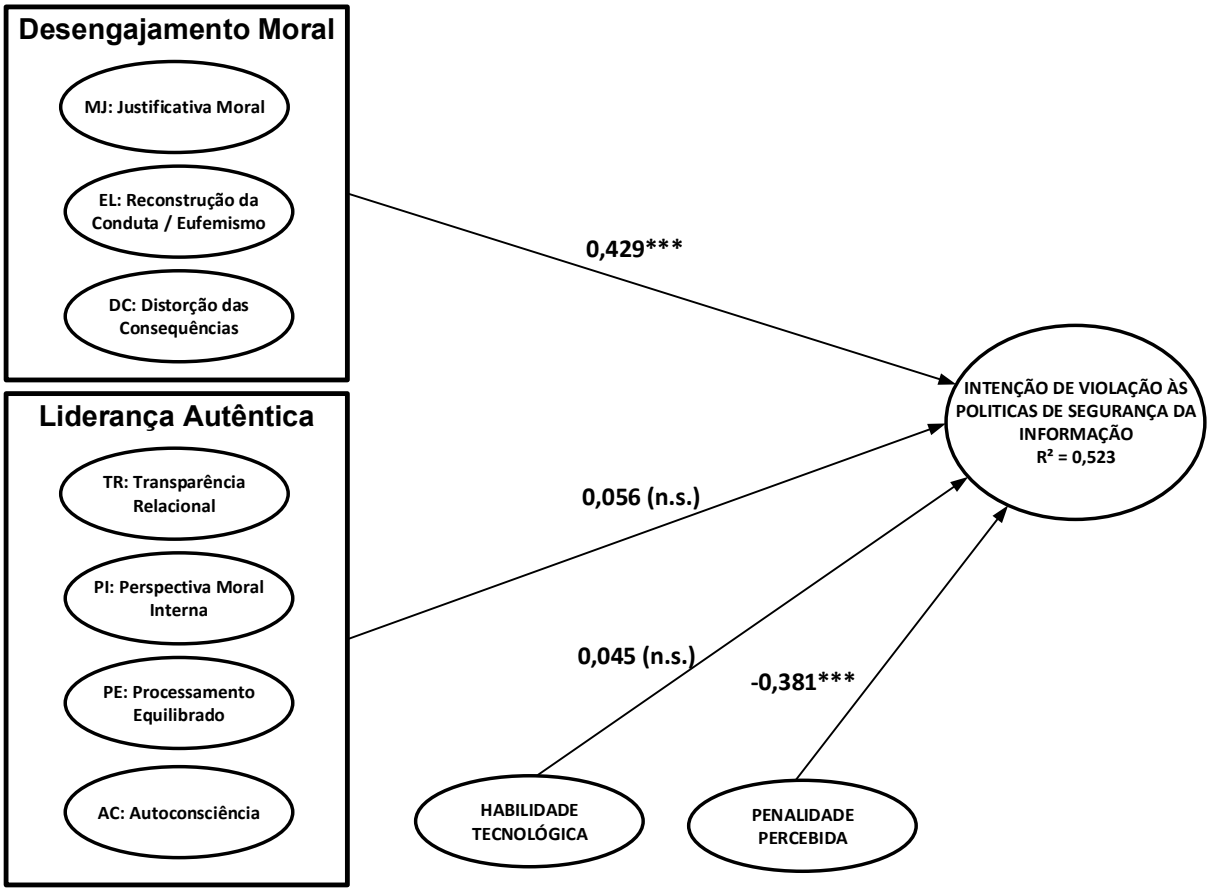
Tabela 3 - Coeficientes do modelo estrutural – entre construtos

Caminho	Média	Desvio Padrão	Estatística T	P Valor
Desengamento Moral -> Intenção	,429	,041	10,571	,000
Habilidade Tecnológica -> Intenção	,045	,044	,845	,398
Liderança Autêntica -> Intenção	,056	,076	,964	,335
Penalidade Percebida -> Intenção	-,381	,042	9,015	,000

Fonte: elaborado pelos autores

O coeficiente de determinação (R^2) foi avaliado conforme os estudos de Cohen (1988) e seu valor apresentou resultado igual 0,523, o que representa um valor significativo dos fatores componentes do modelo como variáveis que explicam a intenção de violação das políticas de segurança. O modelo resultante da pesquisa é apresentado na Figura 2.

Figura 2 - Modelo resultante da pesquisa.



Nota: ***: p-valor<0,001; N.S.: não significante.
Fonte: elaborado pelos autores

A primeira hipótese, que afirma que o Desengajamento Moral influencia positivamente na intenção violação de políticas de segurança da informação foi

confirmada. O resultado positivo dos relacionamentos indica que quanto mais os colaboradores se desengajam, moralmente, mais há intenção de violação de políticas de segurança da informação. A subdimensão Justificativa Moral, quando relacionada com o construto Intenção de Violação de Políticas de Informação, apresenta um resultado positivo e significante, o que vai de encontro com o estudo realizado por D'Arcy et al (2014) e a Justificativa Moral pode ser identificada, quando os colaboradores violam intencionalmente a Política de Segurança da Informação (PSI), e justificam que foi necessária a ação errada para entregar uma atividade com excelência e atender o prazo, pois os colaboradores entendem que mesmo agindo errado a ação foi para atender os interesses da organização.

O resultado positivo e significante do Item Justificativa Moral relacionada à Intenção de Violação de Políticas de Informação, também corrobora com Bandura et al (1996) e D'Arcy et al (2014) quando afirmam que a Justificativa Moral ampara as pessoas em condutas erradas, ato como o apresentado pela vinheta do questionário que compõe este estudo, a justificativa moral explica que a conduta prejudicial realizada passa a ser aceitável e pode trazer resultados positivos para os fins organizacionais.

O resultado da subdimensão Eufemismo relacionado à Intenção de Violação de Políticas de Informação foi positivo e significante. Assim, o Eufemismo, segundo Bandura et al. (1996), fornece uma ferramenta conveniente para mascarar atividades repreensíveis ou até mesmo conferir a elas um status respeitável. O Eufemismo, segundo D'Arcy et al (2014) reduz a dissonância associada à Intenção de Violação de Políticas de Informação em declarações como: "oferecer a senha para um colega de trabalho acessar meu computador é a ação menos grave nesta empresa".

Quando relacionado o Item de Distorção de Consequências do construto Desengajamento Moral, com Intenção de Violação de Políticas de Informação, o resultado é não significante, o que não invalida a primeira hipótese. D'Arcy et al. (2014) exemplifica a distorção de consequências, quando colaboradores violam a política de segurança da informação, por julgar o ato de violar como não prejudicial a organização, pelo menos não diretamente.

Já a Habilidade Tecnológica não obteve significância à intenção de violação, e não corrobora com os dados obtidos por Ye (2018), apesar do autor

relatar que há uma relação moderada entre este constructo e as violações de política de segurança.

A terceira hipótese, que a Liderança Autêntica influencia negativamente na intenção de violação de políticas de segurança da informação, não foi confirmada e não corrobora o estudo de Walumbwa et al. (2008) que afirma que o Líder Autêntico influencia no comportamento positivo de seus liderados. O resultado demostra que, quando há intenção de violação de políticas de segurança da informação, por partes dos colaboradores, a liderança autêntica pode não influenciar negativamente nesta intenção errônea do funcionário. No entanto, o resultado corrobora com o estudo de Algera e Lips-Wiersma (2012), quando afirmam que os líderes não podem ser autênticos em relação a todos os indivíduos, em todas as situações e em todos os momentos, uma vez que a realidade prática da vida não o permite.

Ao analisar o resultado do construto Liderança Autêntica, o resultado não confirma a influência negativa desses relacionamentos em nenhuma das suas sub-dimensões. O Processamento Equilibrado da Liderança Autêntica, segundo Luthans e Avolio (2003) está relacionado com as considerações feitas por outras pessoas ao que se refere as informações e reflexões. Pode-se concluir, conforme resultado desta pesquisa, que mesmo o líder considerando as opiniões dos colaboradores, não influencia na Intenção de Violação de Política de Segurança da Informação.

A quarta hipótese, de que a Penalidade Percebida influencia negativamente a violação de políticas de Segurança da Informação, foi confirmada e reforça as teses de que a Certeza da penalidade, a Severidade da penalidade e as Pressões organizacionais são considerados fatores inibidores nas tentativas de violação de políticas de Segurança da Informação das organizações em que trabalham (HERATH; RAO, 2009; D'ARCY; HOVAV; GALLETTA, 2009). Desta forma, os indivíduos se sentirão dissuadidos de praticar possíveis atos ilícitos, na medida em que tiverem a certeza de que ocorrerá a punição e perceberem a severidade das punições cabíveis.

A síntese dos testes de hipóteses do estudo é apresentada no Quadro 3 a seguir.

Quadro 3 - Síntese dos Testes de Hipóteses

Hipóteses	Descrição	Resultado
H1	O Desengajamento Moral influencia positivamente a intenção de violação de políticas de segurança da informação.	Confirmada
H2	A Habilidade Tecnológica influencia negativamente a violação de políticas de segurança da informação.	Não Confirmada
H3	A Liderança Autêntica influencia negativamente a intenção de violação de políticas de segurança da informação.	Não Confirmada
H4	A Penalidade Percebida influencia negativamente a intenção de violação de políticas de segurança da informação.	Confirmada

Fonte: elaborado pelos autores

4 CONSIDERAÇÕES FINAIS

As violações da política de acesso do sistema pelos funcionários representam um problema crescente que cria enormes riscos e custos para organizações. Um dos cenários comuns de violação de políticas ocorre quando invasores acessam informações restritas sem permissão, o que infringe as regras estabelecidas nas políticas organizacionais (VANCE et al., 2015). No entanto, segundo D'Arcy et al (2014), as organizações costumam sofrer vários tipos de violações das políticas de segurança da informação, por parte dos colaboradores, apesar das crescentes ações a fim de mitigar esses comportamentos como implementação de novas políticas de segurança e programas de conscientização.

Um estudo relatou que na Coreia do Sul, um funcionário do Standard Chartered Bank, da Coreia, obteve ilegalmente dados de 130.000 clientes, por meio de acesso à rede da empresa e compartilhou os dados com os vendedores de uma outra companhia de seguros. Como resultado, a reputação do Standard Chartered Bank foi severamente prejudicada, e a empresa fez grandes pagamentos a seus clientes como resultado de ações judiciais e penalidades incorridas. Casos como este, reflete a importância das organizações em adotarem medidas internas adequadas de segurança para protegerem os dados do cliente (CHUA et al., 2018).

As abordagens teóricas foram integradas neste estudo, em um único modelo conceitual, em que se buscou analisar estatisticamente a relação entre todos os constructos. Este estudo permite ao gestor identificar as possíveis

causas de violação de Políticas de Segurança da Informação, cujas consequências podem comprometer seriamente a imagem da instituição, proporcionar o conhecimento da concorrência sobre seus segredos industriais e comerciais, sofrer impactos financeiros devido ao compartilhamento de informações sigilosas, entre outras consequências. Estudos similares evidenciam que o treinamento contínuo dos funcionários em relação a importância deles se aderirem a política da segurança da informação deve ser inserido no perfil de comportamento ético esperado no exercício de suas atribuições profissionais.

Conforme os resultados desta pesquisa, o fator de Justificativa Moral é o que mais influencia na Intenção de Violação de Política de Segurança da Informação, quando comparado aos outros fatores. A partir desta descoberta, sugere-se que as políticas organizacionais contenham requisitos que coíbam ações de violação de políticas com destaque a mecanismos cognitivos de desengajamento moral, a fim de mitigar ações que podem causar problemas à organização.

Trata-se de uma constatação interessante, pois, parece ser razoável que o “senso comum” explora diversos exemplos em que a reconstrução cognitiva de um ato culpável em relação as normas e procedimentos corporativos possa se tornar algo normal, aceitável e passível de complacência por outros colaboradores criando a empatia necessária para reduzir o sentimento de culpa pelas consequências desses atos.

Para os gestores, esta constatação é importante, no sentido em que a gestão deve evitar o surgimento de um ambiente propício a prática de Justificativa Moral, e demanda um desafio contínuo nas organizações no planejamento de ações capazes de mitigar os riscos relacionados a este fenômeno. Entre as ações deve-se destacar a ênfase na importância de um ambiente ético, fortalecido por programas de treinamento e workshops voltados para uma conscientização acerca das consequências negativas que estas ações possam causar às organizações.

A dimensão Eufemismo, também considerada como fator de gatilho para adoção de práticas de violação, também foi apontada neste estudo como sendo um fator significante, porém com peso menor do que aquele observado na Justifica Moral. Neste caso específico, o estudo sugere que seria mais fácil

justificar uma ação ruim em aceitável do que adequar o vocabulário, o discurso de ações ilícitas para mascarar ou, tornar mais agradável ou respeitável esta ação.

Uma forma de se evitar que esta dimensão possa causar danos a organização seria um acompanhamento contínuo no comportamento dos colaboradores, checando se praticam o eufemismo em outras situações e obter os registros sistêmicos do que os colaboradores fazem para comparar o discurso com a prática. A fim de se evitar essa prática, os gestores devem implementar controles, de forma a obter registros de operação dos sistemas e analisá-los a fim de se detectar padrões anómalos, indicando uma provável violação de política de Segurança da Informação.

Este estudo também indica que não foi comprovada a hipótese de que a Habilidade Tecnológica influenciaria negativamente a ocorrência de violações da política de segurança da informação, pois esta dimensão foi sobreposta pelos fatores vistos de Desengajamento Moral. Entretanto, o valor apontado para este fator possui um sinal negativo, o que poderia indicar a tendência de que esta hipótese poderia ser corroborada em pesquisas futuras que pudessem analisar este fenômeno em particular.

Esta informação tem uma importância relevante para organização pois, ao contratar pessoas com maior conhecimento tecnológico, potencialmente, poderiam ser evitadas a ocorrência de violações na política de segurança, já que pessoas com essa qualificação têm condições de colaborar até mesmo na adequação das políticas e na observação de colegas no uso das tecnologias da informação e comunicação.

A busca pelos motivadores na intenção de mau uso de Sistemas de Informação, ou de violação de políticas de segurança atende a uma proposta de pesquisa futura a partir de fatos como cultura de segurança, clima ético e compromisso da alta gerência com a segurança sugerida por D'Arcy (2009).

A hipótese associada com a Liderança Autêntica não foi confirmada, ou seja, não se pode afirmar, que a Liderança Autentica influencia, negativamente, na intenção violação de políticas de segurança da informação a partir dos resultados deste estudo. Portanto, propõe-se que a disseminação de princípios morais e éticos nas organizações, não seja apenas papel do líder; mas, sim, de toda a equipe. A realização de campanhas organizacionais de conscientização,

sobre a importância a ações firmadas na ética e na moral, por parte de todos da empresa, é benéfica e poderá promover bons resultados tanto para a empresa, quanto para os colaboradores.

Entende-se que os líderes autênticos podem influenciar a autenticidade nos colaboradores, mas ações de integridade relativos à moral e à ética só depende deles próprios. Esta proposta não anula a ação fundamental da liderança em disseminar condutas morais e éticas aos seus colaboradores: segundo Luthans e Avolio (2003) não se pode excluir o impacto de que líderes exercem sobre a vida das pessoas, principalmente, quando a ética e a moral encontram-se na essência da liderança.

Com relação à percepção de penalidade, o estudo evidenciou a importância de que as políticas de gestão de segurança da informação deixem claro as penalidades cabíveis, bem como a severidade das punições na prática de atos ilícitos. Contudo, uma boa política de segurança de informação, não deve deixar de considerar a educação dos colaboradores com relação às necessidades de segurança deste ativo tão precioso para as organizações. Influenciar e sensibilizar o colaborador pode trazer resultados melhores do que as ações meramente punitivas.

O estudo busca ampliar o portfólio de pesquisas futuras para uso do modelo de Bandura (2002), em que o autor foca a utilização de sua escala para compreender o desengajamento moral em aspectos relacionados a atividades criminosas, uso de força excessiva, pena de morte, abuso infantil e apoio às desigualdades que empobrecem e desmoralizar os membros menos favorecidos de sociedades afluentes.

Entre as limitações desta pesquisa está o fato de que ela diz respeito a uma região específica do país e, portanto, não possui abrangência nacional. Pesquisas futuras poderão coletar dados de outras regiões a fim de se verificar se estes resultados poderiam ser observados em uma amostra mais diversificada para uma análise mais abrangente. Outra limitação desta pesquisa está no fato de que ela não foi dirigida apenas a profissionais de TI, mas sim a colaboradores de uma forma geral. Talvez a segmentação nesse perfil pudesse explorar outros resultados.

Já a escala da dimensão Habilidade Tecnológica buscou medir apenas a percepção da habilidade dos colaboradores e não a habilidade propriamente

dita. Com isso, outras pesquisas podem ser realizadas no sentido de se verificar esta relação específica com uma medida objetiva que possa aferir a habilidade.

Este estudo é limitado em relação à análise do nível de criticidade de segurança da informação das organizações consideradas, propõe-se à pesquisa futura inserir variáveis de controle que versam sobre aspectos relacionados à importância da disponibilidade de criticidade das informações. Pesquisas futuras também podem mensurar a percepção dos colaboradores em relação as contramedidas adotas por organizações no sentido se evitar as ilicitudes relacionadas ao uso de tecnologias da informação e comunicação.

REFERÊNCIAS

ABNT ISO 27002. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR/ISO/IEC 27002:2013** tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação, 2013.

AFFONSO, E. P.; OLIVEIRA, S. C.; SANT'ANNA, R. C. G. Análise do equilíbrio entre privacidade e utilidade no acesso a dados. **Informação & Sociedade: Estudos**, João Pessoa, v.27, n.1, p. 81-92, jan./abr. 2017.

ALGERA, P. M., & LIPS-WIERSMA, M. Radical authentic leadership: Co-creating the conditions under which all members of the organization can be authentic. **The Leadership Quarterly**, v. 23, n.1, p.118-131, 2012. https://doi.org/10.1016/j.leaqua.2011.11.010

AURIGEMMA, S.; PANKO, R. A **Composite Framework for Behavioral Compliance with Information Security Policies**.Hawaii International Conference on System Sciences, p.3248-3257, 2012.

AVOLIO, B. J.; GARDNER, W. L.; WALUMBWA, F. O.; LUTHANS, F.; MAY, D. R. Unlocking the mask: A look at the process by which authentic leaders' impact follower attitudes and behaviors. **The Leadership Quarterly**, v 15, p.801–823, 2004.

AVOLIO, B. J.; GARDNER, W.L. Authentic leadership development: Getting to the root of positive forms of leadership. **The Leadership Quarterly**, v. 16, n. 3, p.315-338, jun. 2005.

BANDURA, A. Selective activation and disengagement of moral control. **Journal of Social Issues**, v. 46, n. 1, p. 27-46, 1990.

BANDURA, A. Social cognitive theory of self-regulation. **Organizational Behavior and Human Decision Processes**, v.50, n.2, p.248-287, 1991. https://doi.org/10.1016/0749-5978(91)90022-L

BANDURA, A. Selective moral disengagement in the exercise of moral agency. **Journal of moral education**, v. 31, n. 2, p. 101-119, 2002.

BANDURA, A.; BARBARANELLI, C.; CAPRARA, G.V.; PASTORELLI, C. Mechanisms of moral disengagement in the exercise of moral agency. **Journal of Personality and Social Psychology**, v.2, n. 71, p. 364–374, 1996.

BARLOW, J. B. et al. Don't make excuses! Discouraging neutralization to reduce IT policy violation. **Computers and Security**, v. 39, p.145-159, 2013.

BECKER, J. M.; KLEIN, K.; WETZELS, M. Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models. **Long Range Planning**. Elsevier Ltd, v.45, n.5, pp. 359–394, 2012. doi: 10.1016/j.lrp.2012.10.001.

BÉLANGER, F. et al. Determinants of early conformance with information security policies. **Information and Management**, v. 54, n. 7, p.887-901, 2017.
BRIN, S.; PAGE, L. The anatomy of a large-scale hypertextual web search engine. **Computer networks and ISDN systems**, v. 30, n. 1-7, p. 107-117, 1998.

BROWN, C.; MURPHY, T. J.; NANNY, M. Turning techno-savvy into info-savvy: Authentically integrating information literacy into the college curriculum. **The Journal of Academic Librarianship**, v. 29, n. 6, p. 386-398, 2003.

CHUA; WONG; LOW; CHANG. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. **Telematics and Informatics**, v. 35, n. 6, p.1770-1780, 2018.

CLARK, D. N.; DOUGLAS, H. Information and communication technology adoption and diffusion in micro-enterprises: the case of techno-savvy home-based businesses. **International Journal of Entrepreneurship and Small Business**, v. 14, n. 3, p. 349-368, 2011.

COHEN, J. **Statistical power analysis for the behavioral sciences** (2nd ed.). Hillsdale, NJ: Erlbaum, 1988.

DALFOVO, M. S.; LANA, R. A.; SILVEIRA, A. Métodos quantitativos e qualitativos: um resgate teórico. **Revista interdisciplinar científica aplicada**, v. 2, n. 3, p. 1-13, 2008.

D'ARCY, J.; HERATH, T.; SHOSS, M. K. Understanding employee responses to stressful information security requirements: A coping perspective. **Journal of Management Information Systems**, v. 31, n. 2, p. 285-318, 2014.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. **Information Systems Research**, v. 20, n. 1, p. 79-98, 2009.

DETERT, J. R.; TREVIÑO, L. K.; SWEITZER, V. L. Moral disengagement in ethical decision making: a study of antecedents and outcomes. **Journal of Applied Psychology**, v. 93, n. 2, p. 374, 2008.

FAUL, F.; ERDFELDER, E.; BUCHNER, A.; LANG, A.-G. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. **Behavior Research Methods**, v. 41, pp. 1149-1160. 2009.

FAUL, F.; ERDFELDER, E.; LANG, A.-G.; BUCHNER, A. G. *Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. **Behavior Research Methods**, v.39, 175-191. 2007.

FIDALGO, J. T. S. **A Relação entre Liderança Autêntica e Empenhamento Afetivo, Orientação para o cliente e Intenção de Turnover**. Dissertação de Mestrado, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, 2018.

FLOWERDAY, S. V.; TUYIKEZE, T. Information security policy development and implementation: The what, how and who. **Computers e Security**. v.61, p. 169-183, 2016.

FONSECA, A. M. O.; PORTO, J. B.; BORGES-ANDRADE, J. E. Liderança: Um Retrato da Produção Científica Brasileira. **Revista de Administração Contemporânea**, v. 19, n. 3, p. 290-310, 2015.

GIBBS, J. P. **Crime, Punishment, and Deterrence**. Elsevier, New York, 1975.

GUO, K. H.; YUAN, Y. The effects of multilevel sanctions on information security violations: A mediating model. **Information & Management**, v. 49, n. 6, p. 320-326, 2012.

HAIR, J. F. et al. When to use and how to report the results of PLS-SEM. **European Business Review**, v.31, n.1, pp. 2–24, 2019. doi: 10.1108/EBR-11-2018-0203.
HAIR, J.F., ANDERSON R. E., TATHAM R. L. E BLACK, W.C. **Análise multivariada de dados**. 5ª ed. Porto Alegre: Bookman. 2005.

HENDERSON, J. R.; RUIKAR, K. Technology implementation strategies for construction organisations. **Engineering, Construction and Architectural Management**, v. 17, n. 3, p. 309-327, 2010.

HERATH, T., RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, **Decision Support Systems**, v. 47, n. 2, p. 154-165, 2009. https://doi.org/10.1016/j.dss.2009.02.005.

KAVUSSANU, M.; HATZIGEORGIADIS A.; ELBE A.; RING C. The moral disengagement in doping scale. **Psychology Sport And Exercise**, v. 24, p.188-198, 2016.

KERNIS, M. H.; GOLDMAN, B. M. **A multicomponent conceptualization of authenticity: Theory and research**. In M. P. Zanna (Ed.), Advances in experimental social psychology, v 38, pp. 283–357. San Diego: Academic Press, 2006.

KRISTOF, A. L. Person-organization fit: An integrative review of its conceptualizations, measurement, and implications. **Personnel psychology**, v. 49, n. 1, p. 1-49, 1996.
LEÓN, D. A. D. **Análise fatorial confirmatória através dos softwares R e Mplus**. 2011.

LIPNACK, J.; STAMPS, J. Virtual teams: The new way to work. **Strategy & Leadership**, v. 27, n. 1, p. 14-19, 1999.

LOGAN, D. **What is information governance? And why is it so hard?** Disponível em: <http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/>. Acesso em: 20 de jan de 2019

LUTHANS, F., E AVOLIO, B. J. Authentic leadership: A positive development approach. **Positive Organizational Scholarship,** p.241–258. San Francisco: Berrett-Koehler. 2003.

MANÃS, A. V., GIORDANO, C. V. **Aplicativos Comerciais - Suporte a Sistemas e Usuários**. Ed. Érica/Saraiva.SP. 2014.

McCANDLESS, D.; EVANS, T. World´s biggest data breaches & hacks. **Information is beautiful**, 2021. Disponível: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. Acesso em: 05/04/2021.

MILTGEN, C. L.; SMITH, H. J. Exploring information privacy regulation, risks, trust, and behavior. **Information e Management**, v. 52, n. 6, p.741-759, 2015.

MONSEN, E. R. Techno-savvy dietetics professionals are setting the pace. **Journal of the Academy of Nutrition and Dietetics**, v. 99, n. 11, p. 1346, 1999.

MOORE, C. Moral disengagement. **Current Opinion in Psychology**, v. 6, p.199-204, 2015

NAGIN, D. S., G. POGARSKY. Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. **Criminology**, v. 39, n. 4, p. 865–891, 2001.

PAHNILA, S.; SIPONEN, M.; MAHMOOD, A. **Employees' Behavior towards IS Security Policy Compliance University of Oulu**, Department of Information Processing Department of Information and Decision Sciences, University of Texas at El Paso. Proceedings of the 40th Hawaii International Conference on System Sciences, p. 1–10, 2007.

PECK, J. A.; HOGUE, M. Acting with the best of intentions… or not: A typology and model of impression management in leadership. **The Leadership Quarterly**, v. 29, n. 1, 2018.

REGO, A., SOUSA, F., MARQUES, C., & E CUNHA, M. P. Authentic leadership promoting employees' psychological capital and creativity. **Journal of Business Research**, v.65, n.3, p.429-437, 2012. doi: 10.1016/j.jbusres.2011.10.003.

REYNOLDS, S. J. et al. The role of moral knowledge in everyday immorality: What does it matter if I know what is right? **Organizational Behavior And Human Decision Processes**, v. 123, n. 2, 2013.

RINGLE, C. M. et al. Partial least squares structural equation modeling in HRM research. **International Journal of Human Resource Management**. Routledge, (January), p. 1–27, 2018. doi: 10.1080/09585192.2017.1416655.

RINGLE, C. M.; WENDE, S.; BECKER, J.M. **SmartPLS 3**. Boenningstedt: SmartPLS GmbH. 2015.

SAFA, N. S. et al. Motivation and opportunity based model to reduce information security insider threats in organizations. **Journal of Information Security And Applications**, v. 40, p.247-257, 2018.

SANTOS, J. G.; CAPPELLOZZA, A.; ALBERTIN, A. L. Antecedents of Perceived Benefits of Compliance Towards Organizational Data Protection Policies. **IEEE Latin America Transactions**, v. 16, p. 891-896, 2018

SANTOS, R. A.; GUEVARA, A. J. H.; AMORIM, M. C. S.; FERRAZ-NETO, B. **Compliance and leadership: the susceptibility of leaders to the risk of corruption in organizations**. Einstein São Paulo. v.10, n.1, 2012.

SILVA, E.; DAMIAN, I. P. M.; VALENTIM, M. L. P. Análise das convergências entre os modelos de maturidade de gestão do conhecimento e os pilares do índice global de inovação. **Informação & Sociedade: Estudos**, João Pessoa, v.30, n.1, p. 1-20, jan./mar. 2020.

SIPONEN, M. T. An analysis of the traditional IS security approaches: implications for research and practice. **European Journal of Information Systems**, v. 14, n. 3, 2005.

SOLOVE, D. J. **The future of reputation: Gossip, rumor, and privacy on the Internet**. Yale University Press, 2007.

STONE-ROMERO, E. F.; STONE, D. L., HYATT, D. Personnel Selection Procedures and Invasion of Privacy. **Journal of Social Issues**, v. 59, n. 2, p. 343-368, 2003.

TANIGUCHI, S. P.; SANCHEZ, P. D. O.; CAPPELLOZZA, A; FILENGA, D. **Desonestidade acadêmica: A influência de fatores pessoais e práticas de grupo
na atitude de estudantes de Administração**. Rio de Janeiro: Enanpad. 2011.

TREVIÑO, L. K.; NELSON, K. A. **Managing business ethics: Straight talk about how to do it right**. John Wiley & Sons, 2011.

VANCE A.; LOWRY P. B.; EGGETT D. A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. **MIS Quarterly,** v.39, n.2, p. 345-366, 2015.

VANDAGRIFF, D. P. **Survival of the Techno-Savvy-Electronic Communication for Lawyers Will Be Vital in a Computerized Future**. ABAJ, v. 81, p. 84, 1995.

VON SOLMS, B. Information Security – The Fourth Wave. **Computers & Security**, v. 25, n.3, p.165-168, 2006.

WALUMBWA, F. O., AVOLIO, B. J., GARDNER, W. L., WERNSING, T. S., E PETERSON, S. J. Authentic Leadership: Development and validation of a theory-based measure. **Journal of Management**, v. 34, n.1, 2008.

WARKENTIN, M.; WILLISON, R. Behavioral and policy issues in information systems security: the insider threat. **European Journal of Information Systems**, v.18, n.2, 2009.

WEISS, M. et al. Authentic leadership and leaders' mental well-being: An experience sampling study. **The Leadership Quarterly**, v. 29, n.2, p. 309-321, 2018.

YAZDANMEHR, ADEL; WANG, JINGGUO. Employees' information security policy compliance: A norm activation perspective. **Decision Support Systems**, v. 92, p.36-46, 2016.

YE, Q. **Extending research on technostress: exploring the moderating effects of techno-savvy and the proactive personality on the relationship between technostress and job satisfaction and stress**. (Dissertação de Mestrado), Universidade de Canterbury, 2018.

Esta obra está licenciada com uma Licença Creative Commons Atribuição-Não Comercial 4.0 Internacional.