

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO**

PLINIO SILVA DE GARCIA

**A INFLUÊNCIA DO AMBIENTE ORGANIZACIONAL
NA MOTIVAÇÃO PARA PRÁTICA DE CRIMES CIBERNÉTICOS**

PORTO ALEGRE

2016

PLINIO SILVA DE GARCIA

**A INFLUÊNCIA DO AMBIENTE ORGANIZACIONAL
NA MOTIVAÇÃO PARA PRÁTICA DE CRIMES CIBERNÉTICOS**

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientadora: Profa. Dra. Marie Anne Macadar

PORTO ALEGRE

2016

Dados Internacionais de Catalogação na Publicação (CIP)

G216 Garcia, Plinio Silva de
A influência do ambiente organizacional na motivação para prática de crimes cibernéticos. / Plinio Silva de Garcia. – Porto Alegre, 2016. 112 f.

Dissertação (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia, PUCRS.
Orientação: Prof^ª. Dr^ª. Marie Anne Macadar.

1. Administração. 2. Clima organizacional. 3. Motivação criminal. 4. Crimes cibernéticos. I. Macadar, Marie Anne. II. Título.

CDD 658.3144

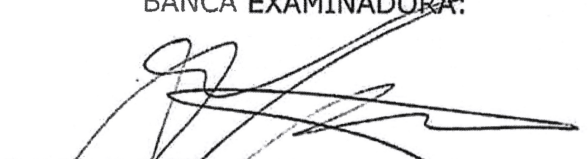
Plínio Silva de Garcia

A Influência do Ambiente Organizacional na Motivação para Prática de Crimes Cibernéticos


Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em 28 de março de 2016, pela Banca Examinadora.

BANCA EXAMINADORA:



Profa. Dra. Marie Anne Macadar Moron
Orientadora e Presidente da sessão



Profa. Dra. Mirian Oliveira



Profa. Dra. Edimara Mezzomo Luciano



Profa. Dra. Cristiane Pedron

*“Somente amadores atacam máquinas;
profissionais miram pessoas.”*

Schneider (2000)

AGRADECIMENTOS

Agradeço aos Professores do Programa de Pós-Graduação em Administração da PUCRS pelo suporte, orientação e ensinamentos. Dedico a eles a maturidade acadêmica e pessoal que adquiri nesses dois anos de convívio.

Agradeço aos colegas de curso pela parceria e amizade ao longo desta intensa e transformadora jornada.

Sem o carinho, o apoio e a confiança da minha família, absolutamente nada disso teria sido possível.

Para a minha esposa Gabriela, utilizo as palavras de uma pessoa muito importante na minha vida: a minha querida irmã Flávia. Um certo dia, a muitos anos atrás, voltando para casa e sentados no fundo da lotação, ela me disse: obrigado por existir!

Gabi, obrigado por tudo que já vivemos! Obrigado por fazer parte da minha história.

Minha eterna gratidão aos meus pais, Carmem e Valério. Eles sempre rejeitaram a ignorância e a insciência como valor existencial. Eles sempre cultivaram o amor à cultura e ao conhecimento. Eles sempre incentivaram a dedicação aos estudos. Devo tudo a eles!

Espero transmitir tais valores fundamentais para a minha filha Antonella, nascida no começo desta caminhada acadêmica. As lembranças deste Mestrado estarão, para sempre, confundidas com a minha querida Antonella. Que ela tenha amor ao conhecimento científico e suas infinitas possibilidades.

RESUMO

A motivação das pessoas para a prática de crimes cibernéticos vem sendo investigada com objetivo de melhorar a eficácia e a eficiência da segurança cibernética em âmbito organizacional. A equidade das decisões gerenciais sobre recompensas e reconhecimento, a igualdade e imparcialidade de políticas e práticas organizacionais, a qualidade do tratamento interpessoal, preservando o respeito e a dignidade das pessoas, bem como a transparência, clareza e precisão das informações comunicadas são elementos inerentes ao local de trabalho que impactam nas emoções das pessoas. Esses fatores influenciam a motivação criminal dos indivíduos, mediante o desenvolvimento de sentimentos negativos. A percepção de injustiça organizacional e a consequente sensação de descontentamento experimentada por trabalhadores de uma empresa pode estimular retaliações contra a própria organização e seus respectivos membros. Esta pesquisa buscou analisar como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham. Foram realizadas entrevistas semiestruturadas com especialistas em segurança cibernética que desempenharam suas funções em organizações brasileiras. Esses profissionais têm, pelo menos, cinco anos de experiência na área de segurança cibernética. As percepções e vivências dos entrevistados produziram dados que foram transcritos, analisados e categorizados para consequente atribuição de significados. Nesta pesquisa, a vingança e a ganância foram identificados como sendo os principais fatores motivacionais para o crime cibernético, com uma participação importante e complementar de elementos relacionados à oportunidade, ao costume, à associação e, principalmente, à impunidade. A expectativa de que não haverá punição se um crime for cometido é um determinante em muitos crimes cibernéticos. Os resultados sugerem que a percepção de injustiça, no contexto organizacional brasileiro, produz nos indivíduos prioritariamente sentimentos negativos como a baixa-estima, a frustração e a ausência de culpa, e que essas emoções motivam as pessoas a cometer crimes cibernéticos nas organizações onde trabalham.

Palavras-chave: Justiça organizacional. Motivação criminal. Crime cibernético. *Insider*. Segurança cibernética.

ABSTRACT

The motivation of people to the practice of cybercrimes has been investigated in order to improve the effectiveness and efficiency of cybersecurity at the organizational level. The fairness of management decisions on rewards and recognition, equality and fairness of organizational policies and practices, the quality of interpersonal treatment, preserving the respect and dignity of people, as well as transparency, clarity and accuracy of the information are elements inherent to the workplace. The experience of situations related to these elements produces emotions in people, which occasionally are negative emotions such as frustration, stress, anger or discontent. These factors influence the motivation of criminal individuals by developing negative feelings. The perception of organizational injustice and the consequent feeling of dissatisfaction experienced by workers can stimulate retaliation against their organization and its members. This study aimed to analyze how the organizational perceptions of unfairness motivate insiders to commit cybercrimes in the organizations where they work. Semi-structured interviews with cybersecurity experts who worked for Brazilian organizations were conducted. These professionals have at least five years of experience in the field. The narratives of the respondents have produced data that was transcribed, analyzed and categorized for subsequent interpretation. In this research, revenge and greed were identified as the main motivating factors for cybercrime, with an important and complementary participation of elements related to opportunity, habits, association, and especially impunity. The expectation that there will be no punishment for a crime encourages the commission of cybercrimes. The results suggest that the perception of injustice in the Brazilian organizational context produces primarily negative feelings such as low self-esteem, frustration, and lack of guilt in individuals and that these emotions motivate people to commit cybercrimes in the organizations where they work.

Key Words: Organizational justice. Criminal motivation. Cybercrime. Insider. Cyber security.

LISTA DE FIGURAS

Figura 1 - Pilha da Execução do Crime Cibernético	17
Figura 2 - Modelo Conceitual.....	60
Figura 3 - Imagens do Evento de Segurança Cibernética em Porto Alegre	63
Figura 4 - Imagens do Evento de Segurança Cibernética em São Paulo	65
Figura 5 - Desenho de Pesquisa.....	66
Figura 6 - Transcrições importadas para o Nvivo.....	70
Figura 7 - Processo de codificação no Nvivo	71
Figura 8 - Modelo Conceitual Refinado	86

LISTA DE QUADROS

Quadro 1 - Abordagens Teóricas sobre a Criminalidade	27
Quadro 2 - Habilidades e Motivações de Criminosos Cibernéticos	43
Quadro 3 - Técnicas de Neutralização do Comportamento Desviante.....	45
Quadro 4 - Sentimentos Humanos.....	47
Quadro 5 - Tempos das Entrevistas.....	50
Quadro 6 - Síntese dos Fatores da Justiça Organizacional.....	59
Quadro 7 - O Perfil dos Entrevistados.....	68
Quadro 8 - Relação entre os constructos	85

LISTA DE ABREVIATURAS

EY (*Ernst & Young*) - Ernst & Young Global Limited

SAS (*Statements on Auditing Standards*) - Declarações sobre Normas de Auditoria

SDT (*Self-Determination Theory*) - Teoria da Autodeterminação

SI - Sistemas de Informação

TI - Tecnologia da Informação

SUMÁRIO

1	INTRODUÇÃO.....	12
1.1	DELIMITAÇÃO DO TEMA E DO PROBLEMA DE PESQUISA	16
1.2	OBJETIVOS	18
1.2.1	Objetivo Geral.....	18
1.2.2	Objetivos Específicos	18
1.3	JUSTIFICATIVA	18
1.4	ESTRUTURA DO TRABALHO	21
2	FUNDAMENTAÇÃO TEÓRICA.....	22
2.1	ABORDAGENS TEÓRICAS DO CRIME.....	22
2.2	O CRIME CIBERNÉTICO NAS ORGANIZAÇÕES	28
2.2.1	O Impacto do Crime Cibernético	32
2.2.2	A Ameaça do <i>Insider</i>.....	33
2.3	AS MOTIVAÇÕES HUMANAS.....	35
2.3.1	Abordagens Teóricas da Motivação.....	36
2.3.2	Motivações para o Crime Cibernético	41
2.4	SENTIMENTOS HUMANOS	46
2.4.1	A Natureza dos Sentimentos	47
2.4.2	Sentimentos Negativos.....	49
2.5	JUSTIÇA ORGANIZACIONAL	50
2.5.1	O Conceito de Justiça	53
2.5.2	Justiça Distributiva.....	54
2.5.3	Justiça Procedimental	56
2.5.4	Justiça Interpessoal e Informacional	57
2.6	MODELO CONCEITUAL.....	59
3	MÉTODO DE PESQUISA.....	62
3.1	ESCOLHA DO MÉTODO	62
3.2	DESENHO DE PESQUISA	66
3.3	INSTRUMENTO DE PESQUISA	67
3.4	COLETA DE DADOS	67

4	ANÁLISE DOS DADOS	72
4.1	JUSTIÇA ORGANIZACIONAL	72
4.2	SENTIMENTOS NEGATIVOS.....	76
4.3	MOTIVAÇÕES PARA O CRIME.....	79
5	DISCUSSÃO DOS RESULTADOS	84
6	CONSIDERAÇÕES FINAIS.....	87
6.1	CONTRIBUIÇÕES DA PESQUISA	88
6.2	LIMITAÇÕES DA PESQUISA	90
6.3	SUGESTÕES PARA FUTUROS ESTUDOS.....	91
	REFERÊNCIAS.....	93
	APÊNDICE A - TERMO DE SIGILO	107
	APÊNDICE B - INSTRUMENTO DE PESQUISA.....	108
	APÊNDICE C - AMEAÇAS CIBERNÉTICAS.....	110

1 INTRODUÇÃO

Atualmente, são necessárias mais informações que possibilitem uma análise e compreensão dos fatores que levam pessoas a cometer crimes cibernéticos (RASMI; JANTAN, 2013). Em uma discussão sobre crimes que ocorrem em um contexto fundamentalmente tecnológico e virtual, pode parecer estranho incluir traços psicológicos, características pessoais, questões morais e condições socioambientais. Como qualquer outro crime, pessoas estão envolvidas e a inclusão das ciências comportamentais torna-se evidente (ROGERS; SEIGFRIED; TIDKE, 2006). Devido à importância do comportamento humano relacionado com a segurança cibernética, considerar a relevância das motivações pessoais e dos fatores contribuintes para o crime cibernético beneficia gestores que necessitam influenciar seus usuários, clientes e fornecedores (STANTON et al., 2005).

Segurança, ameaças, vulnerabilidades e a criminalidade cibernética correspondem a conceitos que emergem no espaço cibernético, "ambiente fictício em que a comunicação ocorre através de redes de computadores" (OXFORD DICTIONARIES, 2015, s./p.). O termo foi criado por *William Gibson* em seu romance "*Neuromancer*" (GIBSON, 1995), e virou realidade no mundo em que vivemos hoje, constituindo-se um fato da vida diária, dada a sua onipresença (CHOUCRI; MADNICK; FERWERDA, 2013). Tal denominação é comumente utilizada para descrever o contexto associado à Internet e suas tecnologias (ARPAD, 2013). Trata-se de uma metáfora para um espaço não físico criado por redes de computadores onde as pessoas podem se comunicar (CANONGIA; MANDARINO JUNIOR, 2010). Pode ser considerado como um novo espaço social (em contraste com o "espaço real"), com estruturas ontológicas e epistemológicas próprias, formas de interação, papéis, regras, limites e possibilidades (YAR, 2005).

A Internet nasceu essencialmente como um ambiente desregulamentado e com características propícias para a ocorrência de variados tipos de crimes (RICHARDSON, 2008). Originalmente, a rede mundial de computadores foi concebida como um sistema aberto, sendo a confiabilidade e previsibilidade dos usuários uma premissa (LEFEBVRE; ACM, 2012). A questão do controle e da segurança das informações que trafegavam na Internet não era foco daqueles que planejavam e definiam sua estrutura e regras de comunicação. Todavia, o rápido crescimento trouxe vulnerabilidades e, por conseguinte, o crime cibernético, com seus impactos imediatos e futuros (LEFEBVRE; ACM, 2012). Considerando que quase todos os locais no mundo têm algum grau de acesso ao ciberespaço, as oportunidades para prática criminosa tornaram-se quase ilimitadas. No curto prazo,

indivíduos, organizações ou governos têm suas atividades diárias prejudicadas pela ocorrência de fraudes, corrupção de sistemas e indisponibilidade serviços. No longo prazo, danos significativos podem comprometer a credibilidade, a propriedade intelectual, a estabilidade social, a soberania e a segurança da população (CHOO, 2011).

Na literatura, “Segurança Cibernética” é um termo frequentemente usado de maneira análoga ao termo “Segurança da Informação”. Embora exista alguma sobreposição, os conceitos possuem diferenças, sendo a principal delas, o escopo mais abrangente da segurança cibernética (SOLMS; NIEKERK, 2013). Está última engloba a proteção de pessoas e de outros ativos, além da informação (SOLMS; NIEKERK, 2013). Essa abrangência oferece implicações éticas e morais na medida em que a proteção das pessoas torna-se uma evidente responsabilidade da sociedade no que tange o ambiente cibernético.

No universo das organizações, a segurança cibernética engloba as várias medidas necessárias para proteger infraestruturas de tecnologia da informação (TI) contra ataques que variam desde a recreação de *hackers* até crimes que destroem o patrimônio financeiro, material e humano das organizações (ISO/IEC_27000, 2014; LEFEBVRE; ACM, 2012). A segurança cibernética compreende aspectos relacionados a prevenção e repressão (CANONGIA; MANDARINO JUNIOR, 2010), devendo proteger o acesso, a manipulação, a transmissão e a destruição indevida e não autorizada da infraestrutura e da informação pessoal e organizacional (ITU, 2015). Tais iniciativas ocorrem mediante o desenvolvimento e implantação de políticas, normas, orientações, ferramentas e tecnologias (ITU, 2015).

O enorme volume de informação sensível presente nas organizações passou a ser um problema de segurança (SILVA NETTO; SILVEIRA, 2007). A dependência da comunicação eletrônica e das transações *on-line* para fazer negócios agravou tal situação (CAPPELLI; TRZECIAK, 2009). A ampla utilização de sistemas de informação (SI) neste cenário, em adição, evidenciou a importância da segurança física, lógica e operacional destinada aos ambientes computacionais, com objetivo de proteger ativos organizacionais contra ameaças cibernéticas (SÊMOLA, 2003; SIPONEN, 2005).

Estudos atuais passam a abordar o problema considerando processos organizacionais e, principalmente, pessoas com intenções criminosas (THEOHARIDOU et al., 2005). Políticas de segurança, controles sistematizados, referenciais de boas práticas, níveis de maturidade e gestão de riscos são métodos comumente utilizados. A avaliação de ameaças é parte essencial da gestão da segurança cibernética, antecipando a estratégia de um ataque e o comportamento do atacante (WU; SHUPING; JUNHUA, 2009). Esse exercício de previsão é um desafio complexo e nem sempre produz os efeitos esperados.

O número de crimes cibernéticos vem aumentando e a investigação criminal tem relevante papel no processo de análise dos incidentes de segurança cibernética (RASMI; JANTAN, 2013). Utilizando a tecnologia como meio de obter benefícios, invasores cibernéticos tornam-se arquétipos para um dos principais tipos de crime no século 21 (BURDEN; PALMER, 2003). Para auxiliar na compreensão de quem é o “inimigo” no universo cibernético, é necessário identificar as pessoas com motivações para destruir, corromper e abusar de infraestruturas de TI (ROGERS, MANUS K., 2006). Adicionalmente, compreender como o ambiente organizacional e suas variáveis de contexto favorecem ou não essas motivações individuais ou coletivas (WILLISON; WARKENTIN, 2009). Existem trabalhos prévios que analisam as escolhas feitas pelos criminosos considerando o ato e o respectivo contexto. A compreensão desta relação é de óbvio interesse para os gestores. Eles tentam manipular variáveis de contexto para influenciar as escolhas do agressor, desestimulando o ato criminoso. A Prevenção Situacional do Crime (SCP) é uma escola do pensamento que considera essa perspectiva, desviando o foco da criminologia para o âmbito das circunstâncias as quais possam prever tipos específicos de crime (WILLISON, 2005). Visando a configuração do contexto, e não somente as características do indivíduo, medidas específicas de manipulação do local de trabalho são introduzidas na organização com objetivo de reduzir as oportunidades para o crime (WILLISON, 2005).

O trabalho de Goode e Cruise (2006) mostrou que os indivíduos que corrompem as proteções tecnológicas e desrespeitam a política de licenciamento de sistemas computacionais não o fazem somente por recompensa financeira. Justificativas para essa motivação vão desde questões éticas, crenças, posicionamento político, e até mesmo vontade de superar obstáculos e mostrar aptidão técnica para seu grupo social. Neste sentido, reconhecer uma intenção criminosa impõe um esforço para inferir os objetivos do intruso e prever suas ações futuras.

Originalmente, os sistemas de detecção de intrusão analisavam características técnicas do tráfego de dados que passava nas redes de computadores em busca de anomalias e mau uso (LAUREANO; MAZIERO; JAMHOUR, 2003). O foco das investigações estava nas ameaças externas às organizações; invasores desconhecidos tentavam penetrar as fronteiras virtuais de uma empresa para roubar dados, corromper sistemas, vandalizar páginas web ou tornar recursos cibernéticos indisponíveis. Atualmente, já está sendo considerado, no âmbito da segurança cibernética, antecipar eventos anômalos, comportamentos atípicos e potencialmente danosos (SMAHA, 1988). Em paralelo, percebeu-se que um volume maior de incidentes originava-se dentro das empresas (NEUMANN, 1999). Os autores identificados eram pessoas

que possuíam acesso e conhecimento sobre os processos internos, sendo capazes de explorar, maliciosamente, as vulnerabilidades organizacionais (NEUMANN, 1999).

Os indivíduos que pertencem a uma organização e que nela desempenham atividades profissionais são denominados *insiders*. Pode ser qualquer pessoa com acesso, privilégio ou conhecimento aprofundado dos sistemas e serviços de informação (CAPPELLI; TRZECIAK, 2009). O *insider* é alguém que recebeu privilégios que autorizam o acesso e a utilização de sistemas ou instalações na respectiva organização (NEUMANN, 1999). Quando tais indivíduos prejudicam a organização de maneira intencional, recebem a denominação de *insiders maliciosos* (ANDERSON; BRACKNEY, 2004). Ataques cibernéticos originados por pessoas internas à organização passam, então, a representar um grande risco operacional. Acessos legítimos e maliciosos indesejados limitam-se, muitas vezes, a uma conexão autenticada mediante credenciais válidas (MAGKLARAS; FURNELL, 2005).

Seja a prática do crime cibernético motivada por ganância, necessidade, oportunidade, descontentamento ou problemas psicológicos, o potencial de perdas e danos para uma organização pode representar desde um pequeno contratempo operacional ou financeiro, até sua total destruição. Uma análise aprofundada do tema deve então considerar fatores adicionais e não menos relevantes sobre o fenômeno. Investigações devem englobar não somente as ações para execução do crime cibernético e os respectivos antecedentes imediatos (intenção e dissuasão). É fundamental estender o foco incluindo também fenômenos que precedem a decisão pela prática do crime (WILLISON; WARKENTIN, 2013). Cita-se a influência que os fatores inerentes ao local de trabalho exercem sobre a tomada de decisão do *insider* antes de qualquer dissuasão. A dinâmica interação entre o pensamento dos criminosos e o respectivo ambiente onde se perpetua um crime pode afetar, significativamente, a eficácia da estratégia de proteção (WILLISON; WARKENTIN, 2013).

A força que o contexto exerce no indivíduo é reconhecidamente relevante: “não existem relações sociais entre os indivíduos e os grupos nem entre estes e os objetos sociais que se deem sem referência a um tempo e a um espaço” (FREITAS, 2000, p. 4). A busca perpétua pelo bem-estar no trabalho ocorre subordinada a diferentes variáveis de contexto. O sentimento de justiça, por exemplo, oriundo da equidade de recompensas e reconhecimento vivenciada durante o exercício profissional produz satisfação e, conseqüentemente, um comportamento social positivo em prol da organização. Em virtude desse sentimento, o indivíduo retribui à organização como um todo e não somente a pessoas específicas (MCNEELY; MEGLINO, 1994). A satisfação no trabalho, quando reforçada por relações interpessoais dignas e respeitadas entre líderes e trabalhadores, reduziu as tendências de

retaliação em virtude de uma maior tolerância dos indivíduos às eventuais injustiças organizacionais (SKARLICKI; FOLGER, 1997). Neste sentido, uma das estratégias organizacionais para minimizar sentimentos negativos que possam motivar o crime está na criação ou alteração de características situacionais do ambiente de trabalho que estimulem o almejado comportamento positivo de natureza social e organizacional.

Buscando contribuir, mesmo que timidamente, com o conhecimento já produzido sobre o tema, este trabalho objetiva analisar como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham. O estudo foi realizado a partir da percepção de especialistas em segurança cibernética. Esses profissionais têm, pelo menos, cinco anos de experiência na área, e desempenharam suas funções em organizações brasileiras.

Está evidente a necessidade de um melhor entendimento sobre as ameaças relacionadas ao fator humano para a gestão da segurança cibernética no âmbito organizacional, especialmente quando tais ameaças estão presentes e ocultas dentro das organizações. Líderes e gestores devem ser os maiores beneficiários se compreenderem este fenômeno e, por conseguinte, investirem em contramedidas que protejam seus recursos materiais, financeiros e, principalmente, humanos.

1.1 DELIMITAÇÃO DO TEMA E DO PROBLEMA DE PESQUISA

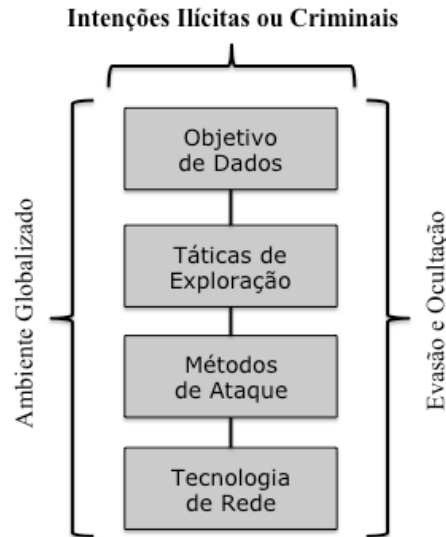
Crimes cibernéticos adquiriram interesse transnacional. O estudo das suas motivações e aspectos influenciadores têm grande relevância no campo da segurança cibernética. O entendimento de questões que antecipam o crime cibernético pode produzir resultados efetivos e gerar medidas capazes de evitar a remediação de danos.

Como em todas as ocorrências criminais, a compreensão e a explicação do comportamento criminoso que determina a prática do delito são fundamentais para os desdobramentos sociais, organizacionais e penais. Fundamentado na revisão de literatura, o presente estudo analisa de que maneira percepções sobre fatores relacionados ao local de trabalho impactam na motivação das pessoas para o crime cibernético.

A intenção criminosa que produz um determinado comportamento é uma característica investigada no campo da criminologia e possui relevante papel na análise de crimes cibernéticos (HUNTON, 2009). No modelo que define a pilha de execução do crime cibernético ilustrado na Figura 1, os fatores motivacionais para o crime cibernético aparecem

como antecedentes de quatro camadas posteriores, as quais consideram objetivos, táticas, métodos e infraestrutura tecnológica (HUNTON, 2011).

Figura 1 – Pilha da Execução do Crime Cibernético



Fonte: adaptado de Hunton (2011)

A gestão da segurança cibernética é também um desafio humano, pois precisa aceitar que indivíduos possuem, além do papel funcional na organização, uma identidade pessoal e social própria, composta por atitudes, crenças e percepções (ASHENDEN, 2008). Adicionalmente, o meio em que essas pessoas se encontram apresenta variáveis com significativo poder de influência sobre a decisão pelo crime. O papel do agressor tem características comuns em todos os crimes (WILLISON; SIPONEN, 2009). Conforme os estudos recentes da criminologia, as causas desse fenômeno devem considerar, além do perfil do agressor, a maneira como o crime foi cometido, analisando características existentes no contexto (cena do crime) como fatores de impacto.

Diante do exposto, a questão de pesquisa a ser respondida neste trabalho é: **como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham?**

1.2 OBJETIVOS

Com a finalidade de compreender um fenômeno com impacto direto na segurança cibernética e, conseqüentemente, na gestão da maioria das organizações que competem e colaboram em um ambiente complexo e virtual, os objetivos deste trabalho estão apresentados a seguir.

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é **analisar como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham.**

1.2.2 Objetivos Específicos

Para atingir o objetivo geral, o trabalho apresenta os seguintes objetivos específicos:

- a) Analisar os principais aspectos da justiça organizacional;
- b) Analisar as principais percepções de injustiça manifestadas por *insiders*;
- c) Analisar as principais motivações para a prática de crimes cibernéticos.

1.3 JUSTIFICATIVA

A sociedade moderna apresenta uma crescente dependência por recursos de TI (MAGKLARAS; FURNELL, 2005; WILLISON; SIPONEN, 2009). Sistemas de tráfego aéreo, telecomunicações, defesa e distribuição de energia são exemplos de infraestruturas de missão crítica controladas com o uso de TI (MAGKLARAS; FURNELL, 2005). O crescimento exponencial das comunicações via Internet aliado às diferentes motivações e capacidades para explorar as vulnerabilidades inerentes a tecnologia computacional, provocou um relevante aumento nos incidentes de segurança cibernética (JANG-JACCARD; NEPAL, 2014).

Embora o setor privado, os governos, as forças armadas e a academia já tenham investido em infraestrutura e pesquisas, estudos indicam que as perdas decorrentes das falhas

de segurança cibernética continuam aumentando anualmente (ROGERS, MANUS, 2006). E o cenário pode ser ainda pior, considerando que muitas empresas simplesmente não informam sobre as perdas com o crime cibernético (HYMAN, 2013).

Cada vez mais rápido, surgem ameaças internas decorrentes do mau comportamento dos próprios membros da organização (LEACH, 2003). “Atacantes estão se movendo mais rápido; as defesas não”, reportam os engenheiros e consultores da *Symantec* (SYMANTEC, 2015). Neste relatório, a referida empresa ressalta que os atacantes cibernéticos atualizam suas técnicas, e as organizações ainda lutam com velhas táticas já ineficazes.

A pesquisa de segurança global da informação de 2014 publicada pela consultoria *Ernest & Young* (EY) demonstra que 67% dos entrevistados percebem ameaças crescentes que impactam diretamente no dimensionamento dos riscos à informação (KESSEL; ALLAN, 2014). No contexto das pequenas e médias empresas brasileiras, dados coletados sobre a adoção de controles de segurança cibernética, demonstram que aspectos relacionados ao risco do fator humano carece de conhecimento, atenção e investimento (SILVA NETTO; SILVEIRA, 2007). Gestores dessas organizações, conforme este estudo, ainda dedicam seus esforços, principalmente, aos mecanismos de segurança de ordem física e tecnológica, tais como controles de acesso e soluções de antivírus, *backup* e *firewall*. Trata-se de uma estratégia de defesa orientada a proteção do perímetro, a qual tem demonstrado ser cada vez menos eficaz (JANG-JACCARD; NEPAL, 2014).

Atualmente, já é possível encontrar na literatura acadêmica e prática estudos sobre o comportamento do *insider* antes e durante a perpetração de um crime cibernético. Todavia, ainda é necessário desenvolver estudos que melhorem a compreensão sobre o papel que os fatores relacionados ao local de trabalho desempenham nesse processo (WILLISON; WARKENTIN, 2009). O estudo sobre a influência que o descontentamento dos indivíduos em relação ao local de trabalho exerce sobre a motivação para a prática do crime cibernético ainda necessita atenção dos pesquisadores. Especialmente no contexto das organizações brasileiras, a interação entre o invasor e a respectiva dinâmica ambiental ainda está pouco explorada na literatura (WILLISON, 2006). A compreensão desta complexa e mutante relação pode contribuir com a melhoria das atuais práticas de segurança cibernética à disposição dos gestores. Busca-se, com isso, a identificação de novas áreas relacionadas à salvaguarda da informação, da TI e, por conseguinte, das pessoas e seus respectivos interesses.

A falta de consciência sobre o problema pode multiplicar as perdas (EYGL, 2014b). Dados coletados em uma pesquisa global sobre fraudes realizadas entre dezembro de 2014 e janeiro de 2015, com mais de 2.700 executivos em 59 países, mostram que as organizações

enfrentam riscos que não estão retrocedendo (EYGL, 2014b). Conforme esse estudo, metade dos entrevistados considera baixa a probabilidade de perdas com crimes cibernéticos, sendo que 17% deles declararam “risco muito baixo”. Os resultados desta pesquisa indicam provável desconhecimento em relação à escala e gravidade que as ameaças cibernéticas representam aos seus negócios (EYGL, 2014b).

Para reduzir os impactos provocados por criminosos cibernéticos é necessário compreender as pessoas por trás dos ataques (ROGERS, MANUS, 2006). Conhecer o inimigo e o ambiente onde ocorrerá a batalha não é um conceito novo, pois tem sido parte da estratégia militar a séculos.

Se você conhecer o inimigo e conhecer a si mesmo, não precisará ter medo do resultado de cem batalhas. Se você conhecer a si mesmo, mas não conhecer o inimigo, para cada vitória conquistada, haverá uma derrota. Se você não conhecer o inimigo e nem a si mesmo, irá fracassar em todas as batalhas (TZU, 2009 p. 30).

Criminosos cibernéticos têm financiamento, são pacientes, sofisticados, e com objetivos que vão além do tecnológico, pois envolvem processos e pessoas (EYGL, 2014a). Portanto, organizações precisam adotar uma abordagem proativa, pois "antecipar os ataques cibernéticos é a única maneira de estar à frente desses criminosos" (KESSEL; ALLAN, 2014, p. 1). Além disso, identificar as motivações para ataques cibernéticos é uma necessidade para a produção de provas consistentes que possam conduzir satisfatoriamente os processos contra os incriminados. Por fim, reconhecer a intenção para um crime cibernético permite prever danos indesejáveis (WU; ZHIGANG; JUNHUA, 2009).

Estudar o comportamento das pessoas possibilita então um melhor entendimento dos crimes cibernéticos e de possibilidades de controle e prevenção (ME; SPAGNOLETTI; IEEE, 2005). As características desse comportamento humano, por sua vez, sofrem influências do contexto em que estão inseridos indivíduos potencialmente motivados para o crime. Embora a pesquisa sobre crimes cibernéticos praticados por *insiders* esteja relativamente madura, ainda é frágil o entendimento sobre o problema do descontentamento no espaço organizacional e como esta condição impacta na motivação das pessoas para o crime (WARKENTIN; WILLISON, 2009).

O desafio de analisar as ações retaliatórias que ocorrem no local de trabalho e os respectivos prejuízos financeiros, sociais e organizacionais que tais ações provocam demanda que pesquisadores investiguem os determinantes desta conduta prejudicial. O investimento em estudos que levem ao melhor entendimento sobre do comportamento humano em assuntos de

segurança cibernética torna possível aumentar a produção de soluções destinadas à proteção das organizações contra ataques cibernéticos (PFLEEGER; CAPUTO, 2012).

Para garantir proteção adequada aos ativos organizacionais, gestores precisam ter uma visão clara daquilo que precisam salvaguardar (SON, 2011). É necessário compreender as características e o perfil dos potenciais atacantes para que estratégias de segurança sejam implantadas com sucesso. O desenvolvimento de políticas de segurança alinhadas com os interesses da organização é pré-requisito para um programa de gerenciamento de segurança cibernética (SON, 2011). É por essa razão que o sucesso da estratégia de segurança cibernética poderia ser obtido se organizações investissem equilibradamente em recursos técnicos e sócio-organizacionais (BULGURCU; CAVUSOGLU; BENBASAT, 2010). O risco de danos graves aos ativos organizacionais por parte de funcionários, clientes, fornecedores e *stakeholders* não pode ser subestimado (WILLISON, 2005). Uma abordagem holística para a segurança cibernética que combine as pessoas, os processos e a tecnologia seria extremamente útil para ajudar os gerentes a dar foco em comportamentos e atividades que efetivamente representem risco (MILLS et al., 2011).

Portanto, estudos que apresentem novas perspectivas com amplo espectro de análise em relação ao tema do crime cibernético poderão contribuir ainda mais para o desenvolvimento de medidas preventivas que despertem interesse dos gestores e das organizações. Não faltam justificativas para investir nesse tipo de pesquisa, na medida em que a falta de entendimento sobre o tema custará muito mais caro para as organizações.

1.4 ESTRUTURA DO TRABALHO

Este trabalho está organizado em seis capítulos. A primeira parte é composta pela introdução, onde estão inseridos a delimitação do tema e o problema de pesquisa, os objetivos e a justificativa deste estudo. No capítulo 2, encontra-se a revisão de literatura sobre crime cibernético, motivações, sentimentos humanos e a temática da justiça organizacional. O terceiro capítulo contém o método utilizado na pesquisa, incluindo o desenho e o instrumento de pesquisa, bem como as informações sobre o processo de coleta de dados. No quarto capítulo, a análise dos dados coletados é apresentada; e no capítulo seguinte, é realizada uma discussão dos resultados obtidos. Por fim, no capítulo 6 apresenta-se as considerações finais, além das contribuições da pesquisa (acadêmicas e práticas), suas limitações e sugestões para estudos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Na medida em que o universo virtual ia se tornando cada vez mais vulnerável ao crime, e que os ataques criminosos ganhavam repercussão e importância na estratégia de proteção organizacional, intensificou-se o debate entre acadêmicos e práticos a respeito da originalidade do conceito relacionado ao crime cibernético (YAR, 2005). Enquanto alguns estudos indicavam para um novo fenômeno que demandava um arcabouço teórico próprio, outros trabalhos avaliavam tal fenômeno como uma simples variação do crime tradicional, já bastante analisado no campo da criminologia (YAR, 2005).

Um fato relevante sobre o crime cibernético no contexto das organizações é a sua perpetração por pessoas internas, munidas de confiança e autorização para acessar sistemas e infraestruturas de TI (DHILLON, 2001). Percebeu-se que a maioria das violações relacionadas a segurança cibernética nas empresas era cometida pelos seus próprios funcionários (DHILLON; MOORES, 2001). Capacitados e motivados a subverter proteções e controles inerentes aos ativos organizacionais, essas pessoas passam a praticar crimes no contexto cibernético, produzindo danos de natureza social, econômica, pessoal e organizacional.

Este capítulo analisa teorias prévias relacionadas ao crime as quais apresentam elementos importantes que podem exemplificar a problemática do crime cibernético. Em seguida, discute-se as características e o impacto do crime cibernético, especialmente aquele em que ocorre nas organizações, com a participação direta dos seus funcionários. No próximo item, o capítulo de fundamentação revisa as motivações humanas, suas teorias e relações com o crime cibernético. Adiante, discute-se a questão dos sentimentos humanos, especialmente aqueles de caráter negativo. Por fim, o tema da justiça organizacional é apresentado considerando sua definição seminal e quatro conceitos subjacentes que possuem relação e relevância com os objetivos desta pesquisa. O modelo conceitual proposto na última parte deste capítulo estabelece conexões entre os conceitos inerentes ao tema desta pesquisa, cujas relações serão efetivamente avaliadas na etapa de análise dos dados coletados.

2.1 ABORDAGENS TEÓRICAS DO CRIME

Compreender a motivação criminal é um desafio presente nas pesquisas até os dias atuais. Época, culturas, valores, cenários políticos, econômicos e sociais são variáveis dinâmicas e complexas que atuam sobre as atitudes e o comportamento das pessoas.

As teorias que foram sendo desenvolvidas sobre o crime abrangem as motivações e o comportamento dos indivíduos, bem como a epidemiologia associada a este fenômeno social (CRESSEY, 1968). Fatores genéticos, sociais ou ambientais, bem como as respectivas condições derivadas de uma determinada exposição vinculam-se, nestas abordagens teóricas, com a distribuição espacial e temporal desses elementos (CRESSEY, 1968). A seguir, é apresentado um resumo das principais abordagens teóricas que analisam as causas do crime sob diferentes perspectivas.

As teorias relacionadas às patologias individuais explicam o comportamento criminoso a partir de três categorias: de natureza biológica, psicológica e psiquiátrica (CERQUEIRA; LOBÃO, 2003). Indicadores para uma patologia criminosa estariam relacionados às características físicas e mentais do indivíduo. Uma das principais hipóteses era que a baixa inteligência seria uma importante causa da criminalidade (CRESSEY, 1968).

As teorias relacionadas à desorganização social têm uma abordagem sistêmica, explicando o crime como uma derivação de um complexo sistema de redes de associações formais e informais (comunidades locais), de relações de amizades, parentescos e demais formas de socialização e aculturação do indivíduo (CERQUEIRA; LOBÃO, 2003). Essas relações sociais sofrem, conforme essa abordagem, influência de fatores estruturais, como status econômico, heterogeneidade étnica, mobilidade residencial, desagregação familiar e urbanização. O crime emergiria a partir de organizações sociais problemáticas e indesejáveis (ENTORF; SPENGLER, 2000).

As teorias relacionadas ao estilo de vida agrupam três elementos fundamentais: uma vítima em potencial, um agressor em potencial e uma tecnologia de proteção, ditada pelo estilo de vida da vítima em potencial. Quanto maior a proteção, maior será o custo para perpetrar o crime, e menores as oportunidades do agressor. Neste caso, indivíduos que permanecem mais tempo em espaços públicos, teriam mais chances de sofrer uma agressão. Pessoas que trabalham em casa ou moram com outros familiares, teriam menos chance de serem vitimadas (CERQUEIRA; LOBÃO, 2003). Essa perspectiva sobre o crime peca em não analisar os fundamentos do indivíduo relacionados à sua motivação, comportamento e epidemiologias associadas. O foco está direcionado para os hábitos das vítimas, aproximando tal abordagem de uma tautologia e não de uma teoria.

As teorias relacionadas à associação diferencial (SUTHERLAND; SCHUESSLER, 1973) analisam os processos sociais, através dos quais, os indivíduos determinam seus comportamentos a partir de suas experiências pessoais em situações de conflito. A determinação favorável ao crime seria aprendida nas interações sociais mediante as

comunicações interpessoais. Neste sentido, a família (supervisão dos pais), as amizades (envolvimento com grupos delinquentes) e a comunidade em geral têm papel relevante nesse processo (CERQUEIRA; LOBÃO, 2003).

A pressão social é aquela que os indivíduos sentem para atingir metas determinadas pela sociedade como necessárias, valorosas ou importantes (ARVANITES; DEFINA, 2006). Essa pressão é intensificada na medida em que se alarga a distância entre objetivos e meios para atingi-los; ou seja, a discrepância entre aspiração e expectativa. Uma implicação da tensão social é que as pressões para atingir metas socialmente estabelecidas conduzem os indivíduos a persegui-las por meios ilegítimos, quando os legítimos estão indisponíveis ou inalcançáveis (ARVANITES; DEFINA, 2006). A teoria geral da tensão corrobora com essa perspectiva, determinando que a motivação criminosa é produto da exposição a tratamentos e condições negativas, de forma que as pessoas se sintam mal, e sejam pressionadas a remediar esta situação (AGNEW, 1992). Sob essas condições, a tensão pode estimular a crença de que o crime compensa.

As teorias relacionadas à aprendizagem social estabelecem que, em um sistema de aprendizado social, padrões de comportamento podem ser adquiridos através da experiência direta ou pela observação do comportamento de outros indivíduos (BANDURA; MCCLELLAND, 1977). Esta seria a forma mais rudimentar de aprendizado, enraizada na experiência direta, amplamente governada pela gratificação ou pela punição sobre os atos realizados (BANDURA; MCCLELLAND, 1977). Algumas práticas sociais são adquiridas pelo condicionamento ou imitação (AKERS et al., 1979). Um comportamento é incentivado por recompensas, ao mesmo tempo que é evitado pela perspectiva da punição ou pela perda de gratificações. Em síntese, as pessoas adquirem, pela convivência social, noções sobre as normas de conduta estabelecidas. Quanto mais os indivíduos definem um determinado comportamento como bom e desejável, mais provável será vivenciá-lo (AKERS et al., 1979).

As teorias relacionadas ao controle social procuram compreender porque alguns indivíduos não cometem crimes. O foco está em analisar os elementos capazes de dissuadir a intenção criminal os quais estão relacionados à ligação do indivíduo com a sociedade (acordo social). Nesta perspectiva, quanto maior for o envolvimento no sistema social, maior será o grau de concordância do indivíduo com os valores e normas vigentes (CERQUEIRA; LOBÃO, 2003). Assim, menores seriam as chances de engajamento ao crime.

As teorias relacionadas ao autocontrole analisam a capacidade das pessoas em antecipar e agir perante consequências negativas de determinados atos, com base em forças internas contrárias às atrações que despertam as motivações (TITTLE; BOTCHKOVAR,

2005). Considera-se que os indivíduos que apresentam vícios ou comportamento desviante não desenvolveram mecanismos psicológicos de autocontrole na infância e adolescência. O processo de socialização desses indivíduos foi ineficaz, evidenciando falha na respectiva conduta educacional. Pais e mães que não conseguiram estabelecer limites, endossando um comportamento egoísta de filhos que passam a agir com base em interesses próprios (CERQUEIRA; LOBÃO, 2003).

Aqueles que praticam o crime estão sensíveis ao prazer imediato, e insensíveis às consequências de longo-prazo. A criminalidade está diretamente relacionada ao baixo autocontrole, aumentando a probabilidade de que indivíduos incapazes de resistir à fácil e imediata gratificação pratiquem o crime (PRATT; CULLEN, 2000). O autocontrole forte tende a resistir às tentações, enquanto o fraco tende a sucumbir (TITTLE; BOTCHKOVAR, 2005). Conforme o grau de efetividade desta capacidade de contenção motivacional, bem como dos níveis de percepção das respectivas consequências, as forças impeditivas para o ato de violar aumentam ou diminuem. O autocontrole é um mecanismo interno, influenciado por restrições externas que contradizem os eventuais estímulos motivacionais para o crime (TITTLE; BOTCHKOVAR, 2005). Adicionalmente, evidências indicam que as características individuais de personalidade interferem na probabilidade de cometer crimes (BURT; SIMONS, 2013). O crime pode ser atraente, mas a intensidade dessa atração varia.

Em âmbito sociológico, a anomia (MERTON, 1938) explica que a motivação para a delinquência seria resultante da impossibilidade de atingir metas desejadas pelo indivíduo, tais como o status social ou o sucesso econômico. Os estudos nesse campo abriram três perspectivas subjacentes: a) as diferenças das aspirações individuais e os meios econômicos disponíveis, ou expectativa de realização; b) oportunidades bloqueadas (indivíduo percebe que seu insucesso é consequência de forças externas), e c) privação relativa (distância entre o ideal de sucesso vivido por algumas pessoas e aquela situação específica em que o indivíduo se encontra) (CERQUEIRA; LOBÃO, 2003).

A igualdade pode ser aspiração dos invejosos, que almejam os mesmos favores dos privilegiados; dos despeitados, que pretendem o rebaixamento dos demais; dos perversos, felizes ao assistir a desgraça dos outros; dos vingativos, que desejam aos outros os mesmos males que sofreram (RADBRUCH; MONCADA, 1961, p. 25).

A teoria interacional propõe que o comportamento desviante ocorre em um processo interacional dinâmico (THORNBERRY, 1987). A delinquência é causa e consequência de uma variedade de relações recíprocas desenvolvidas ao longo do tempo. Esta abordagem é suportada por dois elementos (ENTORF; SPENGLER, 2000): a perspectiva evolucionária e

os efeitos recíprocos. A primeira declara que o crime não é constante na vida do indivíduo, possuindo um momento de iniciação, evolução e encerramento. Os efeitos recíprocos dizem respeito à relação intrínseca das variáveis a serem explicadas, como por exemplo, ligação com os pais, envolvimento escolar, grupos de amizades, punição paternal para desvios, e ligação com grupos delinquentes (CERQUEIRA; LOBÃO, 2003).

As teorias relacionadas à escolha racional econômica estabelecem que o ato criminoso decorre de uma avaliação racional em torno dos custos e benefícios relacionados ao exercício do crime (BECKER, 1974). Implicitamente, o potencial agressor realiza uma análise em que compara a iniciativa criminosa em relação ao esforço equivalente de trabalho lícito. Estudos posteriores incluíram dois vetores condicionantes: os fatores positivos (que levariam o indivíduo a escolher o mercado legal), como o salário, direitos e garantias legais, etc. De outro, os fatores negativos, ou dissuasórios, tais como a eficiência do poder de polícia (captura) e as consequências legais (punição) (CERQUEIRA; LOBÃO, 2003).

O trabalho de Cantor e Land (1985) construiu a base para a relação entre as condições econômicas e crime. Eles apresentam duas possibilidades para que os ciclos de negócio afetem a motivação criminal (ARVANITES; DEFINA, 2006): a primeira deriva do impacto da evolução das condições econômicas na deformação social e no controle social. A segunda consiste em influenciar a disponibilidade e vulnerabilidade de alvos potenciais, e, portanto, as oportunidades criminais. Em uma economia fraca, a motivação criminal poderia aumentar, porém as oportunidades reduziriam (CANTOR; LAND, 1985).

Na medida em que as condições econômicas se transformam de maneira assíncrona, oportunidades ocorreriam em descompasso com as respostas motivacionais para o crime (ARVANITES; DEFINA, 2006). O aprofundamento de um cenário de recessão econômica mostrou relação com o aumento de práticas criminosas, quando indivíduos tornam-se mais propensos a cometer violações, uma vez que se encontram presumidamente em estado de privação material (YEARWOOD; KOINIS, 2011). Uma condição financeira desfavorável influenciaria significativamente a propensão à delinquência. Presume-se, desta forma, que uma economia mais pobre aumentaria a motivação criminal.

A seguir, o Quadro 1 sintetiza as abordagens teóricas desenvolvidas na literatura sobre o crime, ressaltando as principais variáveis de cada uma delas.

Quadro 1 – Abordagens Teóricas sobre a Criminalidade

(Continua)

Teoria	Abordagem	Variáveis
[1] Patologias Individuais	Criminalidade é uma doença. Algumas características físicas e biopsicológicas constituiriam indicadores da patologia criminosa.	Formação óssea do crânio, formato de orelhas, pouca inteligência, desordens mentais, alcoolismo, neuroses, neuropatologias.
[2] Desorganização Social	Abordagem sistêmica em torno das comunidades, entendidas como um complexo sistema de rede de associações formais e informais.	Condição socioeconômico; familiar; étnica; mobilidade residencial; desagregação urbanização; redes de amizades locais; grupos de adolescentes sem supervisão; participação institucional; desemprego; existência de mais de um morador por cômodo.
[3] Estilo de Vida	Conforme essa perspectiva, existem três elementos fundamentais: uma vítima em potencial, um agressor em potencial e uma tecnologia de proteção, ditada pelo estilo de vida da vítima em potencial.	Provisão de recursos, custos do crime, menores oportunidade. Indivíduos que possuem atividades de lazer dentro de casa estão menos expostos. Pessoas que trabalham fora ou moram sozinhas são vítimas potenciais.
[4] Associação Diferencial	Os indivíduos determinam seus comportamentos a partir de suas experiências pessoais com relação a situações de conflito, por meio de interações pessoais e com base no processo de comunicação.	Grau de supervisão familiar; intensidade de coesão nos grupos de amizades; existência de amigos com problemas com a polícia; percepção dos jovens sobre outros envolvidos em problemas de delinquência; jovens morando com os pais; contato com técnicas criminosas.
[5] Aprendizagem Social	Condicionamento ou imitação. Padrões de comportamento podem ser adquiridos através da experiência direta ou pela observação.	A relação entre recompensas e punições. Estímulos adversos ou gratificações produzem reações. Normas e atitudes dos grupos sociais.
[6] Controle Social	O que leva o indivíduo a não enveredar pelo caminho da criminalidade? A crença e a percepção do mesmo em concordância com o contrato social (acordos e valores vigentes), ou o elo com a sociedade.	Envolvimento do cidadão no sistema social; concordância com os valores e normas vigentes; ligação filial; amigos delinquentes; crenças desviantes.

(Conclusão)

Teoria	Abordagem	Variáveis
[7] Autocontrole	O não desenvolvimento de mecanismos psicológicos de autocontrole na fase que segue dos 2 anos à pré-adolescência, que geram distorções no processo de socialização, pela falta de imposição de limites.	Frequentemente eu ajo ao sabor do momento sem medir consequências; eu raramente deixo passar uma oportunidade de gozar um bom momento.
[8] Anomia	Impossibilidade de o indivíduo atingir metas desejadas por ele. Três enfoques: a) diferenças de aspirações individuais e os meios disponíveis; b) oportunidades bloqueadas; e c) privação relativa.	Participa de redes de conexões? Existem focos de tensão social? Eventos de vida negativos; sofrimento cotidiano; relacionamento negativo com adultos; brigas familiares; desavenças com vizinhos; tensão no trabalho
[9] Interacional	Processo interacional dinâmico, onde constata-se dois ingredientes principais: a) perspectiva evolucionária, cuja carreira criminal inicia-se aos 12-13 anos, ganha intensidade aos 16-17 anos e finaliza aos 30 anos; e b) perspectiva interacional que entende a delinquência como causa e consequência de um conjunto de fatores e processo sociais.	As mesmas daquelas constantes nas teorias do aprendizado social e do controle social.
[10] Escolha Racional Econômica	O indivíduo decide sua participação em atividades criminosas a partir da avaliação racional entre ganhos e perdas esperadas advindos das atividades ilícitas vis-à-vis o ganho alternativo no mercado legal	Salários; renda familiar per capita; desigualdade da renda; acesso a programas de bem-estar social; eficiência da polícia; adensamento populacional; magnitude das punições; inércia criminal; aprendizado social; educação.
[11] Ecológico	Combinação de atributos pertencentes a diferentes categorias condicionaria a delinquência. Esses atributos, por sua vez, estariam incluídos em vários níveis: estrutural, institucional, interpessoal e individual.	Todas as variáveis anteriores podem ser utilizadas nessa abordagem.

Fonte: adaptado de Cerqueira e Lobão (2003)

2.2 O CRIME CIBERNÉTICO NAS ORGANIZAÇÕES

A adoção da Internet possibilitou a interação virtual, *on-line*, a partir de qualquer ponto do globo, em um ambiente comum denominado ciberespaço. Atualmente, quase todos

os elementos de uma organização têm alguma dimensão cibernética. Sistemas e equipamentos oferecem cada vez mais funcionalidades e integração. O crime, por sua vez, não demorou a se manifestar no espaço cibernético. As ameaças e os riscos aos ativos organizacionais, conseqüentemente, aumentaram (VASHISTH; KUMAR, 2013). A denominação do crime que ocorria dentro das fronteiras do ciberespaço, utilizando computadores e dispositivos que compõe essa rede mundial, ficou conhecida como crime cibernético ou *cybercrime* (HUNTON, 2009). Essa terminologia é rótulo para atividades ilegais e comportamentos indesejáveis que envolvem o uso de tecnologias interligadas em rede (HUNTON, 2011). Um único indivíduo pode, em tempo real, alcançar, interagir e afetar milhares de pessoas simultaneamente (YAR, 2005). Embora dispondo de mínimos recursos, é possível provocar enormes efeitos negativos.

A informação é um ativo organizacional essencial, e conseqüentemente, precisa ser protegida da melhor forma possível (CAMPOS, 2006). A segurança cibernética visa proteger a integridade, a disponibilidade e a confidencialidade da informação (BEAL, 2005). Ela é desenvolvida nas organizações para reduzir a ocorrência do crime cibernético, através da aplicação e gestão de medidas adequadas, as quais considerem um diversificado conjunto de ameaças. Os objetivos da segurança cibernética são alcançados pela implantação de um conjunto de controles, tais como políticas, processos, procedimentos, estruturas organizacionais, *softwares* e *hardwares* (ISO/IEC_27000, 2014). Estes controles devem ser continuamente monitorados e atualizados para garantir um adequado alinhamento com os objetivos do negócio (ISO/IEC_27000, 2014).

Dinâmico e em constante evolução, o crime cibernético é um crime econômico com amplitude global, de complexa identificação e rastreamento, com impactos variados, cujos riscos e recompensas diferem do crime convencional (PARTON, 2011). São atividades ilegais realizadas mediante o uso da tecnologia, com objetivo de acessar ou comprometer sistemas computacionais (BURDEN; PALMER, 2003). Compreendem atos desonestos ou maliciosos, originados no ambiente virtual ou herdados do mundo real, e que são perpetrados na Internet, onde criminosos encontram a sensação de facilidade, anonimidade, velocidade de operação e uma enorme quantidade de alvos (BURDEN; PALMER, 2003). Estes alvos, naturalmente, variam. O ataque pode ser diretamente contra o sistema de informação, o qual pode ser ferramenta ou suporte tecnológico para realização do crime (ME; SPAGNOLETTI; IEEE, 2005). Em outros casos, um sistema de informação comporta-se apenas como repositório passivo de dados relativos a um crime (ME; SPAGNOLETTI; IEEE, 2005).

Os criminosos deste universo virtual já realizaram invasões em organizações tradicionais da área da segurança, tais como Interpol, Casa Branca, Pentágono, OTAN, bancos e operadoras de cartão de crédito; e já foram recrutados pela Máfia Italiana, Yakuza Japonesa, gangues chinesas, cartéis colombianos e grupos do crime organizado na Rússia e Malásia (KSHETRI, 2010). Os cibercriminosos possuem atuação global e organizada, e desafiam as medidas de segurança e os órgãos de investigação no mundo inteiro. Eles visam violar a confidencialidade, integridade e disponibilidade de dados e informações (SÊMOLA, 2003). Corrompem, indiretamente, a conformidade, legalidade, propriedade e rastreabilidade do conteúdo produzido e armazenado no universo cibernético (SÊMOLA, 2003).

Em linhas gerais, o crime cibernético ocorre nas redes de computadores (YAR, 2005), e vem sendo identificado desde a criação da Internet (NYKODYM; TAYLOR; VILELA, 2005). Introduziu-se novos conceitos e um vocabulário próprio, apesar da visão cética de que, na melhor das hipóteses, essas atividades criminosas estariam diferenciadas apenas por ferramentas e técnicas específicas (YAR, 2005). Ele é composto, normalmente, por ataques baratos, convenientes, sofisticados, com foco definido ou aleatório, indiferentes à distância geográfica ou nacionalidade (PADMAVATHI; SHANMUGAPRIYA, 2009). Portanto, a atribuição de responsabilidade para essa modalidade criminal é difícil, fortalecendo a sensação de impunidade e baixo risco percebida pelo criminoso quando este compara os riscos a serem administrados no mundo real (PADMAVATHI; SHANMUGAPRIYA, 2009).

Vários termos foram utilizados para descrever o comportamento criminoso envolvendo computadores na literatura (MCQUADE, 2006): ciber criminalidade (*computer-related crime*), crime cibernético (*cybercrime*), crime tecnológico (*technological crime*), crime auxiliado por computador (*computer-assisted crime*), crimes digitais (*digital crime*), crimes eletrônicos (*electronic crime*) e crime de Internet (*Internet crime*). Um elemento comum entre essas definições é a utilização ilegal de dispositivos tecnológicos por indivíduos, grupos ou organizações que possuem conhecimento avançado na área de TI (MOON; MCCLUSKEY; MCCLUSKEY, 2010).

Originalmente, os crimes cibernéticos foram separados em dois grupos, de acordo com sua natureza (BURDEN; PALMER, 2003). Existem os atos criminosos já conhecidos no mundo real, os quais foram viabilizados no ciberespaço, tais como fraudes, roubos de informação, difamação, chantagem, pornografia, lavagem de dinheiro, violação da propriedade intelectual e terrorismo (BURDEN; PALMER, 2003). Por outro lado, existem os crimes cibernéticos puros, que compreendem atos desonestos ou mal-intencionados que não existiriam fora do ambiente virtual. Neste grupo, é possível citar o vandalismo virtual, a

disseminação de vírus ou *softwares* maliciosos, os ataques de negação de serviço, a falsificação de endereços na Internet e o envio de spam ou mensagens eletrônicas indesejadas (BURDEN; PALMER, 2003). A classificação dos tipos de crimes cibernéticos considera fatores como os meios utilizados para o crime, o tipo de dano causado às vítimas, a natureza da atividade criminosa e, não menos relevante, as motivações pessoais para cometer um crime cibernético (CHUNG et al., 2006).

As definições supracitadas englobam duas perspectivas subjacentes que são inerentes ao crime cibernético (FURNELL, 2003): ações que ocorrem com apoio da computação (crimes anteriores à Internet que adquirem uma nova perspectiva); e ações que nasceram com a computação em rede. Estas últimas surgiram em paralelo com a Internet, e não poderiam existir além dela, como por exemplo, as atividades de *hacking*, a inundação de tráfego de rede para negação de serviço, os ataques virais, e o vandalismo virtual (FURNELL, 2003). Essas duas perspectivas ressaltam papéis distintos desempenhados pela tecnologia.

Invasões, destruições, sobrecargas, falsificações, pirataria, contaminações, espionagem, roubos, fraudes, lavagem de dinheiro, desrespeito a propriedade intelectual, distribuição de materiais ilícitos, assédio moral e sexual, preconceito, discurso do ódio, pornografia, pedofilia entre outras ações ilegais e imorais são operacionalizadas através de vírus de computador, *worms*, *logic bombs*, *trojan horses*, *backdoors*, *exploits*, *rootkits*, *spammers*, *keyloggers*, *denial of service attacks*, *spywares*, *phishing*, *vishing*, *pharming*, *spoofing*, *sniffing* ou *data leakage* (vazamento de dados) (CHOO, 2011; HUNTON, 2009; PENNING et al., 2014). Tais iniciativas são exemplos comuns de crimes cibernéticos, os quais estão caracterizados de modo detalhado no Apêndice C.

Uma definição final, ratificada e amplamente aceita pela comunidade acadêmica e profissional ainda carece de unanimidade. Pesquisadores concordam que o crime cibernético trata de atividades ilegais realizadas através de um computador ou dispositivo conectado à Internet (CHUNG et al., 2006). Alguns discordam sobre a sua delimitação espacial, no que tange o local onde acontecem (CHUNG et al., 2006) e, por conseguinte, no espectro social em questão. O foco deste debate na literatura questiona se o crime cibernético é, de fato, uma novidade que obrigaria dispensar, modificar, complementar ou estender o conjunto de teorias já existentes no campo da criminologia; ou, se ele é somente uma variação de um fenômeno social antigo e conhecido, cujas casualidades e influências têm explicações já estabelecidas na literatura (YAR, 2005).

Estudos recentes apresentam o crime cibernético como um fenômeno que sofre influência de elementos ligados a criminologia tradicional, possuindo, contudo, características

inerentes a um contexto virtual exclusivo, com propriedades e elementos próprios. As teorias tradicionais sobre o crime abordam tipos, características, perfis e motivações relacionados ao fenômeno. Elas ajudam a compreender as peculiaridades do crime no contexto cibernético na medida em que analisam o fator humano como elemento central dos atos criminosos. Assim, torna-se evidente a importância de considerar as explicações teóricas sobre o crime e suas motivações ao estudar o fenômeno dentro do escopo cibernético.

2.2.1 O Impacto do Crime Cibernético

Desde a identificação das vulnerabilidades no ambiente computacional na década de 1980 (SPAFFORD, 1994), usuários da TI têm sido submetidos a uma série de riscos de segurança cibernética, intrusões e ataques virtuais nas formas de roubo de informação, espionagem, violação da privacidade, indisponibilidade de serviços, implantação indevida de software malicioso (*malwares*), fraudes financeiras, falsidades e extorsão (MARTIN; RICE, 2011). Os dispositivos móveis (*smartphones* e *tablets*) utilizados amplamente na vida pessoal e profissional dos indivíduos, a partir de 2004, também são alvos de infecções (PENNING et al., 2014). A intrusão de um sistema de informação é “uma atividade que viola a política de segurança” (NING; JAJODIA; WANG, 2004, p. xv) e configura-se, desta forma, num ato ilegal.

Investigações, nos últimos cinco anos, demonstram, mediante dados quantitativos, a relevância que o crime cibernético assumiu na estratégia de gestores e líderes empresariais (PRICEWATERHOUSECOOPERS, 2014). Segundo este relatório, os casos de violação de segurança continuam crescendo e os prejuízos por eles causados também. O número de incidentes detectados subiu para 42,8 milhões em 2014 – uma alta de 48% em relação ao ano anterior. Isso é o equivalente a 117.339 ataques recebidos por dia, todos os dias.

Apesar das tentativas de reduzir a ocorrência do crime cibernético nas organizações, sua incidência continua crescendo globalmente (ARPAD, 2013; BACKHOUSE; DHILLON, 1995; CHUNG et al., 2006; JANG-JACCARD; NEPAL, 2014; MARTIN; RICE, 2011; RASMI; JANTAN, 2013). Em 2013, o Brasil perdeu entre 7 e 8 bilhões de dólares com roubos de senha, clonagem de cartões, pirataria virtual, espionagem, entre outros ataques (SCIARRETA, 2014). Esse dado confirma cenários apresentados pelos principais fabricantes de solução de segurança cibernética no mundo. Cita-se, por exemplo, o mapa de ameaças cibernéticas mantido pela *Kaspersky Lab*, o qual apresenta o Brasil entre os cinco países da América do Sul com maior percentual de infecções por vírus de computador, envio de *spam* e

ataques de rede (KASPERSKY-LAB, 2015). O país também apresenta indicadores relevantes (participação no volume total de *spam*, URLs maliciosas, computadores infectados e *malwares* para as plataformas *mobile* e bancária) no relatório publicado pela *Trend Micro* sobre os desafios da segurança cibernética em uma economia de mercado (TREND-MICRO, 2013). Juntamente com Rússia, China, Nigéria e Vietnã, o Brasil participa de um grupo de países em desenvolvimento que abriga cada vez mais ocorrências do crime cibernético em virtude da frouxa legislação relativa ao tema (RAYMAN, 2014). Em 2014, uma pesquisa foi realizada, entrevistando 9.600 executivos em mais de 115 países (ALVES; D'ANDREA, 2014, p. 4):

[...] apesar de o investimento em segurança ter aumentado, nota-se que as empresas ainda se perdem na hora de definir as melhores práticas, têm dificuldade de conduzir análises situacionais e de identificar e priorizar os dados que precisam ser adequadamente resguardados. Poucas estão realmente preparadas para lidar com os riscos crescentes do ciberespaço.

O custo das fraudes vem aumentando desde 2011: 62% dos casos relatados em 2014 geraram prejuízos maiores que US\$ 100 mil, contra 47% na pesquisa de 2011. Para 46% dos entrevistados brasileiros, o comprometimento da reputação da marca é o maior impacto dos crimes econômicos (ALVES; D'ANDREA, 2014). Levando em consideração esses indicadores, no final do ano de 2012, a Presidente Dilma Rousseff sancionou a Lei Carolina Dieckmann, como ficou popularmente conhecida a Lei Brasileira 12.737/2012, a qual altera o Código Penal brasileiro, tipificando crimes e infrações relacionadas ao meio eletrônico (BRASIL, 2012a). A norma estabelece que a violação indevida de equipamentos e sistemas conectados ou não à rede de computadores são considerados crimes cibernéticos (BRASIL, 2012b; BRASIL, 2012c). Igualmente visando a regulamentação do setor, foi sancionado o Marco Civil da Internet, que estabelece direitos e deveres para o uso da Internet no Brasil e cujo texto trata de questões como neutralidade da rede, privacidade dos usuários, retenção de registros de acesso, bem como define a função social que a rede deve cumprir, especialmente no que tange a liberdade de expressão e a transmissão de conhecimento (BRASIL, 2016).

2.2.2 A Ameaça do *Insider*

As ameaças originadas por indivíduos que integram uma organização são amplamente reconhecidas como assunto de extrema importância para a gestão da segurança cibernética (THEOHARIDOU et al., 2005). Uma pesquisa realizada nos Estados Unidos relata que 75%

das organizações registraram fraudes perpetradas pelos seus próprios funcionários, com perdas estimadas em cerca de 652 bilhões de dólares anuais (HOLTON, 2009). O comportamento orientado para o crime já foi observado entre 33 e 75% dos trabalhadores naquele país, destacando a prática de atividades ilícitas relacionadas ao roubo, fraude, desvio de dinheiro, vandalismo, sabotagem, absenteísmo e agressão (ROBINSON; BENNETT, 1995). Neste sentido, as organizações direcionam esforços para reduzir vulnerabilidades no contexto tecnológico, dedicando menos atenção ao escopo dos seus recursos humanos internos (VASHISTH; KUMAR, 2013). Compreender as motivações e as influências que precedem os crimes cibernéticos, principalmente quando os autores desses crimes fazem parte da organização, é decisivo para controlar ameaças e adotar medidas protetivas que reduzam a probabilidade de que vulnerabilidades sejam exploradas, gerando danos organizacionais (D'ARCY; HOVAV, 2008).

Os colaboradores de uma empresa, também denominados *insiders*, usualmente, têm autorização para acessar e utilizar sistemas e recursos computacionais. Desta forma, podem representar um alto risco gerencial, na medida em que cometem erros, contornam políticas, ignoram procedimentos ou mesmo agem de forma incompetente, insuficiente, negligente ou imprevidente (BULGURCU; CAVUSOGLU; BENBASAT, 2010). Entre as várias propriedades dos *insiders* que praticam crimes cibernéticos, uma se destaca: o nível de sofisticação desses indivíduos (MAGKLARAS; FURNELL, 2005). Conforme os autores, estudos indicam que a sofisticação do *insider* e o potencial uso inadequado dos recursos de TI são variáveis fortemente relacionadas. Embora o fator humano necessite de atenção na gestão da segurança cibernética, soluções protetivas ainda operam sobre medidas puramente técnicas (FERNANDO; YUKAWA, 2013).

O fator humano é considerado o elo mais fraco na cadeia da segurança cibernética (BULGURCU; CAVUSOGLU; BENBASAT, 2010). A ameaça interna é complexa devido a uma variedade de fatores que a torna de difícil detecção até que realize danos (MILLS et al., 2011). Tais ameaças podem ser analisadas sob três perspectivas de comportamento (WILLISON; WARKENTIN, 2013): 1) passivo e não volitivo, ocorre quando um *insider* está negligente, descuidado, desmotivado ou mal treinado, e age de forma não deliberada contra as normas e políticas de segurança da organização; 2) volitivo, porém sem motivação maliciosa, quando esse *insider* quebra regras de segurança em benefício próprio sem a intenção de produzir graves danos organizacionais; e por fim 3) maliciosamente intencional, quando o *insider* realiza ações imorais ou ilegais com objetivo de destruir, roubar, fraudar, prejudicar ou revelar informações sensíveis em benefício próprio ou de terceiros.

Os *insiders* têm vantagens que vão além da capacidade de acesso à infraestrutura de TI. Eles estão cientes sobre vulnerabilidades e informações sensíveis: quais são, onde estão, quanto valem, como e quando acessá-las (NEUMANN, 1999). Possuem tempo e tranquilidade para atingir seus objetivos; e, não raro, conseguem ocultar rastros.

2.3 AS MOTIVAÇÕES HUMANAS

A necessidade individual que desencadeia ações direcionadas a um objetivo específico pode ser determinada pela hereditariedade, pelo ambiente e pelas interações sociais (KANFER, 1992). Tais fatores influenciam características individuais, como personalidade, sentimentos, atitudes, crenças e habilidades. Por sua vez, estes fatores impactam nas ações escolhidas, na intensidade do esforço, bem como na resistência do comportamento orientado a um determinado objetivo (KANFER, 1992).

As pessoas motivam-se conforme um senso particular de comprometimento, ou pelo medo de estarem sendo vigiadas (DECI; RYAN, 2000). Podem encaminhar suas ações a partir de aspirações, pretensões ou interesses pessoais legítimos. Alternativamente, movimentam-se por estímulos externos, como ameaças, chantagens, culpas, subornos ou gratificações ilícitas. Os indivíduos intrinsecamente motivados têm mais interesse, entusiasmo e confiança em relação a indivíduos externamente controlados (DECI; RYAN, 2000). O potencial humano é encorajado em determinadas situações, e debilitado em outras. Indivíduos positivamente motivados (demonstrando disposição de colaborar, de ser útil ou construtivo) acreditam na conquista de objetivos através do esforço e da iniciativa individual. Indivíduos negativamente motivados (nocivos, prejudiciais, contrários ou contraproducentes) utilizam meios imorais ou ilegítimos para os devidos fins (SMITTON, 1993).

Uma intenção é a determinação (composta por interesses subjacentes) para agir de uma determinada maneira, enquanto que um desejo é um impulso consciente em direção a algo que promete prazer ou satisfação (WU; ZHIGANG; JUNHUA, 2009). Apenas um desejo não é suficiente. É preciso ter as capacidades, habilidades e ferramentas para atingir a meta, levando em consideração as oportunidades e custos inerentes (WU; ZHIGANG; JUNHUA, 2009). A ponderação entre capacidades, oportunidades e interesses subjacentes precede o desenvolvimento de uma intenção criminal.

Em determinadas circunstâncias, aspectos organizacionais estimulam a violação das regras estabelecidas. Frustração, estresse, raiva ou descontentamento, envolvendo elementos psicológicos, financeiros e sociais, motivam pessoas a tomar o caminho da criminalidade

cibernética, utilizando habilidades e conhecimentos em prejuízo de terceiros (ARPAD, 2013). É uma realidade, nas organizações, que indivíduos que detinham status de confiança tenham se envolvido com violações de segurança (DHILLON, 2001). Em virtude de fatores pessoais e profissionais, aproveitando oportunidades específicas, essas pessoas praticam o crime cibernético (BACKHOUSE; DHILLON, 1995).

2.3.1 Abordagens Teóricas da Motivação

A palavra motivo origina-se do latim “*moveres*” ou “*motum*”, que significa aquilo que faz mover (ECCHELI, 2008; STEERS; MOWDAY; SHAPIRO, 2004). “[...] motivar significa provocar movimento, atividade no indivíduo” (CAMPOS, 1987, p. 108). Motivação diz respeito à energia, direção, persistência e equifinalidade, direcionando o indivíduo a fazer alguma coisa (RYAN; DECI, 2000). Definições clássicas que analisam a natureza abstrata e subjetiva das motivações nos seres humanos estão apresentadas a seguir.

A motivação refere-se a um processo voluntário. Ela guia decisões sobre o engajamento em atividades particulares (ECCLES; WIGFIELD, 2002). É tudo aquilo que estimula um indivíduo a agir ou deixar de agir de determinada maneira, produzindo um comportamento específico, frente a determinadas circunstâncias e estímulos (GOULART, 2006). As condutas incentivadas pela energia motivadora têm uma meta ou finalidade. Os motivos compreendem causas determinantes de um comportamento não fortuito ou habitual.

A motivação não é uma variável ou atributo passível de observação e mensuração direta. Ela é um conceito abstrato, constituído de particularidades e fundamental para todos os aspectos da vida. O construto motivação pode ser entendido por determinantes ambientais, por forças internas (necessidades e desejos) e por incentivos que movimentam o organismo a executar uma determinada tarefa (LOMÔNACO; WITTER, 1984). Basicamente, existem dois componentes essenciais: o impulso e o motivo (MURRAY, 1964). O primeiro tem relação com um processo interno de incitação, e o segundo produz um comportamento que se extingue quando o objetivo é atingido, na medida em que a recompensa sacia a incitação inicial (MURRAY, 1964).

As teorias motivacionais têm raízes na Grécia Antiga (termo utilizado para denominar o mundo grego entre os anos 1.100 a.C. e 146 a.C.), quando filósofos propuseram as primeiras hipóteses sobre os conteúdos das motivações fundamentadas no hedonismo (STEERS; MOWDAY; SHAPIRO, 2004). Esta visão filosófica postulava a busca do ser humano pelo prazer e o distanciamento da dor (PETRI; GOVERN, 2012). As pessoas faziam escolhas que

aumentassem a satisfação ou reduzissem o sofrimento, visando recompensas e/ou evitando punições (PETRI; GOVERN, 2012).

No final do século XVIII, com a Revolução Industrial¹, uma nova concepção de trabalho modificou estruturas sociais e comerciais, rompendo com a ordem econômica até então vigente. A mecanização da indústria, da agricultura e o desenvolvimento fabril aceleraram os transportes e as comunicações, tornando fundamental o papel das organizações na sociedade (WOMACK; JONES, 2004). Estruturas organizacionais foram baseadas na ideia de ação, resultado, hierarquia, especialização e divisão do trabalho (WEBER; BARBOSA; BARBOSA, 1994). As deficiências deste modelo não tardaram a redirecionar o foco da teoria das organizações para o elemento humano, importando conceitos de outras ciências como a sociologia, a antropologia e a psicologia. A nova perspectiva passa a ser fundamentada em elementos complexos inerentes ao indivíduo, tais como crenças, valores, satisfação, realização, autodesenvolvimento, responsabilidade, comportamento e liderança (MORGAN; GREGORY; ROACH, 1997).

Muitas das teorias contemporâneas da motivação assumem que as pessoas iniciam e persistem em um comportamento na medida em que acreditam que esse comportamento irá conduzi-las a um objetivo desejado (DECI; RYAN, 2000). A partir da Grande Depressão de 1929 (também denominada Crise de 1929, considerada a maior recessão econômica mundial), a escola das relações humanas propôs uma nova abordagem teórica para o campo da Administração, reformulando a visão do ser humano. O estudo denominado “Experiência de Hawthorne”, desenvolvido em 1927, pelo Conselho Nacional de Pesquisas dos Estados Unidos (*National Research Council*), em uma fábrica da companhia *Western Electric Company*, situada em Chicago (EUA), no bairro de *Hawthorne*, trouxe constatações relevantes sobre o impacto de questões ambientais, sociais, organizacionais e afetivas inerentes aos funcionários (MAYO, 1945). O conceito de satisfação do trabalhador emerge. Partindo da Teoria Clássica da Administração (FAYOL, 1970), com ênfase na estrutura e eficiência organizacional, o foco muda do *Homo Economicus* (uma ficção que restringia as dimensões do homem, analisando suas ações econômicas exclusivamente a partir das funções elementares de consumo e produção) (PRESTES MOTTA, 1972) para uma perspectiva mais

¹ A Revolução Industrial mudou a forma como as coisas eram produzidas e a maneira como as pessoas viviam. Entre os anos de 1700 e 1800, a mecanização possibilitou a produção em massa de bens de consumo nas novas fábricas movimentadas à vapor (ASHTON, 1966). Foi um período de grandes transformações na economia da Europa e nos Estados Unidos, quando ocorreu a substituição do trabalho artesanal pelo assalariado e o avanço da indústria têxtil, mecânica e logística (TAYLOR, 1951).

complexa, denominada *Homo Social* (DECI; RYAN, 2000) fundamentada nas teorias das relações humanas e seus desdobramentos (MOTTA; VASCONCELOS, 2002).

A teoria da autodeterminação, ou *Self-Determination Theory* (SDT), estabelece basicamente dois tipos de motivação: autônoma e controlada (DECI; RYAN, 2008). O primeiro tipo compreende motivações intrínsecas e extrínsecas do ser humano, quando as pessoas correlacionam positivamente ações aos seus valores fundamentais. A motivação na forma autônoma oferece a experiência de volição (vontade, um processo cognitivo de querer pelo qual se decide praticar uma ação) e de autoaprovação das realizações. O segundo tipo possui regulação externa, mediante um esquema de recompensas ou punições. Trata-se de um controle internalizado e impulsionado por fatores sociais e individuais, como aprovação, vergonha, ego e autoestima. Existe um sentimento de pressão para pensar, sentir ou proceder de acordo com determinada orientação (DECI; RYAN, 2008). A SDT, em síntese, é uma teoria da motivação e da personalidade humana em contextos sociais, a qual diferencia a motivação entre o ser autônomo e o ser controlado (DECI; RYAN, 2011).

Historicamente, o tema motivação foi estudado com base em perspectivas que ajudaram a fundamentar as teorias modernas da motivação (BERNARD et al., 2005). A primeira delas é a biológica, que introduz o conceito de instinto como função da genética, conectada a estrutura cerebral e base para a motivação (JAMES, 1890). Partindo dessa premissa, os instintos inatos, definidos em função da genética, são causas das motivações, e ocorrem independentemente de processos racionais ou conscientes (BERNARD et al., 2005). Portanto, os genes desempenham papel causal na motivação. Estudos influenciados por essa corrente teórica tendem a ignorar agentes racionais ou conscientes como responsáveis pelas forças que movimentam as pessoas (BERNARD et al., 2005).

A segunda perspectiva é a comportamental, que declara os fatores externos como preponderantes para a motivação (THORNDIKE, 1911). O comportamento não é resultado exclusivo do instinto, mas também de consequências ambientais (BERNARD et al., 2005). Quando seguido de satisfação e recompensa, tende a se repetir, mas quando seguido de insatisfação e punição, tende a não se repetir (BERNARD et al., 2005). O ambiente possui papel causal na motivação. Os behavioristas (pesquisadores de uma área da psicologia, também denominada comportamentalismo) atribuem aos fatores externos a capacidade de influenciar no comportamento, inclusive aquele com origem nos instintos humanos. De acordo com a teoria comportamental, a motivação é um processo orientado a reflexos automáticos, que busca satisfazer requisitos moldados pelo ambiente externo (BERNARD et al., 2005). Os pesquisadores da corrente comportamentalista enfatizam a aprendizagem como

fator direcionador da motivação, postulando um determinismo do passado sobre o comportamento atual do indivíduo (AGUIAR, 1992). As ações do presente são consequência das experiências anteriores em uma abordagem, portanto, histórica. Nesta perspectiva, os estímulos externos (condicionamentos positivos e negativos oriundos do ambiente) compõem as forças diretivas.

A terceira perspectiva é a cognitiva, cujos pressupostos estão relacionados aos processos mentais como inteligência, racionalidade, consciência e tomada de decisão (BERNARD et al., 2005). Na perspectiva cognitiva, a motivação é causada por um processo mais racional e deliberativo em relação às perspectivas biológicas e comportamentais. Ela considera processos conscientes para o estudo da motivação, os quais influenciam o comportamento humano (BERNARD et al., 2005). Os cognitivistas consideram que os indivíduos são detentores de um conjunto de valores, opiniões e expectativas em relação ao mundo (AGUIAR, 1992). Esse conjunto de forças estimulam ações na direção de objetivos. As forças direcionadoras originam-se de estímulos internos, tais como elementos psicológicos relacionados à percepção e ao pensamento (AGUIAR, 1992).

O termo motivação possui uma variedade de definições no campo da psicologia. Ela se expressa como força, instinto, impulso ou desejo, figurando como causa determinante para ações ou reações das pessoas frente a determinadas configurações ambientais (TODOROV; MOREIRA, 2005). Ela tem sido questão central e perene nos estudos dos fenômenos psíquicos, das funções mentais e do comportamento humano, sendo núcleo de regulação biológica, cognitiva e social (RYAN; DECI, 2000). A motivação é relevante por causa das suas consequências, ou seja, aquilo que ela gera ou produz no ambiente social. Ao mesmo tempo, é fundamental para líderes, gerentes, professores, e treinadores no contexto organizacional e familiar (RYAN; DECI, 2000).

Em sintonia com estudos sobre a sexualidade (modelo psicosssexual), a libido é energia motivacional primária da vida humana (FREUD et al., 1970). *Freud* relaciona a motivação aos instintos, cujas forças internas direcionam, conscientemente ou não, a satisfação (PERVIN; JOHN, 2008). Esta visão explicita um determinismo biológico que a hereditariedade adquire perante o comportamento. Adicionalmente, *Freud* coloca de lado as questões puramente fisiológicas e neurológicas sobre o tema para valorizar um fator intrínseco da personalidade de cada indivíduo: suas emoções. Elas passam a ser estudadas como elementos capazes de impulsionar o ser humano, condicionando comportamentos específicos (BERGAMINI, 1990). Sintomas e comportamentos do presente poderiam estar conectados a acontecimentos vividos no passado, outrora registrados no inconsciente. A

infância adquire relevância nos desdobramentos lógicos dessas histórias de vida, e, por conseguinte, na determinação da personalidade e da conduta humana. A visão psicanalítica sobre comportamento humano estabelece o caráter inconsciente da motivação. Aquilo que realmente orienta o comportamento está oculto no interior das pessoas segundo o pai da psicanálise, e a sua comprovação empírica, através do experimento, torna-se inviável (BERGAMINI, 1990).

Abordagens sócio-cognitivistas sustentam duas orientações motivacionais não aditivas, porém interativas, que são a intrínseca e a extrínseca (MARTINELLI; BARTHOLOMEU, 2007). Segundo os autores, a motivação intrínseca estimula a busca por novidades, desafios, sem a necessidade de pressões externas ou prêmios pelo cumprimento de tarefas. A motivação extrínseca se apresenta como resposta a obtenção de recompensas materiais ou sociais, de reconhecimento, de obediência a ordens ou pressões externas. Ao mesmo tempo, evita punições ou insatisfações. Enquanto a primeira está associada a resultados positivos de caráter estável e duradouro, a segunda provoca níveis elevados de ansiedade e estresse nos indivíduos expostos a um ambiente de pressão e tensão (MASSARELLA; WINTERSTEIN, 2009).

Os seres humanos podem ser produtivos, engajados e construtivos. Contrariamente, podem ser passivos, alienados e indolentes (RYAN; DECI, 2000). O contexto social catalisa essas diferenças motivacionais, e fatores denominados como necessidades psicológicas inatas, fortalecem ou enfraquecem a motivação intrínseca, a autoregulação e o bem-estar dos indivíduos. Estes fatores compreendem competência, autonomia e afinidade (RYAN; DECI, 2000). Quando satisfeitos, produzem aumento da automotivação. Por outro lado, quando frustrados conduzem à redução da motivação e do bem-estar (RYAN; DECI, 2000).

O homem é um animal que deseja; tão logo uma de suas iminentes necessidades seja satisfeita, outra aparece no seu lugar em um processo cíclico sem fim (MCGREGOR, 1960). As pessoas fazem o que elas fazem para atender diversas necessidades psicológicas (PYSZCZYNSKI; GREENBERG; SOLOMON, 1997). Adicionalmente às demandas biológicas (como é o caso do instinto de autopreservação), o ser humano é motivado para atingir objetivos, tal como o reconhecimento de outros que pertençam ao seu grupo social, construção de uma imagem que seja favorável de si próprio, e uma visão próspera do mundo que lhe rodeia (PYSZCZYNSKI; GREENBERG; SOLOMON, 1997). Estes objetivos compõem as causas de uma variedade de comportamentos.

Maslow (1943) criou um modelo hierárquico para a motivação humano que é referenciado até hoje. As necessidades dos seres humanos foram organizadas em uma

pirâmide hierárquica. Este modelo teve enorme influência no campo das ciências comportamentais, pois desenvolveu uma proposta teórica de base multidisciplinar, a partir da preponderância de necessidades e suas respectivas motivações para a satisfação, com diferentes níveis de prioridade (SAMPAIO, 2009).

Na base dessa estrutura, estão as demandas fisiológicas, tais como respiração, água, alimento, sono, sexo, excreção e homeostase. Nos níveis seguintes encontram-se as necessidades por segurança (do corpo, emprego, recursos, bens, saúde) e de amor e relacionamento (amizade, família, intimidade sexual). Nos níveis mais altos estão necessidades de estima (autoestima, confiança, conquista, respeito) e de autorealização, a qual considera atingir o pleno potencial individual. Na medida em que um nível inferior é satisfeito, as demandas relativas dos níveis superiores ganham força e relevância no contexto das motivações humanas (MASLOW, 1943). As gratificações parciais de um nível da hierarquia não impedem a busca das demandas de outros níveis. A plena satisfação, se existir, é temporária. As pessoas estão sempre desejando novas metas (SAMPAIO, 2009).

2.3.2 Motivações para o Crime Cibernético

Crimes cibernéticos envolvem intenções antecedentes ao ato criminoso (RASMI; JANTAN, 2013). A motivação para praticar atos criminosos é definida como um desejo de se envolver em comportamentos indesejáveis e condenáveis relativos ao crime, sobrepondo eventuais condições restritivas (ANTONACCIO; BOTCHKOVAR; TITTLE, 2011).

As intenções são equivalentes a planos orientados para alcançar um objetivo específico (WU; ZHIGANG; JUNHUA, 2009). A análise das intenções de um ataque contribui decisivamente para a produção de provas que irão acelerar os processos de controle e punição dos autores (RASMI; JANTAN, 2013). A identificação de uma intenção intrusiva, seus caminhos e consequências são produzidos pela análise de ameaças, envolvendo a inferência de objetivos e a previsão de ações do potencial invasor (WU; SHUPING; JUNHUA, 2009).

O impulso para o crime advém de demandas pessoais, que se ativam na direção da prática ilegal e imoral, conforme a influência de visões, entendimentos, anseios, expectativas, ambições e experiências passadas. As pessoas são atraídas para o desvio, pois é gratificante (PRATT; CULLEN, 2000). Em sentido oposto, o autocontrole explica qual seria a probabilidade de engajamento nesse tipo de ato (PRATT; CULLEN, 2000). A decisão de realizar uma violação legal ou moral considera dois fatores importantes: a recompensa final e

o risco envolvido. Diferenças individuais na atitude frente ao risco influenciam a intenção de transgredir (PRATT; CULLEN, 2000).

As atividades criminosas, no espaço cibernético, originam-se em um comportamento humano desprovido de ética, e aqueles que praticam o crime virtual comportam-se de forma ilícita (VASHISTH; KUMAR, 2013). A parte mais complexa de um criminoso cibernético é a sua motivação (ARPAD, 2013). Os seguintes aspectos principais, em escala crescente de prioridades, propulsionam o crime cibernético (ARPAD, 2013).

- a) **Motivação Psicológica:** compreende a necessidade de provar a si mesmo, e, especialmente, para um círculo de amigos. O indivíduo deseja demonstrar ser alguém, não importa como. Em alguns casos, o desejo de vingança aflora após a rejeição do seu grupo social. Outro fator psicológico é a necessidade de adrenalina, a qual é experimentada nas ações ilegais, ainda que exista um sentimento de segurança física pelas características do ambiente virtual.
- b) **Motivação Financeira:** os estímulos para o crime cibernético por razões pecuniárias. As necessidades psicológicas são sobrepostas por demandas socioeconômicas (dinheiro e status social), quando se busca atender interesses além do prazer. Se bem-sucedidos, esses indivíduos podem integrar organizações criminosas com estrutura e objetivos próprios.
- c) **Reação Pública:** criminosos cibernéticos são beneficiados por um orgulho social, quando suas ações são convertidas em grandes façanhas. A sociedade tem culpa por não condenar firmemente os criminosos cibernéticos. Paradoxalmente, eleva esses indivíduos ao posto de heróis, glorificando suas realizações. Tal reação gera efeito indesejado, incentivando os crimes cibernéticos.

O crime cibernético é um grande negócio com diferentes motivações (EYGL, 2014a). O relatório da consultoria Ernest & Young (EY) de 2014 ressalta uma mudança importante no perfil das ameaças cibernéticas, discriminando quatro variações de perfil (EYGL, 2014a):

- a) Os *hack-ativistas* ou simpatizantes do *hack-ativismo* estão focados em prejudicar reputações, provocando incidentes ou produzindo declarações depreciativas sobre organizações com as quais não concordam. Utilizam as redes sociais para discutir operações e recrutar membros;

- b) O crime cibernético organizado (sindicato do crime) está orientado, primariamente, para o ganho financeiro, visando ativos organizacionais que possam ser negociados clandestinamente;
- c) A espionagem patrocinada por Estados ou nações, com vastos recursos à disposição busca obter vantagens competitivas através do roubo de informações privilegiadas;
- d) Invasões com finalidade política. Pessoas que desejam manipular decisões, influenciando, por exemplo, o relacionamento com parceiros de negócio.

Hipóteses sobre traços de personalidade e comportamento malicioso foram analisadas com objetivo de contribuir em taxonomias de perfis criminosos (ROGERS; SEIGFRIED; TIDKE, 2006). Foram analisadas e comparadas as amostras de indivíduos não criminosos com as amostras de indivíduos autodeclarados criminosos cibernéticos. As características “maior introversão”, “maior abertura a novas experiências”, “maior neurose”, “maior espírito explorador / manipulador”, e “piores escolhas morais” foram analisadas. Os resultados demonstram que apenas a característica “maior introversão” tinha relação com o comportamento criminal (ROGERS; SEIGFRIED; TIDKE, 2006). Conforme os autores, nenhuma das outras hipóteses foi suportada.

As motivações que levam pessoas a cometer crimes cibernéticos podem agrupar-se em categorias conforme suas características (ROGERS, MANUS, 2006). Estas categorias compreendem habilidades e motivações de acordo com o Quadro 2:

Quadro 2 – Habilidades e Motivações de Criminosos Cibernéticos

(Continua)

Tipo	Características	Motivações
[1] Novatos	Indivíduos sem muita experiência na computação e no desenvolvimento de sistemas.	Buscam emoções e satisfação do ego. Querem ser aceitos em grupos sociais, provando seu valor e competência. Desejam aceitação como membros de gangues urbanas.

(Conclusão)

Tipo	Características	Motivações
[2] Punks Cibernéticos	Possuem conhecimentos de computação e linguagens de programação. Envolvem-se em vandalismos virtuais, tais como desfiguração de <i>websites</i> , envio de <i>spam</i> , roubo de dados de cartão de crédito e fraudes nas telecomunicações (violação de privacidade e ligações gratuitas).	Desejam atenção da mídia para obter fama e notoriedade. Quando são capturados, almejam sucesso posterior prestando consultoria na área de segurança da informação.
[3] <i>Insiders</i> (trabalhadores internos)	Trata de uma categoria menos publicitada que representam alto risco. São funcionários descontentes ou ex-funcionários (alguns da área de TI) que violam as regras e a confiança que lhes foi atribuída, usando privilégios de acesso para realizar ataques contra a sua organização. Com frequência, o nível de habilidade é elevado.	A motivação mais citada é a vingança ou a revanche.
[4] Pequenos Ladrões	A pirataria é um dos métodos de promover atividades criminosas. Estas pessoas não estão interessadas em notoriedade pública. Ao contrário, a fama seria perigosa. Este grupo foi atraído à tecnologia e à Internet, pois os alvos potenciais migraram para o ciberespaço (bancos, operadoras de cartões de crédito, pessoas ingênuas). Exibem boas habilidades técnicas.	A necessidade de ganhos fáceis é a principal motivação. É típico desse grupo o desejo de enriquecer, a ganância e, em alguns casos, a vingança.
[5] <i>Hackers</i> da Velha Guarda	Eles não demonstram intenção criminosa, embora desrespeitem a propriedade pessoal e/ou intelectual. São amantes da ideologia dos primeiros hackers, orientados para uma diferenciação intelectual. Este grupo tem habilidades técnicas profundas e, muitas vezes, escrevem os códigos que são usados por criminosos menos qualificados.	As principais motivações para este grupo são a curiosidade e a necessidade de desafio intelectual.
[6] Criminosos Profissionais	São profissionais que orientam suas capacidades e habilidades em prol do crime. Tem alto grau de perspicácia técnica e preparo psicológico. Integram organizações criminosas. São especializados em espionagem corporativa, são bem treinados, e tem acesso ao estado-da-arte da tecnologia.	Motivam-se por dinheiro e ganhos financeiros. Não estão interessados na fama ou publicidade. Buscam uma espécie distorcida de orgulho profissional.
[7] Guerreiros da Informação	Pessoas especializadas em defesa ou ataques para a perturbação e desestabilização social de comunidades ou países, focando organismos ou instituições de controle e tomada de decisão. O grupo envolve-se em guerras cibernéticas patrocinadas por Estados ou nações. São altamente treinados e qualificados, possuindo acesso ao estado-da-arte da tecnologia.	Essas pessoas normalmente são motivadas pelo espírito de patriotismo.

Fonte: adaptado de Rogers e Manus (2006)

As técnicas de neutralização apresentadas no Quadro 3 são normalmente utilizadas para justificar um comportamento desviante (GOODE; CRUISE, 2006). Elas fazem parte de

um framework proposto pela Teoria da Neutralização (SYKES; MATZA, 1957) a qual reúne os conceitos de justificativa e motivação para a prática criminal. A neutralização é um fator relevante para avaliar violações no local de trabalho, podendo prever a intenção criminal (SIPONEN; VANCE, 2010). Na perspectiva dos *insiders*, ela afeta a predisposição para cometer violações contra as políticas da segurança. Em organizações cujo o sistema de punição é informal ou flexível, justificativas neutralizadoras das infrações são comuns (SIPONEN; VANCE, 2010). Em síntese, autores de crimes, quando identificados ou capturados, costumam utilizar essas técnicas de neutralização para justificar e minimizar seus atos, ocultando a principal motivação, e esperando evitar possíveis sanções ou consequências (HEATH, 2008; SIPONEN; VANCE, 2010).

Quadro 3 – Técnicas de Neutralização do Comportamento Desviante

(Continua)

Nome da Técnica	Descrição
<p>Negação de Responsabilidade (<i>Denial of Responsibility</i>)</p>	<p>O criminoso nega responsabilidade e alega que suas ações foram involuntárias, acidentais, ou que estava bêbado ou fora de si. Diz-se incapaz de pensar claramente sobre seus atos, ou não tinha escolha, sendo obrigado a cometê-los. No contexto corporativo, uma ação raramente inicia e finaliza a partir de um único indivíduo. Quando um crime é cometido, todos podem, com algum grau de plausibilidade, apontar o dedo para alguém que possui parte da responsabilidade.</p>
<p>Negação de Dano (<i>Denial of Injury</i>)</p>	<p>O criminoso minimiza ou nega os danos causados, afirmando, por exemplo, que o roubo tinha apenas a intenção de assustar, que o produto do furto seria devolvido (pego emprestado) ou que a vítima consentia com o ato. Em geral, as pessoas têm atitudes mais permissivas em relação ao crime quando a vítima é uma instituição ou um indivíduo desconhecido. É também comum afirmar que nenhum dano ocorreu.</p>
<p>Negação de Vítima (<i>Denial of Victim</i>)</p>	<p>O criminoso reconhece o dano, mas alega que a vítima não merece preocupação, pois merecia as consequências. O crime é retratado como retaliação por alguma ofensa prévia, ou como ato preventivo. Em sua forma mais simples, o argumento restringe-se a “ele ou ela começou”. De maneira mais sofisticada, apresenta o agressor como um justiceiro, que busca impedir a impunidade dos crimes alheios.</p>
<p>Condenação dos Condenadores (<i>Condemnation of the Condemners</i>)</p>	<p>O criminoso invalida os motivos daqueles que o condenam. Seria moralmente inaceitável punir alguém por um delito quando nem todos são punidos da mesma forma. Crimes corporativos seriam reavaliados considerando a premissa de que as regras definidas pelo governo não têm legitimidade e atendem a interesses políticos ou econômicos.</p>

(Conclusão)

Nome da Técnica	Descrição
<p>Apelo a Lealdades Superiores (<i>Appeal to higher loyalties</i>)</p>	<p>O criminoso nega que o ato tenha sido motivado em interesse próprio. Alega que fez em obediência a uma orientação moral externa, de caráter particularista, como a lealdade aos amigos, à família ou aos colegas de turma, grupo ou gangue. No contexto organizacional, empregados podem sentir-se isentos de uma acusação quando suas ações foram realizadas para o bem da empresa. A justificativa de má conduta dos gestores pode estar apoiada, por exemplo, no atendimento dos interesses das partes interessadas ou intervenientes (<i>stakeholders</i>).</p>
<p>Todos Estão Fazendo / Costume (<i>Everyone else is doing it</i>)</p>	<p>O criminoso justifica seus atos pelo fato de que a maioria das pessoas também viola a lei. Seu comportamento estaria alinhado com o comportamento da maioria, e a sociedade não poderia esperar o cumprimento de algo que os outros também violam. A lei não atenderia as expectativas sociais e, portanto, sua aplicação é ilegítima. Em um mercado competitivo, os indivíduos são pressionados a atingir metas arrojadas. Ações que violam direta ou indiretamente a lei podem trazer diferenciais competitivos, e a justificativa de que “todos fazem” é utilizada para minimizar a falta de ética e conformidade.</p>

Fonte: adaptado de Sykes e Matza (1957), Heath (2008) e Siponen e Vance (2010)

Os Quadros 2 e 3 compilam um conjunto de fatores relacionados a ética e a motivação para o crime. Esses elementos ajudam a explicar de que maneira indivíduos neutralizam controles sociais, os quais, de outra forma, atuariam como inibidores da motivação criminal. A neutralização, neste contexto, faz parte do extrato teórico relativo a motivação dos indivíduos para o crime cibernético.

2.4 SENTIMENTOS HUMANOS

Existem três abordagens gerais sobre o estudo dos sentimentos humanos (SCHWARZ; CLORE, 1996): experimental, cognitiva e somática. A primeira enfatiza a qualidade experimental dos sentimentos e fornece informação a respeito. A segunda abordagem enfatiza os pensamentos que acompanham os sentimentos e, por fim, a última foca nos componentes relativos ao próprio organismo, considerando seus respectivos estados afetivos.

Os sentimentos surgem mediante estímulos ao sistema sensorial humano, produzindo sensações ou percepções (FEELINGS, 1998). Atividades neurais paralelas ocorrem, como o processamento de informações, o armazenamento de dados na memória e efeitos periféricos no organismo humano. Alterações neurais e hormonais decorrentes produzem condições psicológicas nos indivíduos que são referenciadas como emoções (FEELINGS, 1998). Conforme este autor, sentimentos podem produzir efeitos observáveis: a felicidade pode

produzir o riso; todavia, o riso não explica a felicidade. O Quadro 4 resume algumas características dos sentimentos.

Quadro 4 – Sentimentos Humanos

1	O sentimento é um constructo cerebral intrínseco ao indivíduo.
2	O sentimento é reconhecido pelo indivíduo quando ele ocorre.
3	Sentimentos podem mudar o comportamento imediatamente ou eventualmente; contudo, não necessariamente.
4	Sentimentos frequentemente atuam como reforços no aprendizado.
5	Sentimentos podem ser positivos ou negativos, promovendo a aproximação ou a rejeição.
6	Exemplos: dor, mal-estar, cansaço, fome, sede, desconforto termal, medo, ansiedade, aflição, frustração, culpa, depressão, tédio, solidão, sofrimento, luxúria, ciúmes, raiva, prazer sexual, prazer alimentar, animação, prazer da conquista, felicidade.

Fonte: adaptado de Feelings (1998)

Sentimentos parecem ter surgido para retratar situações fisiológicas, facilitando a aprendizagem das condições de desequilíbrio, antecipando futuros estados favoráveis ou adversos (DAMASIO; CARVALHO, 2013). Desta forma, os sentimentos proporcionaram um nível adicional de regulação do comportamento. Estudos posteriores sobre o reconhecimento das emoções demonstraram que, ao contrário da tese que considera uma determinada emoção inata e universal, existem diferenças importantes nas emoções presentes nas variadas culturas humanas (WIERZBICKA, 1986). Sistemas de nomenclatura refletem maneiras diferentes de conceituar as emoções. A linguagem necessita administrar essas discrepâncias para que seja possível transmitir a correta percepção de um sentimento (WIERZBICKA, 1986).

2.4.1 A Natureza dos Sentimentos

A temática dos sentimentos humanos é pesquisada com profundidade na Psicologia e na Psiquiatria, e com razoável atenção no campo da Sociologia e Antropologia. “Sentimentos enquanto forças que movem o homem a se relacionar consigo e com os outros” (TOGNETTA, 2005). A presença desse constructo também é observada nas investigações sobre a qualidade de vida das pessoas no contexto profissional (escolas e organizações) e

pessoal (indivíduo, família, amigos, sociedade), frequentemente desenvolvidas no escopo da Enfermagem e demais Ciências da Saúde (PASCHOA; ZANEI; WHITAKER, 2007).

No âmbito do interesse desta pesquisa, a literatura prévia considerada trata dos sentimentos humanos sob a perspectiva da Psicologia orientada para o campo da gestão das organizações. Partindo dessa abordagem teórica, os sentimentos humanos são reflexos de uma representação mental da realidade, e não uma cópia da realidade tal como ela pretensamente seria de fato (AGUIAR, 1992). Os seres humanos selecionam aspectos dessa realidade quando constroem a respectiva representação mental, e a partir desses aspectos criam uma imagem particular e subjetiva da realidade. Esse processo seletivo é determinante na formação de diferentes sentimentos, os quais exercerão influência na organização mental das percepções, crenças e entendimentos sobre o mundo.

Todo esse processo de interpretação da realidade produz significados e emoções para o indivíduo, e é resultado de quatro capacidades humanas essenciais: a percepção, a memorização, a racionalização e a abstração (AGUIAR, 1992). As pessoas discriminam estados corporais decorrentes da interação com eventos ambientais e os nomeiam conforme a descrição conceitual de determinados tipos de sentimento aprendidos na sua formação familiar e social (GUILHARDI, 2002). Conforme este autor, o efeito de um sentimento é o comportamento. Ambos são causados por histórias genéticas e ambientais, juntamente com as circunstâncias que originaram o respectivo estado corporal (GUILHARDI, 2002). O ambiente está definido aqui como eventos do universo capazes de afetar o organismo (TOURINHO; TEIXEIRA; MACIEL, 2000).

Os sentimentos são sensações corporais, próprias da espécie humana (WIERZBICKA, 1986). São derivados das contingências e a sua denominação é determinada pela aprendizagem, cuja origem é social (SKINNER, 1974). *Skinner* declara: “O sentimento parece ser tanto a coisa sentida quanto o ato de senti-la”. Ambos têm diferentes perspectivas. O primeiro, pode referir à sensação do tato. O segundo estabelece uma relação com o ambiente, o qual é percebido mediante a capacidade do indivíduo em responder ao mundo circundante conforme sua percepção e disposição analítica (TOURINHO; TEIXEIRA; MACIEL, 2000).

Ao discriminar os próprios sentimentos, pode-se inferir o sentimento de outra pessoa diante de determinada situação (GARCIA-SERPA; MEYER; DEL PRETTE, 2003). O papel desses estados subjetivos foi tema predominante nas pesquisas de *Skinner*. O autor estabelece que o sentimento é uma ação sensorial, como ver e ouvir, e que, ao discriminar, falar e compartilhar aquilo que é sentido, descreve-se comportamentos que foram ensinados previamente no contexto familiar e social (CARVALHO, 1999).

Como nos sentimos – ou, mais precisamente, como nossos corpos nos parecem – é um aspecto saliente da situação na qual estamos engajados... e desde que frequentemente acreditamos que quando os outros agem como nós, eles também se sentem como nós, não é surpreendente que quando nós queremos que ajam de determinada maneira, nós tentemos fazê-los sentirem-se como nós nos sentimos quando fazemos tal coisa (SKINNER, 1978).

O comportamento pode ser consequência daquilo que é sentido, e o sentimento, por outro lado, ocorre em virtude de um acontecimento (SKINNER, 1995). “Não choramos porque estamos tristes, ou sentimos tristeza porque choramos; choramos e sentimos tristeza porque alguma coisa aconteceu” (SKINNER, 1995). O autor estabelece que é relativamente fácil confundir o sentimento como uma causa de um comportamento, pois o ser humano sente enquanto comporta-se, ou até mesmo antes do respectivo comportamento. Os eventos responsáveis pelo sentimento, portanto, estão no passado.

2.4.2 Sentimentos Negativos

Sentimentos ruins desdobram-se de um estado emocional negativo prévio, frequentemente oriundo de experiências malévolas anteriores (ameaças, brigas, abusos, rejeições), as quais tornam o indivíduo propenso a intenções hostis (DODGE, 1985). Portanto, ao sentir-se ameaçado, o indivíduo desenvolve um conjunto de emoções ruins que estimulam diferentes níveis de agressividade.

As emoções ruins são reações de eventos específicos, e indicam o grau de importância que o respectivo evento adquire para o indivíduo (SCHWARZ; CLORE, 1996). A reação é uma consequência de uma avaliação do evento conforme objetivos pessoais relacionados ao bem-estar. Aversão, raiva ou medo são exemplos de uma reação a circunstâncias que refletem danos, perdas ou ameaças.

Emoções negativas, especialmente aquelas vinculadas ao local de trabalho, incluem oposição às decisões gerenciais, ao comportamento de colegas e à carga de trabalho, considerando níveis cobrados de eficiência versus as políticas e normas da empresa (BASCH; FISHER, 1998). As condições de trabalho, as práticas organizacionais, o salário, o tipo de supervisão, o status e a segurança no trabalho foram as variáveis mais relevantes sobre sentimentos excepcionalmente ruins no contexto das organizações (HERZBERG; MAUSNER; SNYDERMAN, 1959).

Galinha e Ribeiro (2005) realizaram um levantamento de conceitos relacionados ao tema na literatura prévia, trabalhando em uma tradução que foi validada por psicólogos

portugueses com domínio na língua inglesa, objetivando confirmar a validade dos conteúdos traduzidos. No Quadro 5, foram discriminados alguns desses conceitos que fazem conexão com escopo desta pesquisa:

Quadro 5 – Tempos das Entrevistas

Sentimento	Conceito
Cansado	Sonolento, Indolente, Preguiçoso
Desanimado	Desencorajado, Triste, Melancólico, Deprimido
Perturbado	Transtornado, Angustiado, Atormentado, Preocupado
Zangado	Agressivo, Hostil, Antipático, Irritado
Desrespeitoso	Desdenhoso, Desprezível, Sarcástico
Repugnado	Repulsa, Enojado
Amedrontado	Assustado, Medo
Culpado	Humilhado, Arrependido
Nervoso	Trêmulo, Agitado
Rejeitado	Solitário, Isolado
Tímido	Envergonhado, Inibido, Acanhado

Fonte: adaptado de Galinha e Ribeiro (2005)

Os conceitos apresentados no Quadro 5 não cobrem a totalidade de sentimentos ruins. Servem como referencial dessas emoções, ao mesmo tempo que demonstram a complexa e talvez inconclusiva tarefa de relacionar todos esses sentimentos relativos ao ser humano, considerando incontornáveis variações culturais e geográficas.

2.5 JUSTIÇA ORGANIZACIONAL

As profundas mudanças sócio-organizacionais que ocorreram em nossa sociedade contemporânea (competitividade, globalização, incerteza, cenários de crise, indicadores econômicos e redução do emprego) contribuíram para a ampliação de conflitos sociais que foram estimulados pela vivência de situações de injustiça e sofrimento nas relações de trabalho, e ampliados por um comportamento negativo e retaliatório das pessoas no contexto das organizações (MENDONÇA; MENDES, 2005). “Quanto maior é a percepção de injustiça, maior é a prevalência da retaliação organizacional” (MENDONÇA; TAMAYO, 2008, p. 192). A retaliação, igualmente denominada represália, desforra ou desagravo, objetiva, de maneira explícita ou sutil, provocar dano igual ou maior àquele recebido, e está relacionada com a lei ou pena de talião (revanche), que consiste na rigorosa reciprocidade do ato criminoso (ROBINSON; BENNETT, 1995). Os ditados populares “olho por olho, dente

por dente” ou “aqui se faz aqui se paga” ilustram a proposta conceitual da retaliação, cujas raízes permeiam os valores individuais do ser humano, promovendo seus interesses pessoais e favorecendo uma almejada superioridade social ao término de um conflito (MENDONÇA; MENDES, 2005). No local de trabalho, percebe-se que a retaliação pode ser considerada uma estratégia do *insider* diante das situações de injustiça que, uma vez assim percebidas, geram sofrimento e sentimentos negativos complementares.

No Brasil, estudos conclusivos sobre as retaliações perpetradas no local de trabalho são inexistentes, mesmo suspeitando-se que esse tipo de comportamento possa estar na origem de significativos prejuízos organizacionais (MENDONÇA; TAMAYO, 2008). A retaliação pode ser um desdobramento de relações problemáticas e imprevisíveis em nível interpessoal e organizacional, merecendo atenção e esforços de pesquisa sobre suas causas e consequências. Gerenciar adequadamente o comportamento das pessoas está na base da eficácia organizacional. As peculiaridades próprias da complexa natureza humana tornam essa gestão um enorme desafio. Estima-se, por exemplo, que um a dois terços dos trabalhadores norte americanos envolvam-se em roubos, fraudes, desvios de dinheiro, vandalismos, sabotagens, absenteísmos e agressões, impondo prejuízos de dezenas de bilhões de dólares anuais à economia (MENDONÇA; TAMAYO, 2008). Somando-se o fato de que as organizações estão cada vez mais presentes no ciberespaço, riscos relacionados ao crime cibernético motivado pela retaliação e outras formas de descontentamento não aparentam estar sob efetivo controle gerencial.

A qualidade de vida das pessoas no local de trabalho está relacionada com as características da estrutura física da organização, com a natureza das atividades realizadas, com as relações interpessoais desenvolvidas e com percepção dos funcionários sobre a dinâmica sistêmica da organização (MENDONÇA, 2009). Decisões tomadas em relação a distribuição de recursos ou recompensas, bem como aquelas que impactam direta ou indiretamente nas relações humanas dentro do contexto organizacional influenciam vivências de prazer ou sofrimento psíquico e, conseqüentemente, a própria qualidade de vida na empresa (MENDONÇA, 2009). Esse sofrimento está definido como um conjunto de experiências dolorosas (angústia, medo, insegurança) vividas com frequência por um ou mais indivíduos em um cenário de conflito entre as necessidades de gratificação e as respectivas restrições impostas pelas situações de trabalho (MENDONÇA; MENDES, 2005).

Experiências negativas no local trabalho conduzem o indivíduo a diversos níveis de sofrimento psíquico. Avaliações de desempenho ruins, perda ou redução na participação de resultados financeiros da empresa, salário baixo ou desatualizado, assédio e hostilidades nas

relações interpessoais com chefes e colegas, escassez de reconhecimento e gratidão, descumprimento de promessas e quebra de relações de confiança correspondem a situações desfavoráveis que produzem sentimentos de raiva, descontentamento e indignação (MENDONÇA; MENDES, 2005). Um indivíduo insatisfeito ou indignado com a sua empresa, chefe ou colegas de trabalho pode adquirir motivação para cometer um crime nem sempre relacionado a obtenção de vantagens financeiras. O comportamento humano pode ser orientado por múltiplas motivações, intrínsecas ou extrínsecas (LINDENBERG, 2001). Vingança, revanche ou baixa-estima podem ser causas determinantes dessa motivação.

Nos Estados Unidos, o Instituto Americano de Contadores Públicos Certificados (AICPA), emissor das Declarações sobre Normas de Auditoria (SAS), aprova um modelo de referência para a detecção do risco o qual estabelece três condições para a ocorrência de fraudes nas empresas: 1) a oportunidade para cometer fraudes, 2) a racionalização (análise do ato de fraude em relação ao código de ética do fraudador), e 3) o incentivo (sentimentos ou percepções de inadequação e injustiça em relação ao empregador servem como estímulos para a fraude) (AICPA, 2002). Esse modelo é denominado com o triângulo da fraude (HOLTON, 2009). Oportunidades e incentivos ocorrem a partir de elementos (tangíveis ou não) que se tornam disponíveis no contexto (espacial e temporal) de um determinado local de trabalho. Uma vez disponíveis, ficam perceptíveis e conduzem a entendimentos e interpretações pessoais e heterogêneas. Tais elementos exercem influência na racionalização do indivíduo e nas suas conseqüentes intenções.

Na literatura, a questão da oportunidade costuma ser foco nas investigações sobre as fraudes em âmbito organizacional; porém, a insatisfação de funcionários tem aparecido com um relevante preditor desse tipo de crime (WELLS, 2001). O indivíduo percebe elementos em seu contexto de trabalho que produzem, nele, desconforto ou insatisfação. O comportamento desviante adquire relações com as respectivas condições de trabalho dentro da organização: quanto mais insatisfeito estiver esse indivíduo, mais provável que ele cometa um desvio (HOLTON, 2009). Os incentivos oriundos do contexto e o processo de racionalização das pessoas tornam-se fatores chave para o triângulo da fraude. O descontentamento no local de trabalho adquire, assim, relevância para motivação criminal.

O universo social inerente às organizações bem como suas características contextuais têm grande potencial para fornecer importantes esclarecimentos relacionados à psicologia social da justiça e seus desdobramentos. Em diversos cenários organizacionais, busca-se compreender, em estudos de campo, as percepções e reações dos *insiders* sobre justiça e injustiça (ASSMAR; FERREIRA; SOUTO, 2005). Para analisar esse sentimento negativo

adquirido por determinados *insiders*, a linha de pesquisa que estuda a questão da equidade ou justiça (*fairness*) é utilizada como principal referencial teórico. Neste sentido, quatro conceitos relacionados à percepção de equidade entre os *insiders* são agrupados sob a designação de Justiça Organizacional (ASSMAR; FERREIRA; SOUTO, 2005; WILLISON; WARKENTIN, 2009), termo cunhado originalmente por *Jerald Greenberg*, cujo modelo foi empiricamente validado por outros pesquisadores (SILVA; ALMEIDA; CARVALHO, 2008): 1) justiça distributiva, 2) justiça procedimental, 3) justiça interpessoal e, finalmente, 4) justiça informacional. As duas últimas aparecem na literatura agrupadas, ocasionalmente, em uma dimensão única denominada justiça interacional.

A compreensão desses conceitos, no contexto das práticas criminais, pode contribuir para a mitigação de variadas condições negativas que possam emergir nos trabalhadores de uma empresa: sentimentos de indignação, descontentamento, insatisfação, revanche ou desconforto, bem como suas consequências negativas para os indivíduos e a organização. Percebe-se que o cenário social é, assim, delineado pelo ambiente laboral. Os itens subsequentes analisam com maior profundidade cada um desses conceitos, suas características e relacionamentos com a motivação para o crime.

2.5.1 O Conceito de Justiça

O conceito de justiça, especialmente na civilização ocidental, foi sendo desenvolvido desde o período pré-socrático (Pitágoras e Sofistas), passando pela discussão ética-moral de Sócrates, e consolidando-se na proposta teórica de Aristóteles.

Aristóteles coloca a justiça como centro sintetizador ou aglutinador de todas as virtudes morais. A justiça estabelece a relação interpessoal e leva o indivíduo a conviver e se comunicar com o semelhante. Ninguém é ético em-si-mesmo; somos éticos em relação aos outros, enquanto nos relacionamos com as múltiplas alteridades. A justiça é a virtude que relaciona o indivíduo com os outros. A justiça insere o indivíduo na comunidade; ninguém é justo somente para si mesmo, mas em relação aos outros; a justiça é, então, a virtude da cidadania que orienta e regula toda a convivência política, estabelecendo, assim, uma ética social (SILVEIRA, 2001, p. 9).

O pensamento aristotélico criou um tratado sobre justiça, definindo-a e dividindo-a em espécies. Dentre eles, o filósofo grego escreveu sobre justiça distributiva, cujo cerne estava na distribuição de dignidades e vantagens conforme o mérito (SILVA, 2010). Nos tempos modernos, esse conceito confunde-se com “justiça social” ou “justiça econômica”, elementos

inerentes ao Estado de Direito, relacionados ao papel governamental para a redução das desigualdades sociais a partir do fundamento das necessidades individuais.

Justiça é um fenômeno presente na vida social e organizacional dos indivíduos, oferecendo percepções e produzindo sentimentos sobre a tomada de decisão, suas consequências e influências (JESUS; ROWE, 2014). A essência da justiça é a igualdade (tratamento) e a universalidade (normas), levando em consideração o caso concreto do indivíduo e a sua singularidade, os quais, conjuntamente, se denominam equidade (RADBRUCH; MONCADA, 1961). Trata-se de uma busca permanente ou infinita, conforme esses autores, em virtude da sua natureza contraditória, na medida em que a justiça, mesmo aspirando ao indivíduo, sempre se vale de normais gerais, direcionadas para a sociedade como um todo. Adicionalmente, a igualdade é uma abstração da desigualdade; os homens são diferentes, apresentando características e antecedentes que desafiam o estabelecimento de sentenças por um sistema jurídico, considerando os fundamentos da igualdade de tratamento, da universalidade das normas e da respectiva finalidade ética.

2.5.2 Justiça Distributiva

O conceito de distribuição, por sua vez, corresponde a um evento unilateral de alocação (destinação, designação ou divisão de elementos). É realizado por terceiros (uma pessoa ou grupo que está além dos indivíduos envolvidos numa situação) em uma variedade de contextos sociais, com impacto direto na vida das pessoas (KAZEMI; TÖRNBLOM, 2014). Diferencia-se de uma relação de troca, uma vez que esta última é um processo bilateral (KAZEMI; TÖRNBLOM, 2014).

Estudos sobre a teoria da equidade analisam quão equitativamente os distribuidores alocam recursos aos beneficiários. Os resultados destes trabalhos sugerem que, da mesma forma que as pessoas querem resultados equitativos para si mesmos, demandam que os outros, de forma equivalente, recebem recompensas e punições conforme suas contribuições ou infrações (KAZEMI; TÖRNBLOM, 2014). O processo de distribuição deve apresentar equidade, igualdade ou equivalência; do contrário, é injusto.

O princípio da contribuição estabelece que cada um deve receber de acordo com a sua contribuição. O uso desse princípio requer que as contribuições feitas pelos participantes individuais possam ser acessadas. O princípio da igualdade parte do pressuposto de que todos devem receber o mesmo, sem necessidade de qualquer pré-requisito para a aplicação do princípio. O princípio da necessidade estabelece que cada um deve receber de acordo com a sua necessidade. A aplicação do princípio requer que haja informações sobre o caráter e a intensidade das necessidades

individuais. Nota-se que os princípios da contribuição e da necessidade são baseados nos pressupostos da equidade, pois tratam da proporcionalidade em relação à contribuição ou à necessidade das pessoas (MENDONÇA; MENDES, 2005, p. 490).

No universo organizacional, indivíduos comparam suas contribuições com suas recompensas em relação aos colegas; e nessa comparação existem expectativas (denominadas expectativa normativas) que são adquiridas no processo de socialização (casa, escola, trabalho) (ADAMS, 1965). Expectativas intrinsecamente pessoais e de caráter privado; porém, susceptíveis às influências do senso comum e do contexto corrente. O indivíduo adquire um entendimento e avalia constantemente a sua condição de equidade, igualdade ou equivalência em relação a outros indivíduos dentro do seu grupo social (ADAMS, 1965). Independentemente se exista a formalização prévia de como ocorre o tratamento igual aos iguais e o tratamento desigual aos desiguais; tampouco sobre o que é considerado igual ou desigual (ADAMS, 1965).

A percepção da justiça organizacional transcorre durante a distribuição de resultados, bens ou benefícios concretos ou abstratos, através da qual os trabalhadores determinam se receberam adequado e justo tratamento (JESUS; ROWE, 2014). Tal percepção deriva de uma análise subjetiva e continuada de experiências em relação aos sistemas interacionais em que os indivíduos estão inseridos, assim como a posição social ocupada nas estruturas de poder vigentes. Os sistemas individuais e coletivos de crenças, valores, representações, avaliações e normas sociais são considerados nesta análise (JESUS; ROWE, 2014). Os sentimentos desenvolvidos nesse processo impactam as variáveis relacionadas ao conjunto de atitudes e comportamentos desses trabalhadores (JESUS; ROWE, 2014).

As pessoas reagem quando submetidas a situações de injustiça no ambiente de trabalho (HOMANS, 1961, p. 75): “Um homem em uma relação de troca com outro esperará que as recompensas líquidas ou lucro de cada homem sejam proporcionais aos seus investimentos”. Um típico exemplo dessa comparação, sob a ótica do princípio do mérito, ocorre entre dois trabalhadores que analisam qualitativa e quantitativamente suas responsabilidades versus o pagamento recebido pelo respectivo trabalho. Se o resultado desta comparação for o equilíbrio, haverá o sentimento de satisfação; caso contrário, haverá o sentimento de raiva por parte daquele que está em posição de inferioridade (ADAMS, 1965). O resultado desse sentimento negativo são estímulos que motivam o indivíduo a agir, em seu contexto social, para que ocorra uma mudança de percepção ou opinião do valor das conquistas alheias (desvalorização das contribuições dos outros) (ADAMS, 1965). É possível que esse indivíduo, de forma paralela ou complementar, reduza sua contribuição (dedicação,

produtividade, comprometimento, empenho) conforme o nível da sua percepção de injustiça e a respectiva desmotivação por agregar valor a uma organização que lhe produz insatisfação e desconforto.

2.5.3 Justiça Procedimental

O conceito de justiça evoluiu na literatura a partir do contexto jurídico (COLQUITT, 2001). Ao longo do tempo, as noções de justiça distributiva tornam-se incapazes de contemplar o fenômeno da justiça integralmente, surgindo, portanto, conceitos complementares.

Participantes de uma disputa litigiosa não reagem apenas em relação aos resultados (foco da justiça distributiva), mas igualmente reagem em relação aos procedimentos adotados para atingir os respectivos resultados (WILLISON; WARKENTIN, 2009). A sequência de ações encaminhadas e a conduta utilizada para atingir um estágio final também eram relevantes para a construção de uma percepção de justo ou injusto. Daí nasce o conceito de justiça processual, cujo foco é a equidade de procedimentos adotados pelos atores sociais para determinar os resultados de um processo (WILLISON; WARKENTIN, 2009).

A justiça procedimental estabelece procedimentos para regular as trocas e minimizar conflitos em um grupo social, assumindo que procedimentos considerados justos facilitam que o indivíduo assuma e aceite responsabilidades (MENDONÇA; MENDES, 2005). A teoria da justiça procedimental analisa os julgamentos sobre o processo ou o meio através do qual as decisões de alocação de recursos, bens ou benefícios são realizadas (SIMONS; ROBERSON, 2003). Ela estabelece que a equidade das políticas e práticas durante o processo de tomada de decisão têm grande relevância para as pessoas envolvidas (SIMONS; ROBERSON, 2003). Ao perceberem que os processos são justos, os trabalhadores tendem a demonstrar mais lealdade e disposição para agir em conformidade com os interesses e objetivos da organização (JESUS; ROWE, 2014). Consequentemente, estarão menos propensos a trair a instituição e seus líderes (JESUS; ROWE, 2014). O reconhecimento intelectual e emocional de justiça em relação aos procedimentos adotados em uma empresa motiva seus trabalhadores a cooperar com a estratégia organizacional (CROPANZANA; BOWEN; GILLILAND, 2007).

Neste sentido, foram propostos seis critérios para que processos ou procedimentos sejam considerados justos (COHEN-CHARASH; SPECTOR, 2001; JESUS; ROWE, 2014): 1) a regra da consistência determina que os procedimentos devam ser coerentes independentemente do tempo e das pessoas; 2) a regra da eliminação do viés determina que os

interesses pessoais do tomador de decisão devam ser suprimidos na elaboração de procedimentos; 3) a regra de precisão refere-se à acuracidade das informações relativas à elaboração dos procedimentos; 4) a regra da correção lida com a possibilidade de alterar indevidamente uma decisão; 5) a regra da representatividade estabelece que as necessidades, os valores e as perspectivas de todos os indivíduos devam estar, de alguma forma, representadas no processo; 6) a regra da ética define que o processo deva ser compatível com os valores morais e éticos estabelecidos.

2.5.4 Justiça Interpessoal e Informacional

Os aspectos sociais envolvidos na qualidade das relações entre as pessoas que tomam decisões e as pessoas que sofrem os efeitos dessas decisões fazem referência à justiça interpessoal, a qual emerge como uma dimensão independente do conceito geral de justiça (ASSMAR; FERREIRA; SOUTO, 2005). É vista, na literatura, como uma extensão de justiça procedimental, referindo-se ao fator humano presente nos relacionamentos e práticas organizacionais. Adicionalmente, analisa de que maneira a gestão de uma organização lida com as questões de justiça nos processos de comunicação e a subjacente qualidade de tratamento interpessoal durante a interação de atores sociais (COHEN-CHARASH; SPECTOR, 2001). A justiça interpessoal considera a cortesia, a honestidade e o respeito como valores fundamentais desse processo interativo e essencialmente humano (COHEN-CHARASH; SPECTOR, 2001).

A qualidade do tratamento interpessoal no âmbito social apresenta aspectos que determinam sentimentos de justiça ou injustiça, a partir da capacidade de julgamento dos indivíduos sobre a maneira que a comunicação e os procedimentos relacionados a tomada de decisão são encaminhados (ASSMAR; FERREIRA; SOUTO, 2005; SIMONS; ROBERSON, 2003). A noção de justiça, nesta perspectiva, está fundamentada em valores, crenças e sentimentos em relação às ações humanas consideradas justas ou injustas. As atitudes e os comportamentos das pessoas, durante as suas interações sociais, sofrem influência de julgamentos individuais a respeito daquilo que é certo ou errado, merecido ou não merecido e sobre direitos e deveres em geral.

Bies e Moag (1986) propuseram critérios para a equidade de tratamento interpessoal: a tomada de decisão que impacta na vida dos indivíduos deve fundamentar-se na verdade, no respeito e numa adequada comunicação, oferecendo explicações e justificativas para as respectivas decisões. Desta forma, quando um trabalhador percebe algum grau de injustiça

nas relações interpessoais com seu interlocutor (um chefe ou colega que participa da interação social por meio da linguagem), ele pode reagir negativamente considerando aspectos cognitivos, afetivos e comportamentais (COHEN-CHARASH; SPECTOR, 2001). Conforme esses autores, o sentimento negativo originado pela falta de equidade no âmbito da justiça interpessoal não é direcionado para a organização como um todo; a retaliação daquele que se sente injustiçado objetiva a pessoa ou o grupo que participou da respectiva interação.

A justiça informacional, por sua vez, aborda a justificativa para decisões tomadas e de que maneira essas decisões foram comunicadas (REGO; SOUTO, 2004). Segundo os autores, trabalhadores esperam que seus líderes forneçam explicações lógicas, sinceras e adequadas sobre as decisões que são tomadas em âmbito organizacional; especialmente, quando produzem efeitos desfavoráveis. Ao fornecer justificativas aceitáveis, através do melhor conjunto de informações disponíveis, as reações negativas frente a percepção de injustiça informacional são reduzidas (REGO; SOUTO, 2004).

A percepção de justiça ou injustiça, bem como das suas respectivas dimensões subjacentes (distributiva, procedimental, interpessoal e informacional) dependem de peculiaridades próprias da subjetividade humana (RIBEIRO; BASTOS, 2010). Essas percepções são construídas a partir de elementos intrínsecos ao sujeito, tais como sua história, valores, crenças e expectativas sobre o mundo (RIBEIRO; BASTOS, 2010). Mesmo adquirindo similaridade com aspectos culturais estabelecidos em seu contexto social vigente, tais percepções derivam de características próprias e individuais da pessoa.

O Quadro 6 sintetiza as principais dimensões da justiça percebida pelas pessoas no local de trabalho e que estão no foco desta pesquisa. Embora as dimensões de justiça percebidas pelos indivíduos façam parte de um fenômeno mais geral (o conceito de justiça), cada uma delas tem uma dinâmica própria e uma relação específica com os respectivos antecedentes e consequentes, sejam eles positivos ou negativos em relação ao comportamento humano (RIBEIRO; BASTOS, 2010). Esta dimensionalização oferece um melhor entendimento dos elementos relacionados a percepção de justiça; contudo, não são independentes do contexto em que os indivíduos estão situados (GREENBERG, 1990).

Quadro 6 – Síntese dos Fatores da Justiça Organizacional

Dimensão	Descrição conceitual	Definição	Foco
Justiça Distributiva	Avalia o tratamento justo pela adequada proporção entre contribuições e recompensas. A comparação ocorre entre os pares.	Justiça Finalística	Resultados
Justiça Procedimental	Avalia o tratamento justo do processo de elaboração de critérios de avaliação, de reconhecimento e distribuição de resultados.	Justiça dos Meios	Processo
Justiças Interacional e Informacional	Tratamento justo nos contatos interpessoais, entre decisores e quem sofre os efeitos das decisões, considerando o respeito, a dignidade e a disponibilidade de informações precisas, claras, transparentes e oportunas.	Justiça do Diálogo	Comunicação

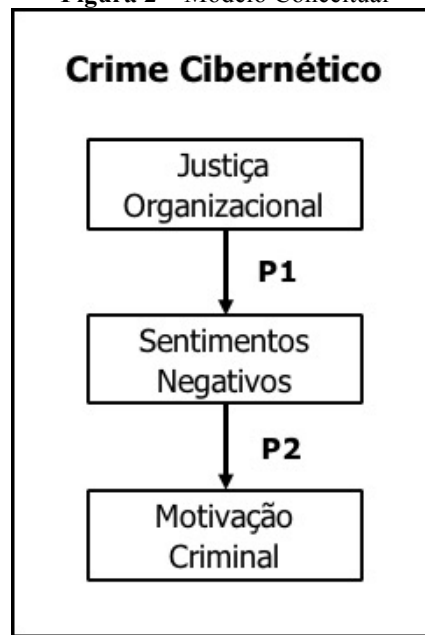
Fonte: adaptado de Ribeiro e Bastos (2010)

2.6 MODELO CONCEITUAL

O modelo conceitual representa o mundo real (DUIT et al., 1996). Ele é um artefato importante que ilustra conceitos e relações inerentes ao domínio desta pesquisa. Ao mesmo tempo, não aspira refletir com perfeição a realidade imaginada. Os elementos, as relações e os significados contidos (implícita ou explicitamente) no diagrama ilustrado na Figura 2 foram propostos a partir de uma reflexão deste pesquisador e, conseqüentemente, estudados para um melhor entendimento do fenômeno em questão.

Através desse modelo, foi possível delinear os procedimentos para coleta e análise dos dados, considerando o contexto em que as variáveis foram trabalhadas (PRODANOV; FREITAS, 2013). O modelo conceitual, em sua fase inicial, estimulou a investigação de uma realidade social com impacto em diferentes realidades organizacionais, criando uma estrutura análoga e abstrata daquilo que se pretendia explorar, sem a pretensão de ser perfeitamente acurado (MOREIRA, 1996).

Figura 2 – Modelo Conceitual



Fonte: elaborado pelo autor (2015)

O conhecimento prévio disponível sobre o tema orienta a importantes premissas sobre a realidade que aqui se investiga. As organizações trabalham para maximizar ganhos e minimizar prejuízos. O crime cibernético provoca danos e, conseqüentemente, prejuízos (YAR, 2005; ROGERS; SEIGFRIED; TIDKE, 2006). Na medida em que se conhece as motivações para o crime e, principalmente, os respectivos antecedentes, seria possível influenciar as variáveis relativas ao ambiente organizacional que incentivam os indivíduos ao crime cibernético (WILLISON; WARKENTIN, 2013).

Estudos relacionados à qualidade de vida das pessoas no local de trabalho constataram que o descontentamento dos trabalhadores impacta diretamente nas atitudes e no comportamento destes indivíduos em relação a organização (WILLISON; WARKENTIN, 2013). Através da percepção sensorial, utilizando seus sentidos e sua inteligência, um indivíduo é capaz de reconhecer, interpretar e compreender informações oriundas do meio (FEELINGS, 1998). Ao receber e decodificar sinais exteriores, o indivíduo atribui significados aos dados analisados e organizados conforme suas crenças, valores éticos e princípios morais (SCHWARZ; CLORE, 1996). Essas percepções sofrem influências das características culturais de uma sociedade.

Sentimentos negativos gerados pela percepção de injustiça no contexto organizacional podem levar a condutas indesejadas contra a empresa e seus gestores (BASCH; FISHER, 1998). A percepção de injustiça na distribuição de recompensas e reconhecimento, na vivência ou participação em processos organizacionais, na relação interpessoal com

superiores e colegas, ou mesmo na qualidade da comunicação de informações produz diferentes intensidades emocionais de dor, mal-estar, desconforto, ansiedade, aflição frustração, culpa, raiva, entre outros estados psíquicos de sofrimento (ADAMS, 1965; SKARLICKI; FOLGER, 1997; WILLISON; WARKENTIN, 2009). Conforme as características psicossociais de cada indivíduo, esses sentimentos negativos podem adquirir maior ou menor importância na motivação para a prática de atos ilegais ou imorais, como é o caso do crime cibernético.

O modelo conceitual proposto neste trabalho demonstra que o crime cibernético praticado por *insiders* tem relação indireta com a percepção de injustiças no contexto organizacional. Esse entendimento é defendido nas pesquisas de Willison (2006), Willison e Siponen (2009) e Willison e Warkentin (2013) sobre descontentamento das pessoas em seu local de trabalho. A redução dos incidentes de segurança cibernética, então, estaria comprometida com estratégias de gestão que minimizassem injustiças distributivas, procedimentais, interpessoais ou informativas.

Quando o gestor desconhece as motivações que levaram pessoas da sua própria organização a praticar crimes cibernéticos, sua capacidade de interferência ou influência diminui. Quando ele compreende os fatores estimuladores que extrapolam as características e patologias individuais, mudanças no local de trabalho podem ser encaminhadas para que os sentimentos negativos não evoluam facilmente. Neste sentido, o entendimento do comportamento potencialmente nocivo das pessoas oferece melhores condições para gerenciar os riscos pertinentes ao crime cibernético no âmbito organizacional (ME; SPAGNOLETTI; IEEE, 2005).

Levando em consideração tais premissas e reflexões, as seguintes proposições emergem sobre as percepções relacionadas à injustiça organizacional que motivariam *insiders* a cometer crimes cibernéticos nas suas próprias organizações:

- a) **Proposição 1 (P1):** A percepção de injustiça, no contexto organizacional, produz sentimentos negativos no indivíduo;
- b) **Proposição 2 (P2):** Os sentimentos negativos do indivíduo influenciam a sua motivação criminal.

3 MÉTODO DE PESQUISA

Esse capítulo apresenta o método de pesquisa que foi utilizado a partir das proposições estabelecidas pelo modelo conceitual derivado da revisão de literatura e proposto pelo pesquisador. Os itens subsequentes apresentam o desenho de pesquisa, o instrumento a ser aplicado nas entrevistas e a estratégia para a coleta de dados.

3.1 ESCOLHA DO MÉTODO

Os objetivos deste trabalho (geral e específicos) foram atingidos através de uma pesquisa qualitativa, desenvolvida a partir de entrevistas em profundidade com especialistas no tema da segurança cibernética. O estudo é exploratório, atitudinal, com corte transversal, e utiliza um roteiro semiestruturado como apoio para a coleta dos dados (MALHOTRA, 2012; MYERS, 2013). Essa estratégia de investigação foi o caminho escolhido para compreender de que maneira fatores relacionados ao local de trabalho podem levar pessoas a praticar crimes cibernéticos.

Coletando dados relacionados a perspectiva desses profissionais, foi possível mapear os principais fatores que teriam impacto na motivação para o crime cibernético no contexto organizacional. Inferências realizadas a partir da análise dos dados, por sua vez, oportunizaram um melhor entendimento do fator humano, suas atitudes e comportamentos, bem como a influência que é exercida pelo local de trabalho sobre as intenções pessoais para alcançar determinados fins. No caso deste trabalho, as intenções que estavam relacionadas ao crime cibernético em organizações brasileiras.

Temas que envolvem a segurança cibernética, bem como as causas ou consequências dos crimes cibernéticos, apresentam elevado nível de restrição no que tange o compartilhamento de estratégias, políticas, planos, análises de risco e histórico de incidentes. A troca de informações sobre o tema é normalmente complicada, mesmo que os dados a serem compartilhados estejam sob a regulação formal de contratos de confidencialidade. As barreiras impostas ao pesquisador foram significativas. Em geral, as empresas têm cuidado especial ao divulgar informações que possam comprometer sua credibilidade junto a clientes e fornecedores. Neste sentido, a coleta de dados sobre crimes cibernéticos nas organizações pesquisadas exigiu do pesquisador o desenvolvimento de um relacionamento construtivo e transparente com os envolvidos neste estudo. Antes, durante e depois das entrevistas, o pesquisador procurou manter relações de confiança, contando inclusive com a credibilidade

do seu passado na área de TI, bem como indicações e recomendações da sua rede de relacionamentos profissionais e pessoais para que o processo de interação produzisse os resultados esperados. Esse esforço foi válido na medida em que os participantes da pesquisa demonstraram interesse, disposição e comprometimento para colaborar com os estudos. A maioria deles manifestou desejo em obter os resultados da pesquisa, confiando na validade e confiabilidade do estudo, e acreditando na contribuição desta pesquisa para campo da segurança cibernética.

Inicialmente, o pesquisador participou do ROADSEC, um evento itinerante destinado a profissionais e estudantes interessados em segurança e tecnologia. Ele percorre o Brasil a pelo menos 5 anos, contando com a contribuição e participação de empresas do ramo, hackers, especialistas, acadêmicos, profissionais, técnicos, gerentes e curiosos sobre a área. Na sua edição em Porto Alegre, realizada em 03 de outubro de 2015, na PUCRS (Prédio 32), o pesquisador procurou familiaridade com o perfil do público alvo para a coleta de dados, conhecendo sua linguagem, percepções, costumes e estilos de relacionamento. Foi o primeiro passo para o levantamento de contatos que poderiam participar das entrevistas programadas para esta investigação. No transcorrer do evento, já foi possível construir as primeiras interações e agendar encontros para a coleta de dados.

Figura 3 – Imagens do Evento de Segurança Cibernética em Porto Alegre



Fonte: ROADSEC Porto Alegre (2015)

Na sequência, o pesquisador participou do encerramento do ROADSEC de 2015 em São Paulo, SP, no dia 12 de novembro, na Áudio Clube, com a presença de mais e 2.000 pessoas da área de tecnologia e segurança cibernética. Profissionais, estudantes e acadêmicos provenientes de várias partes do Brasil compareceram ao evento. O pesquisador participou de oficinas, trilhas de palestras e visitou estandes de patrocinadores (empresas da área da segurança cibernética). Contatou, prioritariamente, palestrantes e representantes de

organizações envolvidas com a segurança cibernética para posterior agendamento de entrevistas. A Figura 4 apresenta fotos do evento ocorrido em São Paulo.

Adicionalmente aos contatos obtidos durante os dois eventos do ROADSEC, o pesquisador utilizou sua rede de relacionamentos profissionais prévios para selecionar outros entrevistados cujo perfil agregaria valor ao trabalho. Na medida em que realizava contato com essas pessoas, foi possível obter indicações importantes (referências de empresas de tecnologia, listas de discussão, grupos em redes sociais,) que oportunizaram o contato com pessoas que não estavam no levantamento inicial. A rede social LinkedIn (<http://linkedin.com>) foi igualmente utilizada para avaliar a possibilidade de convidar outros profissionais para o grupo final de informantes da pesquisa. Algumas entrevistas que foram realizadas são fruto dessas fontes de contato secundárias.

Outra iniciativa importante foi o contato com colegas de curso que pertencem a empresas de tecnologia instaladas no Parque Tecnológico da PUCRS (Tecnopuc), os quais recomendaram possíveis informantes para esta pesquisa. Considerando o nível de importância e influência que algumas empresas instaladas Tecnopuc possuem no mercado e na pesquisa na área de TI, o contato com profissionais dessas organizações era fundamental.

Os convites foram enviados por *e-mail*, onde o pesquisador passava todas as informações relativas a coleta de dados, bem como a finalidade e missão do estudo. Ficou claro que havia interesse e respeito pelo trabalho, pois a maioria dos contatos obteve retorno e agendamento de uma entrevista. Quando o encontro presencial não era possível, avaliava-se a possibilidade de uma conferência virtual que pudesse viabilizar uma coleta dos dados sem ônus para a qualidade de uma adequada interação entre pesquisador e entrevistado.

A presença do pesquisador em eventos da área, bem como o contato junto a representantes da comunidade de TI envolvida com a temática da segurança cibernética foi relevante para o processo de entrevistas. Tal aproximação com o campo de estudos ajudou no reconhecimento de questões chave da área, bem como de peculiaridades sobre o perfil dos indivíduos que participam deste complexo universo social. Inegavelmente, essas experiências colaboraram no aperfeiçoamento das interações entre o pesquisador e os participantes do estudo, proporcionando dados com maior potencial de contribuição para essa pesquisa exploratória.

Figura 4 – Imagens do Evento de Segurança Cibernética em São Paulo



Fonte: ROADSEC São Paulo (2015)

As causas da motivação pessoal têm natureza particular, variada, imprecisa e nem sempre padronizável (FLICK; NETZ, 2004). Captar pontos de vista dos entrevistados em um processo interativo, livre da rigidez de um questionário estruturado, favorece novas descobertas sobre o tema. As entrevistas com os participantes do estudo tiveram flexibilidade e desenvolvimento informal; contudo, não perderam o foco nos objetivos anteriormente estabelecidos. Embora com algum grau de liberdade, as entrevistas tinham orientação e estavam subordinadas a um escopo predefinido (GIL, 2002).

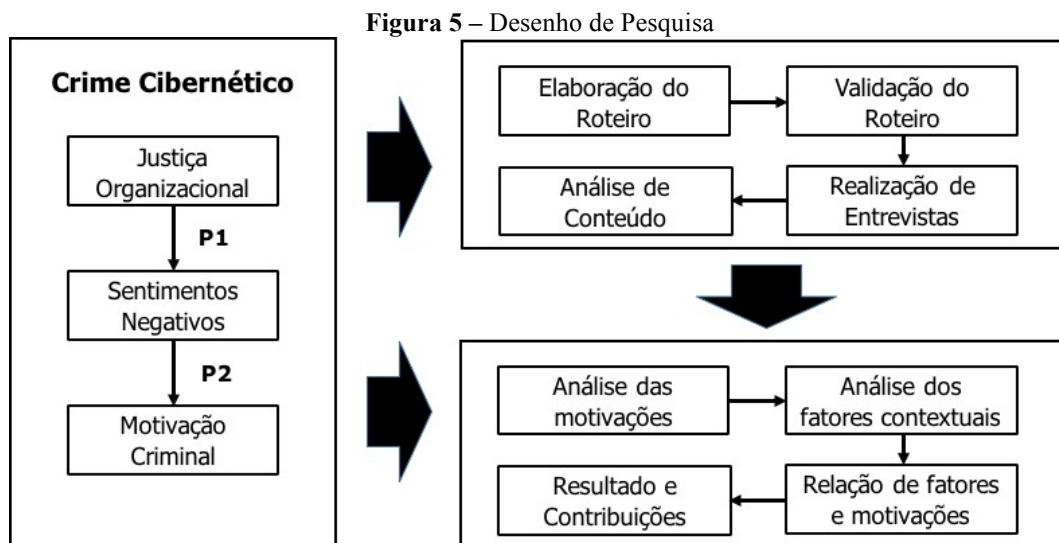
Segundo Hair Jr. et al. (2005), a entrevista ocorre quando o pesquisador “fala” com o respondente ou informante, fazendo perguntas e registrando respostas. As entrevistas podem ocorrer em lugares variados, de forma presencial ou remota (FLICK; NETZ, 2004). Ao utilizar uma entrevista com um roteiro semiestruturado, o entrevistador acompanha as

respostas e realiza perguntas que não foram necessariamente previstas, mas que podem ser interessantes para o estudo.

Compreender as relações entre os sentimentos negativos provocados por percepções de injustiça organizacional e as motivações para o crime cibernético exige uma minuciosa análise dos dados sobre atitudes e comportamentos das pessoas envolvidas em incidentes de segurança. O contato com especialistas da área foi indispensável para obter informações que pudessem, efetivamente, contribuir na construção dos resultados desta pesquisa. Essas pessoas são representantes de um grupo com domínio sobre as questões humanas, tecnológicas e operacionais da segurança cibernética, e com vivências relevantes sobre o tema no contexto das organizações.

3.2 DESENHO DE PESQUISA

A pesquisa foi encaminhada conforme as etapas definidas na Figura 5:



Fonte: elaborado pelo autor (2015)

Considerando aspectos relacionados a uma pesquisa de caráter qualitativo exploratório, o desenho foi construído de forma flexível. Esta estrutura foi pensada para uma investigação narrativa, onde o produto das entrevistas, somado a revisão da literatura, ajudasse na compreensão de um tema ainda pouco explorado, especialmente no contexto das organizações brasileiras. A técnica utilizada de entrevistas em profundidade considera a coleta de narrativas individuais, cujas inferências receberão significados que possam explicar o que, de fato, está acontecendo no universo investigado.

3.3 INSTRUMENTO DE PESQUISA

O instrumento desta pesquisa que guiou e apoiou as entrevistas em profundidade encontra-se no Apêndice B, e aborda a temática das motivações para o crime cibernético e a influência do contexto nesse processo. Este instrumento foi validado por 3 acadêmicos doutores (PUCRS/FACE, PUCRS/FACIN e UFRGS/EA) que sugeririam alterações e melhorias para aumentar a eficácia da coleta. Basicamente, a ordem das perguntas foi alterada, para que existisse uma sequência lógica de conceitos. Por sugestão desses acadêmicos, uma tabela de sentimentos negativos relacionados com fatores estimuladores para o crime cibernético foi excluída, a fim de não induzir as respostas dos informantes. Por fim, questionamentos complementares em cada pergunta foram adicionados para enfatizar a necessidade de respostas justificadas e baseadas em vivência profissionais. Todas essas sugestões de melhorias apresentadas pelos professores validadores foram prontamente incorporadas à redação final do instrumento.

Durante as entrevistas, os participantes da pesquisa não ficaram restritos a respostas fechadas. As perguntas foram formuladas de maneira simples e objetiva, no intuito de facilitar uma compreensão precisa. Foram evitadas palavras ambivalentes ou sugestivas que prejudicassem a espontaneidade das respostas. Portanto, o instrumento teve função diretiva, controlando o foco, delimitando o escopo, e evitando dispersões improdutivas. Os questionamentos procuraram traduzir os objetivos da pesquisa. Perguntas complementares foram realizadas pelo pesquisador sempre que necessário, visando o esclarecimento de questões pontuais.

Considerou-se que o entrevistado possuía amplo e profundo conhecimento sobre o tópico deste estudo, estando apto a articular suas ideias com apoio dos questionamentos existentes no roteiro de entrevistas. Os informantes tiveram liberdade para emitir suas opiniões e responder as perguntas usando linguagem própria. O perfil do respondente seguiu critérios definidos no item 3.4. Adicionalmente, foi entregue a cada informante um termo de sigilo (Apêndice A) formalizando a proteção dos dados coletados e a finalidade exclusivamente acadêmica da coleta.

3.4 COLETA DE DADOS

A seleção dos entrevistados foi “não probabilística” e intencional, adequando-se a estágios exploratórios da pesquisa (AAKER; KUMAR; DAY, 2004). Foram realizadas 16

entrevistas com profissionais de segurança cibernética, entre consultores, gerentes e analistas sêniores, vinculados a empresas que prestam serviços na área da segurança cibernética ou a departamentos de tecnologia da informação (TI). Esse número foi considerado adequado para responder a pergunta de pesquisa, e suficiente durante o processo de categorização do conteúdo analisado (saturação de dados) (MARSHALL, 1996). Ao contrário de uma seleção aleatória, os participantes foram selecionados estratégica e propositalmente conforme seu nível de conhecimento, experiência e capacidade de contribuição com a pesquisa proposta (DRIESSNACK; SOUSA; MENDES, 2007). Os entrevistados são especialistas no assunto, com mais de 5 anos de experiência na área de segurança cibernética e mais de 10 anos de experiência profissional na área de TI.

Os encontros com os participantes deste estudo foram presenciais (reuniões previamente agendadas) e virtuais (via conferência utilizando o aplicativo *Microsoft Skype*). As reuniões presenciais ocorreram na cidade de Porto Alegre, RS. As entrevistas virtuais foram feitas com participantes residentes em São Paulo, SP. Todas as entrevistas foram realizadas no mês de fevereiro de 2016, conforme agendamento prévio com cada entrevistado. As falas dos entrevistados foram gravadas (gravador digital MP3) e, posteriormente, o conteúdo desses áudios foi transcrito em arquivos de texto (*Microsoft Word*). O tempo total de duração das entrevistas foi de onze horas e cinquenta e cinco minutos (11:55). O tempo médio de duração desses encontros presenciais e virtuais foi de quarenta e quatro minutos (0:44). O Quadro 7 detalha essas informações.

Quadro 7 – O Perfil dos Entrevistados

(Continua)

Entrevista	Tempo	Cargo / Função / Formação	Experiência
01	00:31	Consultor de Segurança da Informação Sr.; CISSP; CRISC e Doutorando.	11 anos
02	00:36	Gerente de Segurança da Informação	15 anos
03	00:27	Consultor e Especialista em Segurança da Informação; Palestrante e Instrutor.	16 anos
04	00:14	Delegado de Polícia e Professor Universitário.	05 anos
05	00:15	Gestor de Projetos e TI.	10 anos
06	01:02	Professor Universitário, Consultor e Empreendedor na área de Segurança da Informação.	08 anos
07	00:42	Professor Universitário; Coordenador de datacenter de grande porte.	10 anos
08	00:38	Analista de Segurança e Investigador Forense.	05 anos

(Conclusão)

Entrevista	Tempo	Cargo / Função	Experiência
09	01:08	Analista, consultor e empreendedor na área de TI e segurança da informação.	15 anos
10	00:46	Gestora de Sistemas de Informação e Segurança.	30 anos
11	00:35	Pesquisador de Malwares e Soluções de Segurança.	09 anos
12	00:26	Analista de Segurança da Informação.	05 anos
13	00:47	Consultor e Contratante de Sistemas de Informação e Segurança.	10 anos
14	01:16	Empreendedor e Consultor em segurança da informação.	13 anos
15	00:51	Analista de Infraestrutura, Redes e Segurança.	11 anos
16	01:34	Consultor de Risco; Gestor de Conformidade; Auditor e Especialista em Segurança da Informação.	12 anos

Fonte: elaborado pelo autor (2015)

As entrevistas transcritas foram trabalhadas através da técnica denominada análise de conteúdo (BARDIN, 2006). Tal técnica é composta por um conjunto de procedimentos sistemáticos e objetivos para a clara e efetiva descrição do conteúdo das mensagens coletadas (BARDIN, 2006). Conforme Chizzotti (2006, p. 98), “o objetivo da análise de conteúdo é compreender, criticamente, o sentido das comunicações, seu conteúdo manifesto ou latente, as significações explícitas ou ocultas”.

A análise de conteúdo realizada nesta pesquisa foi estruturada em três fases: primeiramente, logo após a transcrição das entrevistas, ocorreu a pré-análise dos dados, que consiste numa leitura flutuante do material e no tratamento preliminar de resultados (BARDIN, 2006). Nesta fase, nenhuma categoria foi estabelecida. Na segunda fase, os dados foram codificados a partir do conteúdo registrado (BARDIN, 2006). A codificação “corresponde a uma transformação – efetuada (sic) segundo regras precisas – dos dados brutos do texto, transformação esta que, por recorte, agregação e enumeração, permite atingir uma representação do conteúdo, ou da sua expressão” (BARDIN, 2006, p. 103).

Na última fase, uma análise temática foi realizada, na qual categorias emergiram a partir da sensibilidade deste pesquisador. Estas categorias foram consolidadas com aquelas já identificadas na revisão de literatura. A categorização é um processo que classifica os elementos constitutivos de um conjunto por diferenciação (BARDIN, 2006). Em seguida, reagrupa-os segundo critérios previamente definidos. “As categorias são rubricas ou classes, as quais reúnem um grupo de elementos [...] sob um título genérico, agrupamento esse efetuado em razão das características comuns dos elementos” (BARDIN, 2006, p. 117).

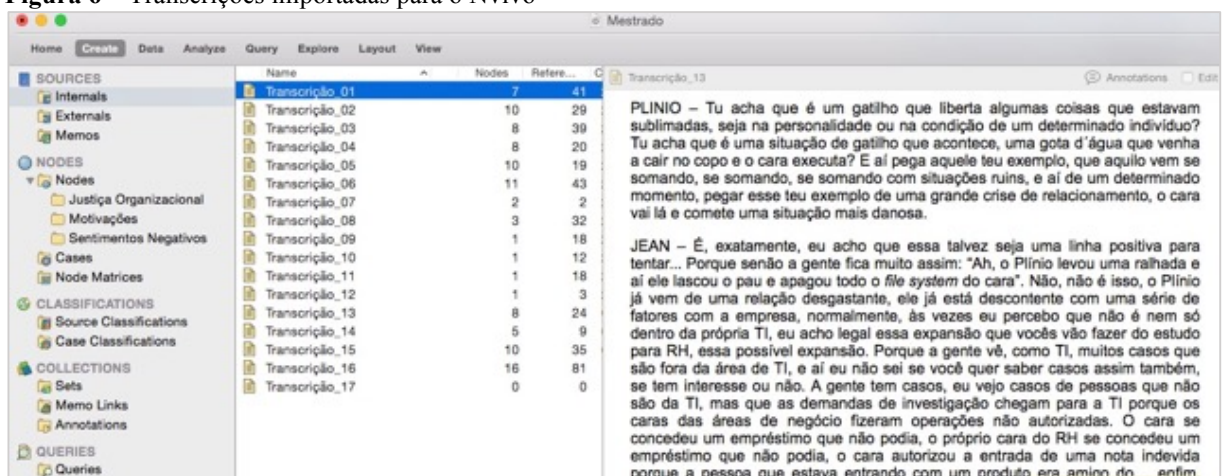
A análise por categorias temáticas tentou encontrar significações que possibilitaram a caracterização de um segmento ou ideia, atribuindo classes a partir do julgamento do pesquisador (CAREGNATO; MUTTI, 2006). A validade da análise de conteúdo não produz, necessariamente, uma “leitura verdadeira” dos dados; sua fundamentação, todavia, precisa estar congruente com as teorias consideradas nesta pesquisa (BAUER; GASKELL, 2000).

Nesse processo, o conteúdo foi desmembrado em unidades e reorganizado. Para classificar os elementos foi preciso identificar suas características comuns (CAREGNATO; MUTTI, 2006). Este trabalho de exploração e categorização foi realizado com auxílio do software de análise de conteúdo denominado NVIVO², da *QSR International*, o qual serviu como facilitador da estruturação das categorias em relação ao volume de dados coletados nas entrevistas.

Entre as 16 transcrições analisadas, foram codificados, a partir da revisão de literatura ou dos diálogos coletados com os participantes das entrevistas, uma variedade de categorias: 3 para o constructo de Justiça Organizacional, 25 para o constructo Motivação Criminal (com 6 subcategorias adicionais), e, finalmente, 29 para o constructo Sentimentos Negativos.

As Figuras 6 e 7 ilustram esta organização conceitual do conteúdo.

Figura 6 – Transcrições importadas para o Nvivo



² NVivo é um *software* desenvolvido especialmente para auxiliar em pesquisas que utilizam o método qualitativo, ajudando a organizar, analisar e encontrar informações em dados não estruturados, como é o caso das transcrições textuais das entrevistas que foram feitas com especialistas em segurança cibernética (QSR INTERNATIONAL, 2016).

Figura 7 – Processo de codificação no Nvivo

The screenshot displays the NVivo software interface. On the left, a tree view shows the project structure under 'Mestrado', including 'SOURCES', 'NODES', 'CLASSIFICATIONS', 'COLLECTIONS', and 'QUERIES'. The 'Motivações' node is selected. The main area shows a list of nodes with columns for 'Name', 'Sources', and 'References'. The 'Ganância' node is highlighted, showing 3 sources and 10 references.

Nome	Sources	Referências
Patologias_Individuais-L2.1	6	19
Vingança-L3.2	4	14
Oportunidade	4	8
Associação-L2.1	3	5
Costume-L3.2	2	5
Impunidade-L2.2	2	4
Autoafirmação-L3.2	2	2
Desorganização_Social-L2.1	1	2
Econômica-L3.2	1	2
Ganância	3	10
Ambição	1	1
Necessidade	2	2
Tensão_Social-L2.1	2	2
Anomia-L2.1	1	1
Chantagem	1	1
Curiosidade-L3.2	1	1
Escusação	1	1
Política	1	1
Sexo	1	1
Status-L3.2	1	1
Adrenalina-L3.2	0	0
Aprendizagem-Social-L2.1	0	0
Ativismo-L3.2	0	0
Autocontrole-L2.1	0	0
Controle_Social-L2.1	0	0
Fama-L3.2	0	0
Patriotismo-L3.2	0	0

The right panel shows the 'Ganância' node details. It includes a 'Summary' tab and a 'Reference' tab. The 'Reference' tab displays five references with their respective coverage percentages:

- Reference 1: 0.36% coverage**
A gente tem muita questão do lucro. Do lucro ser uma das grandes motivações, a gente tem várias vertentes aí
- Reference 2: 0.16% coverage**
Dentro das organizações tu vai ver muito lucro
- Reference 3: 1.56% coverage**
ele vai receber um trojan (0:26:10) do tipo banker (0:26:12), que é um trojan (0:26:13) especializado em obter as informações de internet banking e fazer transações no teu nome. Ali vê-se claramente que é voltado ao lucro e mais do que isso, o mal é classificado por uma empresa de segurança que faz pesquisa como mal da família banker. Aí nas enciclopédias deles eles deixam claro: banker visa o lucro, banker vai obter teus credenciais de acesso ao internet banking
- Reference 4: 1.25% coverage**
Lá na década de noventa até início dos anos dois mil e pouco, quando a gente não tinha tantas transações eletrônicas, aí sim existia mais cenário, mais terreno pra que as motivações fossem vingança, fossem querer aparecer no grupinho, disputas, pertencer a um grupo, não que isso ainda não exista, só que isso perdeu espaço uma vez que o dinheiro passou a ir pro mundo digital
- Reference 5: 0.17% coverage**
Aqui no Brasil é forte, forte, forte, forte o lucro

Fonte: arquivos do autor (2016)

4 ANÁLISE DOS DADOS

A estratégia para a pesquisa foi desenvolver uma investigação exploratória, atitudinal, com corte transversal, que capturasse significados inerentes ao tema a partir da percepção dos respectivos informantes. A análise dos dados coletados considerou, então, a interpretação do respectivo conteúdo existente na contribuição de cada participante da pesquisa, viabilizando descobertas importantes.

Este capítulo de análise de dados apresenta a exploração, a decomposição e o exame minucioso dos dados coletados durante as entrevistas com os especialistas em segurança cibernética. Buscou-se explicar e relacionar conceitos subjacentes ao tema para que fosse possível compreender o fenômeno como um todo.

O processo de análise ocorreu em paralelo com a realização de novas coletas, sofrendo ajustes conforme as revelações evoluíam (COLLADO; LUCIO; SAMPIERI, 2013). Cada entrevista transcrita apresentava dados não estruturados, os quais foram transformados em um sistema de categorias, considerando suas diferenças e semelhanças conceituais. A interpretação das vivências, experiências, sentimentos e opiniões dos entrevistados ocorreu mediante a reconstrução e significação das histórias relatadas, e possibilitou ao pesquisador compreender as circunstâncias envolvidas no respectivo contexto social.

4.1 JUSTIÇA ORGANIZACIONAL

A maioria dos trabalhos sobre o crime cibernético, incluindo aqueles que analisavam o papel do *insider* como ator principal dos incidentes de segurança em âmbito organizacional, não dava a devida atenção aos aspectos relacionados ao local de trabalho e as respectivas percepções de injustiça que dali emergiam. Tal realidade é reconhecida por Willson (2006), cujos trabalhos enfatizam a relevância dos fatores contextuais na produção de sentimentos negativos. Outras pesquisas também corroboram com essa perspectiva sobre as causas do crime cibernético (BURDEN; PALMER, 2003; CHOO, 2011; DHILLON; MOORES, 2001; GOODE; CRUISE, 2006; HUNTON, 2009; ROGERS, MANUS K., 2006; TUNLEY, 2011; VASHISTH; KUMAR, 2013).

Assim sendo, a motivação para o crime cibernético, conforme esse entendimento anterior, estaria fundamentada em elementos intrínsecos ao indivíduo na condição de criminoso no contexto do universo virtual. As características psicossociais dessas pessoas orientariam suas ações para o crime. Elementos que compõe a ética e a moral de determinados

trabalhadores, por conseguinte, seriam determinantes do comportamento malicioso, não sendo possível ao gestor atuar na reversão desse cenário. Caberia aos gestores, tão somente, a função de monitoramento, identificação, punição e exclusão daqueles que fossem pegos praticando o crime cibernético.

Fatores relacionados ao local de trabalho pareciam irrelevantes para a tomada de decisão na direção do crime cibernético. O Entrevistado 16 demonstra esse entendimento a partir das seguintes colocações: “As pessoas sempre foram assim, elas sempre foram más”; “A tal pessoa já queria fazer; ela só encontrou um motivo”; “O que eu quero aqui dizer é que um ambiente organizacional, por pior que ele seja, não gera um ladrão. A pessoa já tinha essas características”.

A visão de que a motivação para o crime cibernético está no indivíduo, e que o contexto organizacional pouco influencia, também é corroborada pelo Entrevistado 1 nas passagens a seguir: “Em alguns casos, quando tu falaste, por exemplo, da relação com o chefe, vai naquela linha das questões psicológicas do atacante ou do potencial atacante ter resistência com a autoridade”; “De repente, o chefe é um cara justo. De repente, o processo dentro da empresa é um processo que é igual para todos, mas na formação dele, por um motivo que somente ele entendia, ele era o real merecedor de alguma coisa”. O Entrevistado 2 complementa com a seguinte visão:

Eu tenho convicção que isso é um desvio de comportamento muito orientado à falta de ética profissional, falta de conduta, falta de uma conduta adequada. Nessa minha vivência aí de mais de doze anos em segurança da informação, o perfil dos profissionais que tiveram atitudes dessa natureza era um perfil de pessoas não só despreparadas, mas até com um histórico.

Pessoas que vieram de uma qualidade de educação não muito boa, que muitas vezes até estavam em posições de alta responsabilidade na empresa, mas não tinham uma formação acadêmica mínima necessária. E, baseada nessa falta de conteúdo, de formação e de educação queriam se autopromover ou queriam fazer mal à alguma outra instituição.

Por fim, o Entrevistado 3 sentencia:

Em todos os grupos, nós vamos encontrar três tipos de indivíduos; 10% vão ser sempre os mal-intencionados [...] você pode dar a cadeira mais confortável, colocar os benefícios para ele, mas nunca ele vai estar satisfeito. Esse cara é um risco iminente ao *business*.

Talvez essas opiniões sejam fruto de uma crença anterior de que as motivações das pessoas estariam dependentes das características individuais de cada um, deixando a influência exercida pelo contexto na condição de irrelevância. Com o avanço de alguns trabalhos na

direção do entendimento sobre a problemática da qualidade de vida das pessoas no seu local de trabalho, observou-se que elementos relacionados aos sentimentos negativos lá adquiridos também exerciam impacto na motivação das pessoas. Para o bem ou para o mal. E é nesse sentido que emergiram colocações importantes relacionadas aos conceitos de justiça distributiva, justiça procedimental e justiça interacional e informacional.

Os informantes falavam, frequentemente, na questão da injustiça percebida pelos indivíduos no contexto organizacional, e como essa percepção fornecia energia para o engajamento em atos de retaliação. Conforme Maia (2010), sentimentos de raiva, ultraje ou ressentimento que surgem em consequência de decisões organizacionais ou ações gerenciais julgadas injustas fornecem o estímulo para a retaliação. Na visão de vários informantes, a vingança tem participação decisiva na motivação para o crime cibernético. O Entrevistado 4 destaca as seguintes ponderações a respeito: “Uma insatisfação em relação à questão do não reconhecimento de um trabalho realizado [...] pode gerar uma vingança”; “Por que o outro e não eu, se eu fiz a mesma coisa?”. O Entrevistado 13, complementa:

Tinha pessoal varrendo ERP para ver quanto o terceiro ganhava. Porque, por exemplo, tinha desenvolvedor interno e desenvolvedor externo, e o desenvolvedor interno varrendo o ERP e lá olhando lançamento de nota e tal para saber quanto o desenvolvedor externo estava recebendo para ir no chefe dele dizer: Tu estás pagando mais caro para o desenvolvedor externo.

Focando especificamente na falta de equidade sobre rendimentos financeiros, o Entrevistado 16 relata: “Tem gente que simplesmente não entende que o cara do lado, por algum motivo, ganha mais”; “A pessoa tem essa percepção de que o outro tem que ganhar igual”.

No que tange às percepções de injustiça procedimental, os dados coletados sugerem que sentimentos negativos capazes de motivar o crime cibernético são igualmente gerados em eventos onde o indivíduo percebe que foi injustiçado em processos organizacionais. O Entrevistado 3 coloca: “Então, quando as pessoas veem que alguém transgrediu uma regra que era clara e esse alguém foi punido, elas sentem uma sensação de satisfação pelo cumprimento da regra”. E depois, o mesmo entrevistado complementa:

Da mesma forma que quando alguém transgride uma regra que é óbvia e não existe punição, elas se sentem violadas, porque elas estão sentindo que estão sendo feitas de palhaço, porque eu estou fazendo isso e uma pessoa transgrediu a regra e não aconteceu nada com ela. Então, a sensação da impunidade é muito ruim (ENTREVISTADO 3).

O Entrevistado 5 destaca problemas comuns na gestão das pessoas em âmbito organizacional, e que certamente gera polêmica: “Na minha última avaliação 360, a empresa me avaliou errado”. O Entrevistado 16, por sua vez, identifica algumas regras organizacionais que normatizam processos internos impondo aos funcionários certas limitações que geram críticas e desgastes de relacionamento.

Tem aquele gerente de TI que me liga e fala assim: “Eu não quero que o cara use USB; eu não quero que ele coloque o fone de *bluetooth* dele; eu quero impedir que ele conecte o Android para carregar no USB; eu não quero que o cara faça nada”. Eu falei: “Puxa, meu irmão, tu queres o quê? Tu estás criando o teu funcionário em cativoiro” (ENTREVISTADO 16).

Certamente, as principais indicações de que a justiça organizacional pode gerar sentimentos negativos que motivam os indivíduos para o crime cibernético está nas percepções de injustiça interpessoal. Nesta dimensão da justiça organizacional residem os mais delicados aspectos da personalidade humana e de que forma o sujeito lida com suas emoções. A sensibilidade e os níveis de reação ao tratamento recebido orientam as percepções posteriores que serão construídas pelo próprio indivíduo.

Os dados analisados sugerem que conflitos nas relações interpessoais produzem intensos sentimentos negativos. Raiva é o principal deles, quando relações conflituosas se encaminham para a demissão de funcionários ou para o desligamento de prestadores de serviços com atuação interna. E com raiva, as pessoas tendem a buscar alguma vingança, retaliando as organizações onde vivenciaram desavenças, desrespeito ou desconsideração de superiores ou colegas de trabalho. O Entrevistado 4 relata as seguintes passagens: “É bastante comum a questão de revolta no sentido de vingança, relativo à alguma situação anterior, algum mal-entendido...”; “E aí envolve também a questão do crime contra a honra, injúria, calúnia e difamação”.

Os entrevistados 6 e 13 relatam pequenas histórias onde a forma de tratamento gerou crises no relacionamento interpessoal. No segundo caso, o dano à informação da empresa foi consumado:

Um cara que trabalhava em uma empresa avisou de uma falha de segurança e a empresa não fez nada, não fez nada e ele ficou avisando a empresa, uma falha muito grave. E o que acabou acontecendo é que a diretoria da empresa chamou ele e xingou ele, quando na verdade ele estava ajudando a empresa, ele estava demonstrando para a empresa que eles tinham um problema muito grave. Então, isso é muito relevante. As empresas, quando são confrontadas com falhas, em geral, elas fecham os olhos, ou, quando não fecham, acabam responsabilizando o funcionário de forma incorreta, ou seja, eles descobriram um problema muito grande e eles culpam o funcionário que descobriu isso ainda... (ENTREVISTADO 6).

Eu tenho um caso de um analista de infraestrutura... ele tinha uma atividade para fazer, não realizou, e um dos gerentes da área de engenharia passou um e-mail para ele com cópia para o gerente dele, para o diretor, dando uma esculachada no cara, uma esculachada forte no cara, e dois dias depois uma porrada de pastas desse servidor foram apagadas, as pastas desapareceram. Isso é algo que ficou bem notório. (ENTREVISTADO 13).

4.2 SENTIMENTOS NEGATIVOS

Sentimentos negativos adquiridos pelos indivíduos podem motivar a perpetração do crime cibernético contra organizações, especialmente nos casos em que tais sentimentos foram adquiridos em circunstâncias organizacionais apreendidas, avaliadas subjetivamente e designadas como injustas (WILLISON; WARKENTIN, 2009). Raiva, frustração, mal-estar ou algum tipo de sofrimento emergem na experiência de uma injustiça distributiva, procedimental, interpessoal ou informacional. A literatura prévia elenca sentimentos negativos, os quais foram lembrados pelos participantes da pesquisa. Feelings (1998), em sua obra, cita exemplos, e estabelece cinco principais atributos relacionados aos sentimentos humanos. Damasio e Carvalho (2013), por sua vez, declaram o impacto que essas emoções produzem no comportamento das pessoas.

A baixa-estima, que denota uma avaliação ruim de si mesmo, está presente em trechos das entrevistas dos participantes 2, 6, 7 e 13. O Entrevistado 2 cita problemas relacionados à autoestima criados durante relações conflituosas no trabalho: “Situações onde a pessoa quer se afirmar pessoalmente ou profissionalmente, ela quer mostrar que tem mais conhecimento que o outro. Ah, eu tenho acesso a essa tabela da base de dados... Ah, eu consigo autenticar naquele servidor”; “E baseada nisso, queiram se autopromover”.

Sobre esse sentimento inerente a consciência que o indivíduo tem a respeito de si mesmo, o Entrevistado 6 destaca os trabalhadores do departamento de TI. Na visão dele, essas pessoas têm elementos ou características inerentes a autoestima que podem influenciar sentimentos de injustiça durante relações interpessoais no local de trabalho. Eventuais retaliações à organização são desdobramentos desse processo. “Isso é uma coisa engraçada, mas o cara da TI quer mais um tapa nas costas que diga... Bah, que legal isso aí que tu fizeste” (ENTREVISTADO 6). O mesmo entrevistado complementa sua opinião apresentando a narrativa de uma situação considerada por ele típica no departamento de TI de muitas organizações.

Ninguém reclamava “Eu ganho pouco”. A reclamação sempre é “Não reconhecem aquilo que a gente faz”. A gente se mata, resolve problemas para os caras e os caras não reconhecem aquilo que a gente faz, ou pior, o cara faz, se mata, e vai o gerente

dele dizer lá que ele que fez, ele que resolveu. Aí o pessoal fica bem chateado e eu acho que as empresas não se dão conta disso, pensam que a questão é só salário. (ENTREVISTADO 6).

Na visão do Entrevistado 7, o próprio ambiente de uma grande organização já oferece um modelo de tratamento interpessoal mais objetivo e menos afetivo, embora sustente relações de confiança. Nas pequenas organizações, as interações sociais frequentemente apresentam laços de amizade e intimidade. Tal característica acaba impactando nas percepções do indivíduo. Este, quando se encontra numa condição de baixa-estima, especialmente no contexto das grandes corporações, tem dificuldade para controlar ou reverter percepções de injustiça, as quais podem emergir facilmente como resultado de decisões, procedimentos, tratamentos ou comunicações.

Gerou uma insatisfação ali dentro. Olha, eu vou ser bem sincero com você. Eu não tenho certeza disso aí. Eu já vi situações, eu já trabalhei com um técnico que foi contratado numa empresa menor. Quando ele foi contratado, no caso por nossa empresa, era uma empresa muito maior, uma empresa de nível nacional, então, profissionalmente a gente supõe que a pessoa vai ficar mais satisfeita porque é uma empresa de grande porte e tal, e não foi isso que aconteceu. Na empresa menor ele tinha um tratamento pessoal, ele era tratado como uma pessoa que as empresas pequenas têm condições de tratar. Numa empresa de grande porte você acaba sendo meio que uma matrícula, de certa forma, de uma forma mais grosseira, uma matrícula. Não que a gente trate as pessoas assim, mas a empresa trata a gente assim. E isso é inerente para quem trabalha numa empresa grande. Quem trabalha numa empresa grande sabe que você é mais um dentro daquele grupo todo. (ENTREVISTADO 7).

Os profissionais que trabalham com TI aparecem novamente neste comentário do Entrevistado 13. Ele ressalta que o tratamento oferecido para essas pessoas, com frequência, é equivocado e produz resultados indesejados. Conforme essa visão, existe um explícito desencontro de expectativas, as quais, invariavelmente, quando não atendidas, geram frustração, decepção, ou até revolta nos casos mais problemáticos.

Eu acho que isso é um dos grandes problemas, na verdade, nas áreas de TI, porque a gente vende – e isso é cultural – aquela ideia que o cara de TI é um “geekzão”, é um nerd que fica, exatamente isso, escovando bit, e muitas vezes a impressão que eu tenho, principalmente nas áreas de RH, é que se eu der um *notebook* novo para o cara ele vai morrer de felicidade, e às vezes o cara não quer um *notebook* novo, o cara quer um “Muito obrigado”, um “Valeu”, “Vem cá, tu vais participar junto na reunião”. (ENTREVISTADO 13).

A frustração é uma emoção que se desenvolve quando algo esperado não ocorreu. Quando um objetivo não é atingido. Quando demandas, necessidades ou desejos não são realizados, impedidos por circunstâncias específicas. O Entrevistado 5 relata que situações relacionadas ao local de trabalho, não raro, produzem ou amplificam o sentimento de

frustração. O tamanho dessas sensações, dependendo das características do indivíduo, pode levar a consequências indesejadas, como é o caso do crime cibernético. Neste sentido, o Entrevistado 5 declara uma vivência importante a respeito: “Ele desanima. Ele larga de mão e diz assim... Ah, eu não vou estar me estressando, já me tiraram tudo o que eu tinha, já me tiraram o que eu gostava de fazer; agora não me interessa mais nada. O cara desanima” (ENTREVISTADO 5).

Em uma passagem da narrativa do Entrevistado 16, fica claro o impacto do local de trabalho no sentimento de frustração que é experimentado por alguns *insiders*: “O ambiente de trabalho influencia? Sim, quando o ambiente não dá o retorno que a pessoa espera. Isso é uma percepção pessoal – a pessoa passa aquele sentimento de que você também não merece nada meu” (ENTREVISTADO 16).

A culpa é uma emoção que produz desdobramentos imprevisíveis, especialmente no escopo desta pesquisa. Guilhardi (2002) destaca o papel desse sentimento com profundos desdobramentos sociais. Trata-se de uma consciência penosa de ter descumprido um compromisso social, religioso, afetivo, moral ou institucional. O indivíduo reavalia um comportamento passado e considera-o reprovável. Assim sendo, na visão do Entrevistado 16, ao invés da presença da culpa, exatamente a sua ausência pode fornecer energia para uma motivação criminal no contexto organizacional. “Se uma pessoa não tem medo das consequências e ela não tem sentimento de culpa nenhum, ela vai fazer”. Em outra passagem, o mesmo entrevistado declara:

A minha empresa é uma superempresa; mas se ela fosse uma empresa ruim, eu não ia me sentir culpado. Afinal, ela seria uma porcária, um desastre; eu ia procurar outra, mas eu não ia sentir dívida moral nenhuma com essa empresa. (ENTREVISTADO 16).

Se a organização fornece elementos que desagradam o indivíduo (injustiças distributivas, procedimentais, interpessoais ou informacionais), somados ao fato de que a pessoa não possui gratidão ou reconhecimento de valor perante a empresa, o chefe ou colegas de trabalho, a prática de crimes cibernéticos pode evoluir sem qualquer remorso ou arrependimento. Sem culpa, a pessoa realiza o crime cibernético, conforme ponderou anteriormente o Entrevistado 16.

4.3 MOTIVAÇÕES PARA O CRIME

Diversas motivações para o crime cibernético já foram investigadas em âmbito acadêmico, e as pesquisas sobre o tema estão disponíveis na literatura desenvolvida neste campo (HEATH, 2008; LINDENBERG, 2001; SON, 2011; STANTON et al., 2005; TITTLE; BOTCHKOVAR, 2005; WU; SHUPING; JUNHUA, 2009). Considerando o impacto que o crime cibernético provoca nas organizações, o estudo dos fatores antecedentes e consequentes desse fenômeno, bem como as relações conceituais com o crime tradicional foram trabalhados por diversos autores (CANONGIA; MANDARINO JUNIOR, 2010; CHOO, 2011; JANG-JACCARD; NEPAL, 2014; LEFEBVRE; ACM, 2012).

No Brasil, algumas motivações foram observadas com mais frequência do que outras, conforme estudos sobre o crime cibernético nas organizações brasileiras (TREND-MICRO, 2013; KESSEL; ALLAN, 2014; ALVES; D'ANDREA, 2014; EYGL, 2014b; SCIARRETA, 2014; KASPERSKY-LAB, 2015). Ataques motivados por ganhos financeiros ilícitos ou por vingança aparecem com grande frequência no país. A percepção de que adolescentes e jovens, na condição de *hackers*, estão por trás da maioria dos crimes cibernéticos que ocorre no Brasil é predominante. A mídia costuma reportar esses fatos alegando que sua motivação é dinheiro, retaliação ou até mesmo diversão. Aspectos relacionados às condições sociais de determinados contextos organizacionais ainda é pouco explorada em relação a motivação para os crimes cibernéticos.

Nesta pesquisa, foram levantadas diversas motivações analisadas pela literatura. Após a coleta de dados, o pesquisador analisou as entrevistas buscando identificar essas e outras motivações que pudessem emergir. A vingança foi a motivação que apareceu com mais frequência nas falas dos informantes. Para vários participantes, sentimentos ligados a raiva e frustração, oriundos da percepção de injustiça nas relações interpessoais, motiva trabalhadores a retaliarem sua organização através do crime cibernético. Brigas com o chefe, demissões ou mesmo disputas de poder aparecem como fatores estimuladores da vingança. As passagens abaixo atestam essa visão: “A gente já pegou casos, por exemplo, onde era um cara se vingando ou um cara que sabia que ia ser demitido” (ENTREVISTADO 1); “Saiu mordido, não recebeu o que tinha que receber, o cara se sentiu excluído ou se sentiu injustiçado. E ele, de uma forma ou de outra, disse... Ah, eu vou lá e vou detonar” (ENTREVISTADO 5).

Conforme o Entrevistado 6, “o ambiente de TI é um ambiente um pouco diferente de outros ambientes dentro da empresa, e tem muito essa coisa da vingança; tem muito essa coisa do tratamento, do descontentamento de algumas pessoas”; “São sempre pessoas ligadas à

empresa, e as motivações são, normalmente, vingança”; “Quando tem um contrato com alguém e esse contrato é suspenso, é cancelado, acaba acontecendo esses incidentes”; “Essas situações, por exemplo, em que terceiros se vingaram... o mais graves deles foi um cara que apagou 400 e poucos gigas de *e-mails* em uma empresa... esse cara teve o contrato trocado do dia para a noite”.

Segundo o Entrevistado 15, “foi na sexta-feira de carnaval. Eles tinham uns rádios, ponto a ponto direto com Carazinho... Só que ninguém tinha acesso à senha, nada. Os caras entraram no rádio e apagaram toda a configuração. Apagaram. Quem entrou sabia o que estava fazendo. Não foi um leigo, não foi sem querer”; “Ele sabia o que estava fazendo e sabia o que ia afetar”; “Eles só fizeram isso para dar risada, entendeu? Isso é para sacanagem, porque não tinha mais volta, eles não iam voltar”; “Ah, tu me demitiste, eu vou te mostrar quem manda aqui! Eles derrubaram o rádio. Aí causou um transtorno; um prejuízo...”; “Entraram e sacanearam um pouco no roteador, que era um Linux...”; “Mas isso é tudo na frustração, é tudo na revolta, na realidade é revolta”. O mesmo entrevistado, em sua narrativa, reforça:

Teve um que foi demitido e os caras não fecharam... aí deixaram ele entrar ali para desligar as coisas, ele foi lá e deletou toda a caixa postal dele, tinha um monte de informação ali, aí ele deletou tudo, e deletou toda a pasta do file server dele onde tinha toda a documentação (ENTREVISTADO 15).

A segunda motivação para o crime cibernético que mais foi lembrada pelos informantes é a oportunidade. Em sua tese, Willison (2002) apresenta um modelo denominado Estrutura do Crime Específico de Oportunidade, o qual mapeia elementos formadores da oportunidade para o crime. Ele analisa potenciais infratores em um ambiente de trabalho, considerando que existe uma tomada racional de decisão para o crime, influenciada pelas oportunidades e a respectiva relação de custo e benefício que o contexto oferece num dado momento. Assim, na fala de alguns informantes, um *insider* que eventualmente já adquiriu sentimentos negativos, aproveitando o surgimento de uma oportunidade específica ou explorando uma condição especial relativa ao seu cargo, perpetra um crime cibernético. A seguir, algumas passagens que reforçam essa justificativa.

Então, o acesso é o segundo, quanto mais acesso ela tem, mais, talvez, a oportunidade ou o atrativo fiquem visíveis. Então, tu imaginas que um cara que era um simples gerente passa a ser um diretor financeiro, então, ele tem ali acesso irrestrito aos dados financeiros da empresa, balancetes, acesso a contas corporativas, acesso no SAP onde ele pode lançar ali pagamentos sem que ninguém analise ou valide isso (ENTREVISTADO 3).

O Entrevistado 3 acredita que a oportunidade ganha relevância na medida em que é exposta ao indivíduo. E assim ele declara: “Quando você expõe a pessoa a um atrativo, você aumenta a oportunidade”. O Entrevistado 6 pondera sobre um risco inerente a pessoas que trabalham com a TI na organização: “O cara da TI normalmente tem acesso a tudo, ou no mínimo ele tem acesso a um conjunto de ativos importantes naquele ambiente; e ele se sente com o poder de fazer o que ele bem entender na empresa”. De maneira similar, o Entrevistado 13 opina baseado em suas vivências: “Então, eu acho que o risco, principalmente para TI, ocorre quando eu tenho o fator acesso à informação ou aos meios para executar o crime”; “Teve um caso de uma pessoa do RH que autorizou a si própria um empréstimo que ela não tinha direito. Por quê? Porque ela tinha poder para isso e as ferramentas para isso”. Ainda sobre a questão da oportunidade como elemento motivador para o crime cibernético, o Entrevistado 16 argumenta de acordo com experiências prévias: “O dia em que ele consegue ter uma oportunidade de fazer alguma coisa errada, sem medo de ser pego, ele vai fazer”; “A gente sempre fala que uma ameaça se consolida com três coisas: vontade, oportunidade e capacidade”; “Se o cara tiver a oportunidade, ele pode roubar uma informação confidencial. Se ele está com vontade agora, ele vai fazer. Então, esse ambiente influencia? Sim, influencia”.

Relações pessoais com criminosos influenciam a prática de crimes cibernéticos na visão de alguns participantes. Rebellon et al. (2010) tratam essa questão, inclusive propondo o conceito da vergonha como inibidor da motivação criminal. Essas interações sociais negativas estão dentro da própria organização. *Insiders* podem ser influenciados por outros *insiders*. Normalmente, variáveis de contexto, tais como a situação da empresa ou as práticas usuais de tratamento interpessoal, estimulam alguns indivíduos a cometer crimes cibernéticos na empresa. Por exemplo, segundo o Entrevistado 3 “as pessoas são suscetíveis; são pessoas que dependendo de quem chega na orelha, ela vai pender para um lado ou para o outro. E essas pessoas são um risco ao negócio”; “Se um mal-intencionado chegar nela, vai conseguir manipular e fazer com que essa pessoa seja cúmplice de uma fraude interna”; “Então, aquele cara lá que quer ver o circo pegar fogo percebe o colega... e diz... Viu, não te falei, os caras são sacanas; acho que a gente devia meter a mão mesmo, porque ninguém está nem aí”. O Entrevistado 15 relata que “tinha umas falcatruas. Os caras eram bons, tecnicamente eram bons, só que eles queriam proteger a empresa deles de uma maneira, tipo assim, ninguém podia entrar na panela”.

A associação diferencial estabelece que influências para o comportamento criminal advêm de relacionamentos sociais iniciados fora do contexto organizacional. O principal

constructo dessa abordagem é a Determinação Favorável ao Crime, que pode ser mensurada pelas seguintes variáveis: o grau de supervisão familiar, a intensidade de coesão nos grupos de amizades, a existência de amigos que foram pegos pela polícia, a percepção dos jovens acerca de outros jovens na vizinhança que se envolvem em problemas, e se o jovem mora com os dois pais (CERQUEIRA; LOBÃO, 2003). Esse universo social mais abrangente que produz impacto na motivação criminal acaba gerando desdobramentos importantes no contexto organizacional. Neste sentido, elementos do local de trabalho que geram sentimentos negativos atuam apenas como gatilho para o crime cibernético praticado por indivíduos anteriormente motivados. Nas entrevistas, essa perspectiva ficou saliente: “É, já está no sangue do brasileiro”, alegou o Entrevistado 15. E refletindo sobre uma questão de formação pessoal, o Entrevistado 16 afirma: “Problema de pessoas você resolve com educação, e isso é diferente. E isso entra muito da cultura que a gente tem, de como as pessoas pensam em relação a percepção delas”. E este entrevistado complementa:

Um cara vai fazer aquele velho exemplo da janela quebrada. Eles fizeram um teste, eles pegaram uma vizinhança e quebraram uma janela; a partir do momento em que quebrou uma janela e esse cara não consertou essa janela, todo mundo começou a deixar as coisas quebradas também. Tu crias um padrão de comportamento (ENTREVISTADO 16).

Em um dado momento da sua narrativa, o Entrevistado 16 reforça essa crença: “Já que pode quebrar esse vidro aqui, eu posso quebrar outro também, ninguém conserta”. “Você passa a ter um ambiente onde todo mundo começa a cometer infrações; vira um comportamento padrão, não porque as pessoas são más” (ENTREVISTADO 16).

A impunidade pode ser uma importante motivação para o crime cibernético, na medida em que desperta a sensação de que não haverá a punição ou está será insuficiente, eventual ou branda. Son (2011) corrobora com essa probabilidade ao referenciar a teoria da dissuasão (GTD), que foi desenvolvida para explicar o envolvimento das pessoas com atividades indesejadas mediante um comportamento desviante. A GTD postula que os indivíduos são menos propensos a cometer crimes quando os riscos de serem capturados e punidos aumenta (SON, 2011). A certeza das sanções em caso de violação age como inibidor das práticas ilícitas, na medida em que influencia o comportamento do indivíduo frente a relação entre o custo e o benefício durante a tomada de decisão pelo crime. Essa perspectiva também é discutida por Siponen e Vance (2010) e Willison e Warkentin (2013).

O criminoso vislumbra que haverá apenas ganhos nas violações. Ele utiliza recursos do conceito de Neutralização como justificativa social, conforme estudos de Heath (2008) e

Siponen e Vance (2010). No momento em que a percepção de impunidade é compartilhada por membros de uma organização, uma cultura se estabelece, incentivando pessoas a agir contra as políticas da empresa ou mesmo contra a lei.

O espaço cibernético, desde o princípio, oferece essa percepção de impunidade, aumentada pela sensação de anonimato, tal como evidencia Hunton (2009). É, de certa forma, um ambiente desregulamento, aberto, de difícil controle, repleto de oportunidades para o crime. Essa visão aparece claramente ilustrada nas passagens logo a seguir. “A internet tem muito aquele sentimento de terra sem lei, que aquilo que eu vou fazer na internet não dá nada”; “A legislação brasileira, mesmo com a nova lei, é muito frágil nesse sentido” (ENTREVISTADO 2). Seguindo numa linha de raciocínio parecida, o Entrevistado 8 declara, demonstrando alguma resignação: “Aí está aquilo que eu estava querendo te falar; a questão da ideia tanto da impunidade, como a ideia de que isso não está sendo controlado, que não é feito”; “A minha experiência aqui dentro da empresa é a sensação de impunidade. A sensação de que não vai acontecer nada. Além do mais, toda vez que existe esse tipo de coisa, não existe uma exposição do funcionário, justamente por questões legais” (ENTREVISTADO 8).

5 DISCUSSÃO DOS RESULTADOS

Este capítulo apresenta a discussão dos resultados obtidos a partir das inferências realizadas pelo pesquisador sobre os dados analisados. Entre as categorias consideradas sobre justiça organizacional, sentimentos negativos e motivação para o crime cibernético, foi possível verificar que a literatura revisada já possui referências em trabalhos anteriores. É importante registrar, todavia, que no cenário das organizações brasileiras (escopo dessa investigação), conforme a percepção dos especialistas em segurança cibernética entrevistados, existe uma predominância de alguns tipos específicos de sentimentos negativos. Essas emoções ruins surgem e evoluem a partir da percepção de injustiça organizacional, estimulando, por conseguinte, alguns tipos específicos de motivação para o crime cibernético.

Referente ao constructo Sentimentos Negativos proposto no Modelo Conceitual da Figura 2, não foram identificadas evidências que abordassem, por exemplo, sensações de medo, insegurança, cansaço, ansiedade, aflição, depressão, tédio, solidão, luxúria, ciúmes. Tampouco aqueles relacionados a necessidades ainda mais primárias, tal como fome, sede, frio ou calor (FEELINGS, 1998; MASLOW, 1943). No que tange o constructo Motivação Criminal, igualmente ilustrado na Figura 2, não foram mencionadas pelos entrevistados as seguintes variáveis colhidas da literatura (FEELINGS, 1998): Patriotismo, Fama, Controle Social, Autocontrole, Aprendizagem Social, Adrenalina, Status, Sexo, Religião, Política, Ideologia, Curiosidade, Chantagem e Anomia. Esse resultado chama a atenção, pois algumas dessas variáveis apresentaram relevância na identificação das motivações para o crime cibernético em trabalhos pesquisados durante a revisão da literatura (YAR, 2005; ROGERS; SEIGFRIED; TIDKE, 2006; ARPAD, 2013; WILLISON; WARKENTIN, 2013; EYGL, 2014a). Sem a pretensão de generalizar para o universo da criminalidade cibernética nacional, os fatores que mais se destacaram nas entrevistas foram: Vingança, Ganância, Oportunidade, Associação, Costume, Impunidade, Autoafirmação, Desorganização Social Necessidade e Tensão Social.

É importante reconhecer, todavia, que vários entrevistados atribuíram elementos exclusivamente inerentes ao indivíduo como causas da motivação para o crime cibernético. Para os informantes, patologias individuais seriam as determinantes do comportamento ilegal ou imoral. A pessoa, portadora de tais características, persegue, independentemente de eventuais influências do contexto, atender interesses próprios, ou adquirir vantagens e benefícios para satisfazer suas expectativas individuais. Esta perspectiva sobre motivação foi reconhecida em trabalhos científicos de outras ciências humanas, como é o caso da Psicologia

e das Ciências Sociais. Cita-se, neste caso, Eccles; Wigfield (2002), Eccheli (2008), Campos, (1987), Todorov e Moreira (2005), Ryan e Deci (2000), Deci e Ryan (2000) Deci e Ryan (2008). A relevância de anormalidades psicológicas no âmbito do crime muito influenciou a crença entre gestores organizacionais. As pessoas praticavam crimes porque seriam essencialmente criminosas, cujos traços psicossociais precisariam ser cuidadosamente observados e gerenciados. A estratégia de gestão, neste cenário, restringia-se ao monitoramento, identificação, punição e discriminação dos envolvidos nas violações. O gestor teria papel reativo para fatos distantes do seu controle, pois ainda existe entre os práticos a crença de que o crime cibernético é cometido por pessoas com problemas ou desvios psicológicos, e que elementos contextuais do local de trabalho não influenciam essa relação. Tais entendimentos estão representados em algumas narrativas analisadas no capítulo 4.

Considerando as categorias que emergiram durante o processo de análise de conteúdo (BARDIN, 2006), o pesquisador observa que os principais fatores motivacionais para o crime cibernético no contexto das organizações brasileiras, de acordo com a percepção de especialistas em segurança cibernética, são a vingança e a ganância, com uma participação importante e complementar de elementos relacionados à oportunidade, ao costume, à associação e, principalmente, à impunidade. A expectativa de que não haverá punição se um crime for cometido é um determinante em muitas situações relacionadas ao crime cibernético. O Quadro 8 sintetiza esses relacionamentos analisados.

Quadro 8 – Relação entre os constructos

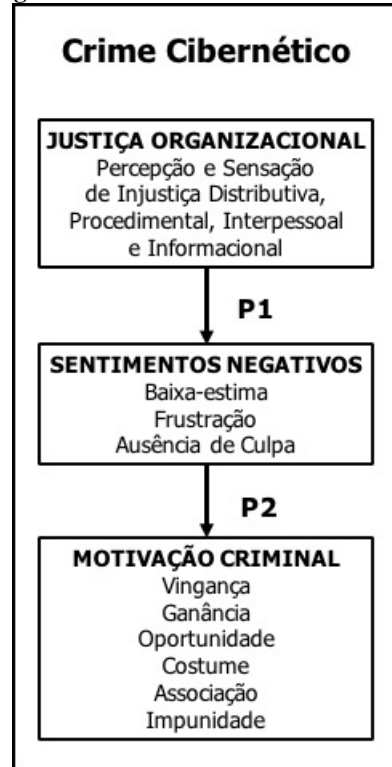
Justiça Organizacional	Sentimentos Negativos	Motivações para o Crime Cibernético
Percepção e Sensação de Injustiça Distributiva, Procedimental, Interpessoal e Informacional.	Baixa-estima Frustração Ausência de Culpa	Vingança Ganância Oportunidade Costume Associação Impunidade

Fonte: elaborado pelo autor (2016)

As relações encontradas e ilustradas no Quadro 8 ajudaram nos ajustes que foram realizados no modelo conceitual da Figura 2. Observa-se que percepções e sensações de injustiça no âmbito distributivo, procedimental, interpessoal e informacional produzem baixa-estima, frustração e podem reduzir o sentimento de culpa dos funcionários em relação a organização. Tais sentimentos estimulam a vingança e a ganância, reforçada por oportunidades, costume, associação ou impunidade no local de trabalho.

Com base nos respectivos sentimentos negativos e as conseqüentes motivações para o crime cibernéticos obtidas na coleta de dados, foi desenvolvido uma nova proposta de modelo conceitual, derivada de um refinamento do modelo original (Figura 2). A principal alteração neste modelo conceitual refinado foi o foco nas variáveis relevantes de cada constructo, conforme ilustra a Figura 8:

Figura 8 – Modelo Conceitual Refinado



Fonte: elaborado pelo autor (2016)

Neste sentido, com base nos resultados dos dados analisados, as seguintes proposições anteriormente propostas sofrem as seguintes alterações para adequação com a realidade organizacional observada pelo pesquisador:

- a) **Proposição 1 (P1):** A percepção de injustiça, no contexto organizacional, produz no indivíduo, sentimentos negativos, tais como a baixa-estima, a frustração e a ausência de culpa;
- b) **Proposição 2 (P2):** Sentimentos negativos, tais como a baixa-estima, a frustração e a ausência de culpa, motivam as pessoas a cometer crimes cibernéticos nas organizações onde trabalham.

6 CONSIDERAÇÕES FINAIS

Esta pesquisa procurou compreender de que maneira as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham. Conforme estudos anteriores, elementos relacionados ao local de trabalho podem desenvolver sentimentos negativos nas pessoas que motivariam a prática criminal. Esses elementos estão relacionados a percepções de injustiça que alguns indivíduos desenvolvem sobre a falta injustificável de equidade em três principais questões organizacionais:

- a) Decisões gerenciais sobre recompensas e reconhecimento (justiça distributiva);
- b) Correção, lisura, retidão, equanimidade, igualdade e imparcialidade de políticas e práticas (justiça procedimental);
- c) Qualidade do tratamento interpessoal predominante no local de trabalho (justiça interpessoal), bem como a maneira como as informações, solicitações e decisões são transmitidas (justiça informacional). A comunicação deve levar em consideração o respeito como valor básico, preservando sempre a honra e a dignidade das pessoas. Soma-se à evidente necessidade de dispor informações precisas, claras, transparentes, adequadas e convenientes.

A influência dos fatores supracitados nos indivíduos em seu local de trabalho é um fenômeno com impacto direto na segurança cibernética e, conseqüentemente, na gestão da maioria das organizações. Por essa razão e pela relevância que os crimes cibernéticos apresentam no mundo dos negócios e na vida das pessoas essa pesquisa objetivou analisar, a partir da percepção de especialistas no tema, de que maneira a injustiça organizacional pode motivar *insiders* a cometer crimes no ambiente cibernético das suas organizações.

Diversos profissionais com experiência na área de segurança cibernética foram contatados. Dentre eles, 16 especialistas aceitaram participar de entrevistas em profundidade, desenvolvidas de forma flexível e interativa, com apoio de um roteiro semiestruturado para a respectiva coleta de dados. Os depoimentos, depois de gravados e transcritos, tiveram seu conteúdo analisado e categorizado. A partir daí, foi possível refinar um modelo conceitual que apresenta a relação entre injustiça organizacional, sentimentos negativos e motivações para a prática de crimes cibernéticos. Assim, foi possível aprofundar o entendimento de que as percepções de injustiça organizacional motivam *insiders* a praticar crimes cibernéticos em retaliação às suas organizações.

A experiência da injustiça distributiva, procedimental, interpessoal ou informacional no âmbito organizacional produz, no *insider*, sentimentos negativos como baixa-estima, frustração e ausência de culpa. Tais sentimentos potencializam motivações relacionadas a prática de crimes cibernéticos. Destacam-se vingança e ganância, com participação complementar de elementos relacionados à oportunidade, ao costume, à associação e, principalmente, à impunidade. Colocando de outra forma, o indivíduo que percebe injustiças organizacionais (distributiva, procedimental, interpessoal ou informacional) adquire sentimentos negativos (baixa-estima, frustração ou ausência de culpa) que produzem desejo de vingança ou estimulam a ganância. Oportunidade, costume, associação e impunidade atuam de forma complementar na motivação criminal.

A compreensão dos motivos que estimulam indivíduos a retaliar sua própria organização contribui para o desenvolvimento de ações gerenciais que reduzam o risco relacionado a segurança cibernética. Esta perspectiva apareceu de forma recorrente nas entrevistas realizadas por este pesquisador. Estratégias que orientem políticas e práticas para a equidade e a justiça na distribuição de recompensas e reconhecimento, em processos organizacionais e nas relações e comunicações interpessoais seriam fatores críticos para que o número de crimes cibernéticos pudesse ser reduzido. Tais iniciativas estariam comprometidas em controlar o surgimento de sentimentos negativos que desencadeiam motivações criminais no local de trabalho. A ideia seria diminuir o descontentamento dos *insiders* para que houvesse condições de reduzir o desejo de retaliação dessas pessoas contra a sua organização.

O pesquisador acredita ter atingido os objetivos da pesquisa quando aprofunda a compreensão deste fenômeno inerente a segurança cibernética no contexto das organizações. Analisando elementos de natureza individual e organizacional, foi possível analisar as relações potencialmente existentes entre variáveis intrínsecas ao ser humano, cujas consequências têm enorme relevância e impacto na segurança da nossa sociedade digital.

6.1 CONTRIBUIÇÕES DA PESQUISA

Atingir a melhor compreensão de um fenômeno com impacto direto na segurança das organizações certamente traz importantes contribuições gerenciais. Adquirir uma visão mais clara sobre elementos do local de trabalho, como é o caso do sentimento de injustiça e as suas consequências na motivação para o crime cibernético, é uma vantagem relevante para organizações que buscam prevenir danos ao invés de remediá-los.

O principal ativo organizacional das empresas está virtualizado: a informação. Adicionalmente, no espaço cibernético estão processos, fluxos, procedimentos, transações, normas, arquivos históricos entre outros documentos inerentes ao negócio. Nada mais crítico do que investir na segurança cibernética desses ativos organizacionais. É vital para uma empresa defender, de maneira eficaz e economicamente eficiente, seu patrimônio físico, material e intelectual das ameaças cibernéticas relacionadas a fraudes, roubos, difamação, chantagem, pornografia, lavagem de dinheiro, violação da propriedade intelectual, terrorismo entre outros crimes. Neste sentido, adquirir conhecimento e, conseqüentemente, habilidades que possibilitem vantagens na gestão dos recursos humanos e da infraestrutura de tecnologia é fator crítico de sucesso em um mercado globalizado e competitivo.

O gestor precisa antecipar, prever e, com base nesse exercício reflexivo, planejar e executar as melhores estratégias conforme os cenários considerados. A capacidade de antecipar um evento, no que tange o crime cibernético perpetrado por *insiders*, se dá mediante a investigação de tendências bem como a análise de atitudes e comportamentos. Um trabalho que, evidentemente, ultrapassa muito as competências puramente técnicas. Trata-se de construir relacionamentos interpessoais positivos, e colaborar pelo desenvolvimento de processos organizacionais e sistemas de distribuição de recompensas e reconhecimentos baseados na justiça, na transparência, na imparcialidade e no respeito a igualmente de direitos. Trata-se também de trabalhar na reversão de situações desfavoráveis, quando circunstâncias específicas provocam frustrações e decepções. O gerenciamento dos conflitos é parte fundamental da gestão da informação e da segurança cibernética.

Ignorar ou desprezar o sentimento de injustiça no contexto organizacional pode representar um risco importante. Não raro, a motivação criminal tem sua origem exatamente nos sentimentos negativos derivados de uma injustiça. Assim sendo, perceber e compreender os valores e as expectativas daqueles que têm acesso a informação e ao patrimônio organizacional é estratégico para que eventuais retaliações e vinganças, encorajadas por sensações de oportunidade, necessidade e impunidade sejam minoradas.

No campo acadêmico, também existe uma contribuição desta pesquisa, mesmo que modesta. A literatura prévia sobre a relação entre as percepções de injustiça no âmbito organizacional e a motivação para o crime cibernético é restrita. Considerando ainda o cenário brasileiro, é praticamente inexistente. A proposta de relacionar aspectos da justiça organizacional e da motivação criminal traz um novo *insight*. A investigação de um escopo específico sobre a problemática da segurança cibernética, com apoio teórico de fundamentos da psicologia, representa um valor agregado para o campo da gestão da informação.

Adicionalmente, o enfoque dado para a questão da motivação criminal deve despertar mudanças em algumas práticas organizacionais, mediante a consideração da importância do fator humano perante o desafio de antecipar crimes cibernéticos. É neste sentido, então, que o pesquisador entende que o resultado deste trabalho colabora com universo acadêmico. A pesquisa exploratória que foi realizada também estimula estudos comprobatórios e quantitativos, os quais poderão validar as particularidades da relação entre justiça organizacional e motivação para o crime cibernético no contexto organizacional brasileiro.

6.2 LIMITAÇÕES DA PESQUISA

O contato prévio com profissionais da área da segurança cibernética foi decisivo para uma adequada coleta de dados sobre os fatores relacionados ao ambiente de trabalho que podem influenciar na motivação para o crime cibernético. Essas pessoas compõem o grupo de profissionais que, desde o surgimento da computação, da Internet e das primeiras ameaças cibernéticas, estão a frente desse tema, trabalhando no seu entendimento e articulação.

Com a evolução e popularização das tecnologias da informação e da comunicação, cada vez mais pessoas e organizações ingressaram no espaço cibernético com as mais diferentes finalidades. Dentre essas finalidades, infelizmente, está o crime. Estudar apenas aspectos técnicos e operacionais sobre segurança cibernética está superado.

O fator humano adquiriu enorme relevância nesse contexto. Prevenir ou remediar crimes cibernéticos exigiu a compreensão de traços psicológicos, características pessoais, questões morais e condições socioambientais. Tal como ocorre em qualquer outro tipo de crime, pessoas estão envolvidas, obrigando a consideração de abordagens teóricas emprestadas das ciências sociais e humanas. Assim sendo, a capacidade de analisar e influenciar atitudes e comportamentos ganha atenção e relevância na pesquisa organizacional e nas práticas de mercado.

Os participantes deste estudo exploratório, com vasta experiência na área de segurança cibernética, relataram histórias, vivências, opiniões e crenças sobre as motivações para o crime cibernético e quais influências estão relacionadas ao local de trabalho. As contribuições foram indiscutivelmente úteis. Porém, é de reconhecimento geral, inclusive dos informantes, das suas limitações nos campos da psicologia, psiquiatria, sociologia ou antropologia. Ficou explícita a necessidade de complementar a coleta de dados com pessoas cuja formação e experiência profissional estejam associadas às ciências humanas e sociais. O pesquisador reconhece que a amostra de informantes possui essa importante limitação. Ela carece da

percepção de profissionais que abordam, com profundidade técnica e científica, a problemática do crime cibernético sob a perspectiva psicossocial do indivíduo. Esses profissionais poderiam contribuir com outras visões desse comportamento nocivo, somando positivamente ao que foi coletado nas entrevistas.

Outra limitação que necessita registro refere-se ao próprio pesquisador, que tampouco possui formação ou experiência prévia em áreas como psicologia, psiquiatria, sociologia ou antropologia. Os processos de coleta e análise dos dados certamente trariam percepções complementares ao considerar perspectivas multidisciplinares, e, possivelmente, ricas, na medida que houvesse possibilidade de contar com a formação e experiência supracitadas.

6.3 SUGESTÕES PARA FUTUROS ESTUDOS

As descobertas realizadas nesta pesquisa podem estimular outros pesquisadores a continuar percorrendo um caminho que ainda necessita ser explorado. O comportamento humano é complexo, dinâmico e imprevisível, e sofre as mais diferentes influências de ordem educacional, social, ética, moral, cultural e temporal.

O crime, seja em âmbito geral ou especificamente no contexto cibernético, é fruto da articulação de um conjunto de elementos de difícil controle e previsão. Estudar esse universo de variáveis, suas causas e consequências no meio organizacional continua sendo um desafio. Práticos esperam desenvolver estratégias e ferramentas cada vez mais eficazes e eficientes para a gestão das suas operações de negócio e, obviamente, para a proteção dos seus ativos intelectuais e organizacionais. O conhecimento produzido na academia é um referencial fundamental para a implantação de soluções cada vez mais inteligentes e inovadoras, capazes de lidar, de maneira holística, com a singularidade e a complexidade dos fenômenos sociais intrínsecos a uma organização.

É neste sentido que o pesquisador sugere a realização de estudos futuros que possam contribuir com o conhecimento no campo da segurança cibernética e da gestão da informação, os quais contemplem os seguintes enfoques de investigação científica:

- a) A validação quantitativa dos resultados aqui apresentados, mediante a coleta de dados estruturados que comprovem, estatisticamente, hipóteses elaboradas a partir da presente pesquisa exploratória;
- b) O local de trabalho apresenta fatores relacionados a justiça organizacional que podem gerar sentimentos negativos, os quais motivam o indivíduo a prática de

crimes cibernéticos. Tais fatores, dependendo do local de trabalho, podem ter diferentes graus de influência? O contexto organizacional poderia ser segmentado, considerando, por exemplo, centros militares, de saúde ou esporte, organizações públicas, assistenciais ou sem fins lucrativos.

REFERÊNCIAS

- AAKER, D. A.; KUMAR, V.; DAY, G. S. **Pesquisa de marketing**. São Paulo: Atlas, 2004.
- AKERS, R. L. et al. Social learning and deviant behavior: a specific test of a general theory. **Am Sociol Rev**, v. 44, n. 4, p. 636-55, Aug, 1979.
- ADAMS, J. S. Inequity in social exchange. **Advances in experimental social psychology**, v. 2, n. 267-299, 1965.
- AGNEW, R. Foundation for a general strain theory of crime and delinquency*. **Criminology**, v. 30, n. 1, p. 47-88, 1992.
- AGUIAR, M. A. F. D. Psicologia aplicada à administração: teoria crítica e a questão ética nas organizações. In: AGUIAR, M. A. F. D. **Psicologia aplicada à administração: teoria crítica e a questão ética nas organizações**: São Paulo: Excellus, 1992.
- AICPA, A. I. O. C. P. A. Consideration of Fraud in a Financial Statement Audit - SAS. **Statements on Auditing Standards**, v. 99, 2002.
- ALVES, F. P.; D'ANDREA, E. R. Uma defesa ultrapassada - Principais resultados da Pesquisa Global de Segurança da Informação 2014 – The Global State of Information Security® Survey 2014. **PricewaterhouseCoopers Brasil Ltda.**, 2014.
- ANDERSON, R. H.; BRACKNEY, R. **Understanding the insider threat**: proceedings a march 2004 workshops. Santa Monica: CA, 2004.
- ANTONACCIO, O.; BOTCHKOVAR, E. V.; C. R. Attracted to crime exploration of criminal motivation among respondents in three european cities. **Criminal Justice and Behavior**, v. 38, n. 12, p. 1200-1221, 2011.
- ARPAD, I. A greater involvement of education in fight against cybercrime. **2nd World Conference on Educational Technology Research**, v. 83, p. 371-377, 2013.
- ARVANITES, T. M.; DEFINA, R. H. Business cycles and street crime. **Criminology**, v. 44, n. 1, p. 139-164, 2006.
- ASHENDEN, D. Information security management: a human challenge? **Information Security Technical Report**, v. 13, n. 4, p. 195-201, 2008.
- ASHTON, Thomas S. **The industrial revolution 1760-1830**: in the hands of a child. London: Oxford University Press, 1966.
- ASSMAR, E. M. L.; FERREIRA, M. C.; SOUTO, S. D. O. Justiça organizacional: uma revisão crítica da literatura. **Psicologia: Reflexão e Crítica**, v. 18, n. 3, p. 443-453, 2005.
- BACKHOUSE, J.; DHILLON, G. Managing computer crime: a research outlook. **Computers & Security**, v. 14, n. 7, p. 645-651, 1995.
- BANDURA, A.; MCCLELLAND, D. C. Social learning theory. 1977.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2006.

BASCH, John; FISHER, Cynthia D. Affective events-emotions matrix: a classification of work events and associated emotions. **School of Business Discussion Papers**, p. 65, 1998.

BAUER, M. W.; GASKELL, G. **Qualitative researching with text, image and sound: a practical handbook for social research**. [s.l.]: Sage, 2000.

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

BECKER, G. S. Crime and punishment: An economic approach. In: BECKER, G. S. (Ed.). **Essays in the economics of crime and punishment**: NBER, 1974. p. 1-54.

BERGAMINI, C. W. Motivação: mitos, crenças e mal-entendidos. **RAE - Revista de Administração de Empresas**, v. 30, n. 2, p. 23-34, 1990.

BERNARD, L. C. et al. An evolutionary theory of human motivation. **Genetic, social, and general psychology monographs**, v. 131, n. 2, p. 129-184, May 2005.

BIES, R. J.; MOAG, J. S. Interactional justice: Communication criteria of fairness. **Research on negotiation in organizations**, v. 1, n. 1, p. 43-55, 1986.

BRASIL. **Ministério Público do Estado de São Paulo**. Nova lei de crimes cibernéticos entra em vigor. 2012a. Disponível em:

<http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%20C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf>.

Acesso em: 15 abr. 2015.

_____. **Casa Civil**. Lei 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da República Federativa do Brasil]. Brasília, DF, n. 232, 03 dez. 2012b. Seção 1, p. 1. Disponível em:

<<http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=03/12/2012>>. Acesso em: 15 abr. 2015.

_____. **Casa Civil**. Lei 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 30 nov. 2012c. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 15 abr. 2015.

_____. **Casa Civil**. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 02 mar. 2016.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS quarterly**, v. 34, n. 3, p. 523-548, 2010.

- BURDEN, K.; PALMER, C. Internet crime. **Computer Law & Security Review**, v. 19, n. 3, p. 222-227, 2003.
- BURT, C. H.; SIMONS, R. L. Self-Control, Thrill Seeking, and Crime Motivation Matters. **Criminal Justice and Behavior**, v. 40, n. 11, p. 1326-1348, 2013.
- CAMPOS, D. M. D. S. **Psicologia da aprendizagem**: Vozes, 1987.
- CAMPOS, L. **Sistema de segurança da informação**: Florianópolis: Visual Books, 2006.
- CANONGIA, C.; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, p. 21-46, 2010.
- CANTOR, D.; LAND, K. C. Unemployment and crime rates in the post-world war II United States: A theoretical and empirical analysis. **American Sociological Review**, v. 50, n. 3, p. 317-332, 1985.
- CAPPELLI, D. M.; TRZECIAK, R. F. Best practices for mitigating insider threat: lessons learned from 250 cases. **RSA Conferences**, 2009.
- CAREGNATO, R. C. A.; MUTTI, R. Pesquisa qualitativa: análise de discurso versus análise de conteúdo. **Texto Contexto Enferm**, v. 15, n. 4, p. 679-84, 2006.
- CARVALHO, S. G. de. O lugar dos sentimentos na ciência do comportamento e na psicoterapia comportamental. **Revista Psicologia-Teoria e Prática**, v. 1, n. 2, 1999.
- CERQUEIRA, D.; LOBÃO, W. **Determinantes da criminalidade**: uma resenha dos modelos teóricos e resultados empíricos. Rio de Janeiro: IPEA, 2003.
- CHIZZOTTI, A. **Pesquisa qualitativa em ciências sociais e humanas**. Petrópolis: Vozes, 2006.
- CHOO, K.-K. R. The cyber threat landscape: Challenges and future research directions. **Computers & Security**, v. 30, n. 8, p. 719-731, 2011.
- CHOUCRI, N.; MADNICK, S.; FERWERDA, J. Institutions for cyber security: international responses and global imperatives. **Information Technology for Development**, v. 20, n. 2, p. 96-121, 2013.
- CHUNG, W. et al. Fighting cybercrime: a review and the Taiwan experience. **Decision Support Systems**, v. 41, n. 3, p. 669-682, 2006.
- COHEN-CHARASH, Y.; SPECTOR, P. E. The Role of Justice in organizations: a meta-analysis. **Organizational Behavior and Human Decision Processes**, v. 86, n. 2, p. 278-321, 11// 2001.
- COLLADO, C. F.; LUCIO, M. D. E. L. P. B.; SAMPIERI, R. H. **Metodologia de pesquisa**. 5. ed. São Paulo: Artmed, 2013.
- COLQUITT, J. A. On the dimensionality of organizational justice: a construct validation of a measure. **Journal of applied psychology**, v. 86, n. 3, p. 386, Jun 2001.

- CRESSEY, D. **Crime: causes of crime.** In: SILLS, D. L. (ed.). **International Encyclopedia of The Social Sciences**, v. 3. The Macmillian Company & The Free Press Ed. 1968.
- CROPANZANA, R.; BOWEN, D. E.; GILLILAND, S. W. The management of organizational justice. **The Academy of Management Perspectives**, p. 34-48, 2007.
- D'ARCY, J.; HOVAV, A. Does one size fit all? Examining the differential effects of is security countermeasures. **Journal of Business Ethics**, v. 89, n. S1, p. 59-71, 2008.
- DAMASIO, A.; CARVALHO, G. B. The nature of feelings: evolutionary and neurobiological origins. **Nat. Rev. Neurosci**, v. 14, n. 2, p. 143-152, 02/print 2013.
- DECI, E. L.; RYAN, R. M. The 'what' and 'why' of goal pursuits: human needs and the self-determination of behavior. **Psychological Inquiry**, v. 11, n. 4, p. 227, 2000.
- _____.; _____. Self-determination theory: A macrotheory of human motivation, development, and health. **Canadian Psychology/Psychologie canadienne**, v. 49, n. 3, p. 182-185, 2008.
- _____.; _____. Self-determination theory. **Handbook of theories of social psychology**, v. 1, p. 416-433, 2011.
- DHILLON, G. Violation of safeguards by trusted personnel and understanding related information security concerns. **Computers & Security**, v. 20, n. 2, p. 165-172, 4 jan. 2001.
- _____.; MOORES, S. Computer crimes: theorizing about the enemy within. **Computers & Security**, v. 20, n. 8, p. 715-723, 12 jan. 2001.
- DODGE, K. A. Attributional bias in aggressive children. **Research Gate**, dec. 1985.
- DRIESSNACK, M.; SOUSA, V. D.; MENDES, I. A. C. Revisão dos desenhos de pesquisa relevantes para enfermagem: parte 3: métodos mistos e múltiplos. **Revista Latino-americana de Enfermagem [online]**, p. 1046-1049, 2007.
- DUIT, R. et al. Mental modelling. **Research in science education in Europe**, p. 166-176, 1996.
- ECCHELI, S. D. A motivação como prevenção da indisciplina. **Educar em Revista**, n. 32, p. 199-213, 2008.
- ECCLES, J. S.; WIGFIELD, A. Motivational beliefs, values, and goals. **Annual Review of Psychology**, v. 53, n. 1, p. 109-132, 2002.
- ENTORF, H.; SPENGLER, H. Socioeconomic and demographic factors of crime in Germany: Evidence from panel data of the German states. **International Review of Law and Economics**, v. 20, n. 1, p. 75-106, 2000.
- EYGL, E. Y. Cyber threat intelligence: how to get ahead of cybercrime. **Insights on Governance, Risk and Compliance**, p. 16, 2014a.
- _____. Overcoming compliance fatigue: reinforcing the commitment to ethical growth. **EY 13th Global Fraud Survey**, p. 28, 2014b.

- FAYOL, H. **Administração industrial e geral**. São Paulo: Atlas, 1970.
- FEELINGS, I. Welfare, stress, and the evolution of feelings. **Advances in the Study of Behavior: stress and behavior**, v. 27, p. 371, 1998.
- FELTEN, E. W. et al. Web spoofing: an internet con game. **Software World**, v. 28, n. 2, p. 6-8, 1997.
- FERNANDO, S. A.; YUKAWA, T. Internal control of secure information and communication practices through detection of user behavioral patterns. **Proceedings of The World Congress on Engineering**, p.1248-1253, 2013.
- FLECK, M. P. de A. O instrumento de avaliação de qualidade de vida da Organização Mundial da Saúde (WHOQOL-100): características e perspectivas. **Ciência & Saúde Coletiva**, v. 5, n. 1, p. 33-38, 2000.
- FLICK, U.; NETZ, S. **Uma introdução à pesquisa qualitativa**. Porto Alegre: Bookman, 2004.
- FREITAS, M. E. D. Contexto social e imaginário organizacional moderno. **Revista de Administração de Empresas**, v. 40, n. 2, p. 6-15, 2000.
- FREUD, S. et al. **Edição standard brasileira das obras psicológicas completas de Sigmund Freud**. São Paulo: Imago, 1970.
- FURNELL, S. Cybercrime: vandalizing the information society. In: LOVELLE, J. M. C. et al. (Ed.). **Web engineering**: Springer, p. 8-16, 2003.
- GALINHA, I. C.; RIBEIRO, J. L. P. Contribuição para o estudo da versão portuguesa da positive and negative affect schedule (PANAS): II–Estudo psicométrico. **Análise Psicológica**, p. 219-227, 2005.
- GARCIA-SERPA, F. A.; MEYER, S. B.; DEL PRETTE, Z. A. P. Origem social do relato de sentimentos: evidência empírica indireta. **Revista Brasileira de Terapia Comportamental e Cognitiva**, v. 5, p. 21-29, 2003.
- GIBSON, W. **Neuromancer**. 1984. New York: Ace, 1995.
- GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.
- GOODE, S.; CRUISE, S. What motivates software crackers? **Journal of Business Ethics**, v. 65, n. 2, p. 173-201, 2006.
- GOULART, F. G. Motivação para o combate. **Coleção Meira Mattos - Revista das Ciências Militares**, n. 12, 2006.
- GREENBERG, J. Organizational justice: yesterday, today, and tomorrow. **Journal of management**, v. 16, n. 2, p. 399-432, 1990.
- GUILHARDI, H. J. Análise comportamental do sentimento de culpa. **Ciência do comportamento: conhecer e avançar**, v. 1, p. 173-200, 2002.

HAIR JR, J. F. et al. **Fundamentos de métodos de pesquisa em administração**: Porto Alegre: Bookman, 2005.

HEATH, J. Business ethics and moral motivation: a criminological perspective. **Journal of Business Ethics**, v. 83, n. 4, p. 595-614, 2008.

HERZBERG, F.; MAUSNER, B.; SNYDERMAN, B. **The motivation to work**. New York: Wiley, 1959.

HINDUJA, S.; PATCHIN, J. Cyberbullying fact sheet: identification, prevention, and response. **Cyberbullying Research Center**. Retrieved January, v. 30, p. 2011, 2010.

_____.; _____. **Bullying beyond the schoolyard**: preventing and responding to cyberbullying. USA: Sage, 2014.

HOLTON, C. Identifying disgruntled employee systems fraud risk through text mining: a simple solution for a multi-billion dollar problem. **Decision Support Systems**, v. 46, n. 4, p. 853-864, mar., 2009.

HOMANS, G. C. **Social behavior**: its elementary forms. [s.l.]: Harcourt, Brace & World, 1961.

HUNTON, P. The growing phenomenon of crime and the internet: a cybercrime execution and analysis model. **Computer Law & Security Review**, v. 25, n. 6, p. 528-535, 2009.

_____. A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, v. 7, n. 3-4, p. 105-113, 2011.

HYMAN, P. Cybercrime: it's serious, but exactly how serious? **Communications of the ACM**, v. 56, n. 3, p. 18-20, 2013.

ISO/IEC_27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary. **International Standard**, 2014.

ITU, I. T. U.-. Definition of cybersecurity. ITU-T X.1205, **Overview of cybersecurity**, 2015.

JAMES, W. **The principles of psychology**. New York: Dover Publications, 1950. Original publicado em 1890.

JANG-JACCARD, J.; NEPAL, S. A survey of emerging threats in cybersecurity. **Journal of Computer and System Sciences**, v. 80, n. 5, p. 973-993, 2014.

JESUS, R. G. D.; ROWE, D. E. O. Organizational justice perceived by teachers of basic, technical and technological education. **RAM. Revista de Administração Mackenzie**, v. 15, n. 6, p. 172-200, 2014.

KANFER, R. Work motivation: new directions in theory and research. **International Review of Industrial and Organizational Psychology**, v. 7, p. 1-53, 1992.

KARLOF, C. et al. Dynamic pharming attacks and locked same-origin policies for web browsers. **Proceedings of the 14th ACM conference on Computer and communications security**, ACM. p. 58-71, 2007.

KASPERSKY-LAB. **Cyberthreat real-time map**. 2015. Disponível em: <<https://cybermap.kaspersky.com/>>. Acesso em: 12 set. 2015.

KAZEMI, A.; TÖRNBLÖM, K. Third-party allocation of rewards: the effects of categorization and request for justice. **Small Group Research**, v. 45, n. 4, p. 435-450, 2014.

KESSEL, P. V.; ALLAN, K. Get ahead of cybercrime: EY's global information security survey. **Insights on Governance, Risk and Compliance**, p. 40, 2014.

KSHETRI, N. The global cybercrime industry: economic, institutional and strategic perspectives. **Springer Science & Business Media**, 2010.

LAUREANO, M. A. P.; MAZIERO, C. A.; JAMHOUR, E. Detecção de intrusão em máquinas virtuais. **5º Simpósio de Segurança em Informática–SSI**. São José dos Campos, p. 1-7, 2003.

LEACH, J. Improving user security behaviour. **Computers & Security**, v. 22, n. 8, p. 685-692, 2003.

LEFEBVRE, R.; ACM. The human element in cyber security: a study on student motivation to act. **Proceedings of the 2012 Information Security Curriculum Development Conference (Infosec Cd '12)**, p. 1-8, 2012.

LINDENBERG, S. Intrinsic motivation in a new light. **Kyklos**, v. 54, n. 2-3, p. 317-342, 2001.

LOMÔNACO, F.; WITTER, G. P. Psicologia da aprendizagem. **Temas básicos de Psicologia**. São Paulo: Pedagógica e Universitária, 1984.

MAGKLARAS, G.; FURNELL, S. A preliminary model of end user sophistication for insider threat prediction in IT systems. **Computers & Security**, v. 24, n. 5, p. 371-380, 2005.

MAIA, L. G. Retaliação em instituição pública – percepção e julgamento: estudo de caso. **ENANPAD**, v. 24, p. 12, 2010.

MALHOTRA, N. K. **Pesquisa de marketing: uma orientação aplicada**. Porto Alegre: Bookman, 2012.

MARSHALL, M. N. Sampling for qualitative research. **Family practice**, v. 13, n. 6, p. 522-526, 1996.

MARTIN, N.; RICE, J. Cybercrime: understanding and addressing the concerns of stakeholders. **Computers & Security**, v. 30, n. 8, p. 803-814, 2011.

MARTINELLI, S. D. C.; BARTHOLOMEU, D. Escala de motivação acadêmica: uma medida de motivação extrínseca e intrínseca. **Avaliação Psicológica**, v. 6, p. 21-31, 2007.

- MASLOW, A. H. A theory of human motivation. **Psychological Review**, v. 50, n. 4, p. 370, 1943.
- MASSARELLA, F. L.; WINTERSTEIN, P. J. Motivação intrínseca e o estado mental Flow em corredores de rua. **Movimento (ESEF/UFRGS)**, v. 15, n. 2, p. 45-68, 2009.
- MAYO, E. **The social problems of an industrial civilization**. Boston: Elton Published, 1945.
- MCGREGOR, D. **The human side of enterprise**. New York: McGraw-Hill Professional, v. 21, p. 166, 1960.
- MCNEELY, B. L.; MEGLINO, B. M. The role of dispositional and situational antecedents in prosocial organizational behavior: An examination of the intended beneficiaries of prosocial behavior. **Journal of applied psychology**, v. 79, n. 6, p. 836, 1994.
- MCQUADE, S. C. **Understanding and managing cybercrime**. Boston: Pearson/Allyn and Bacon, 2006.
- ME, G. L.; SPAGNOLETTI, P.; IEEE. **Situational crime prevention and cyber-crime investigation: the online pedo-pornography case study**. Belgrade: IEEE, p. 1064-1067, 2005.
- MENDONÇA, H. Justiça organizacional, prazer e sofrimento no trabalho: análise de um modelo mediacional. **Revista de administração Mackenzie**, v. 10, n. 4, 2009.
- _____.; MENDES, A. M. Experiências de injustiça, sofrimento e retaliação no contexto de uma organização pública do Estado de Goiás. **Psicol Estud**, v. 10, p. 489-98, 2005.
- _____.; TAMAYO, Á. Valores pessoais e retaliação organizacional: estudo em uma organização pública. **RAC-Eletrônica, Curitiba**, v. 2, n. 2, p. 189-200, 2008.
- MERTON, R. K. Social structure and anomie. **American Sociological Review**, v. 3, n. 5, p. 672-682, 1938.
- MILLS, R. F. et al. A scenario-based approach to mitigating the insider threat. **ISSA Journal**, may 2011.
- MOON, B.; MCCLUSKEY, J. D.; MCCLUSKEY, C. P. A general theory of crime and computer crime: an empirical test. **Journal of Criminal Justice**, v. 38, n. 4, p. 767-772, jul. 2010.
- MOREIRA, M. A. Modelos mentais. **Investigações em Ensino de Ciências**, v. 1, n. 3, p. 193-232, 1996.
- MORGAN, G.; GREGORY, F.; ROACH, C. **Images of organization**. USA: Sage, 1997.
- MOTTA, F. C. P.; VASCONCELOS, I. F. Gouveia de. **Teoria geral da administração**, São Paulo: Cengage Learning, 2002.
- MURRAY, E. J. **Motivation and emotion**. New Jersey: Prentice-Hall Englewood Cliffs, 1964.

- MYERS, M. D. **Qualitative research in business and management**. USA: Sage, 2013.
- NEUMANN, P. G. Risks of insiders. **Commun. ACM**, v. 42, n. 12, p. 160, 1999.
- NING, P.; JAJODIA, S.; WANG, S. Intrusion detection in distributed systems: an abstraction-based approach. **Springer Science & Business Media**, 2004.
- NYKODYM, N.; TAYLOR, R.; VILELA, J. Criminal profiling and insider cyber crime. **Science Direct**, v. 2, n. 4, p. 261-267, 2005.
- OXFORD Dictionaries. **Definition of cyberspace**. Disponível em: <http://www.oxforddictionaries.com/us/definition/american_english/cyberspace>. Acesso em: 10 jun. 2015.
- PADMAVATHI, D. G.; SHANMUGAPRIYA, M. A survey of attacks, security mechanisms and challenges in wireless sensor networks. **International Journal of Computer Science and Information Security**, v. 4, n. 1, 2009.
- PARTON, T. B., WILLIAM; SOMMER, PETER;. Cybercrime: protecting against the growing threat - Global Economic Crime Survey. **PricewaterhouseCoopers Brasil Ltda.**, 2011.
- PASCHOA, S.; ZANEI, S. S. V.; WHITAKER, I. Y. Qualidade de vida dos trabalhadores de enfermagem de unidades de terapia intensiva. **Acta Paul Enferm**, v. 20, n. 3, p. 305-310, 2007.
- PENNING, N. et al. Mobile Malware security challenges and cloud-based detection. **Proceedings of the 2014 International Conference on Collaboration Technologies and Systems (Cts)**, p. 181-188, 2014.
- PERVIN, L. A.; JOHN, O. P. **Personalidade: teoria e pesquisa**. São Paulo: Artmed, 2008.
- PETRI, H.; GOVERN, J. **Motivation: theory, research, and application**. São Paulo: Cengage Learning, 2012.
- PFLEEGER, S. L.; CAPUTO, D. D. Leveraging behavioral science to mitigate cyber security risk. **Computers & Security**, v. 31, n. 4, p. 597-611, 2012.
- PRATT, T. C.; CULLEN, F. T. The empirical status of Gottfredson and Hirschi's general theory of crime: a meta-analysis. **Criminology**, v. 38, n. 3, p. 931-964, 2000.
- PRESTES, F. C. M. **Teoria geral da administração: uma introdução**. São Paulo: Pioneira, 1972.
- PRICEWATERHOUSECOOPERS. **Managing cyber risks in an interconnected world: key findings from the global state of information security® survey 2015**. PwC, 2014.
- PRODANOV, C. C.; DE FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

PYSZCZYNSKI, T.; GREENBERG, J.; SOLOMON, S. Why do we need what we need? a terror management perspective on the roots of human social motivation. **Psychological Inquiry**, v. 8, n. 1, p. 1, 1997.

QSR International. **Nvivo for Mac**. Disponível em: <<http://www.qsrinternational.com/>>. Acesso em: 05 jan. 2016.

RADBRUCH, G.; MONCADA, L. C. de. **Filosofia do direito**. Coimbra: Amado, 1961.

RASMI, M.; JANTAN, A. A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics. **4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)**, v. 11, p. 540-547, 2013.

RAYMAN, N. The world's top 5 cybercrime hotspots. **Time**, 2014.

REBELLON, C. J. et al. Anticipated shaming and criminal offending. **Journal of Criminal Justice**, v. 38, n. 5, p. 988-997, 2010.

REGO, A.; SOUTO, S. A percepção de justiça como antecedente do comprometimento organizacional: um estudo luso-brasileiro. **Revista de Administração Contemporânea**, v. 8, n. 1, p. 151-177, 2004.

RIBEIRO, J. A.; BASTOS, A. V. B. Comprometimento e justiça organizacional: um estudo de suas relações com recompensas assimétricas. **Psicologia: Ciência e Profissão**, v. 30, p. 4-21, 2010.

RICHARDSON, R. CSI computer crime and security survey. **Computer Security Institute**, v. 1, p. 1-30, 2008.

ROBINSON, S. L.; BENNETT, R. J. A typology of deviant workplace behaviors: a multidimensional scaling study. **Academy of management journal**, v. 38, n. 2, p. 555-572, 1995.

ROGERS, M. K. A two-dimensional circumplex approach to the development of a hacker taxonomy. **Digital Investigation**, v. 3, n. 2, p. 97-102, 2006.

_____.; SEIGFRIED, K.; TIDKE, K. Self-reported computer criminal behavior: a psychological analysis. **Digital Investigation**, v. 3, p. 116-120, 2006.

RYAN, R. M.; DECI, E. L. Intrinsic and extrinsic motivations: classic definitions and new directions. **Contemporary Educational Psychology**, v. 25, n. 1, p. 54-67, 2000.

_____.; _____. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. **American psychologist**, v. 55, n. 1, p. 68, 2000.

SALEM, O.; HOSSAIN, A.; KAMALA, M. Awareness program and ai based tool to reduce risk of phishing attacks. Computer and Information Technology (CIT), **IEEE 10th International Conference**, 2010.

SAMPAIO, J. dos R. O Maslow desconhecido: uma revisão de seus principais trabalhos sobre motivação. **Revista de Administração da Universidade de São Paulo**, v. 44, n. 1, 2009.

SCHWARZ, N.; CLORE, G. L. Feelings and phenomenal experiences. **Social psychology: handbook of basic principles**, v. 2, p. 385-407, 1996.

SCIARRETA, T. Brasil perde até US\$ 8 bilhões com crime cibernético. **Folha de São Paulo**, 2014.

SÊMOLA, M. **Gestão da segurança da informação**. Rio de Janeiro: Elsevier, 2003.

SILVA, A. M. M. da; OLIVEIRA G. A. de; CARVALHO, D. Papel das dimensões da justiça organizacional distributiva, processual, interpessoal e informacional na predição do Burnout. **Revista de Administração Mackenzie**, v. 6, n. 1, 2008.

SILVA NETTO, A. da; SILVEIRA, M. A. P. da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375-397, 2007.

SILVA, Juscelino. **A justiça na cidade**. Joinville/SC: Clube de Autores, 2010.

SILVEIRA, D. C. **Os sentidos da justiça em Aristóteles**. Porto Alegre: EDIPUCRS, 2001.

SIMONS, T.; ROBERSON, Q. Why managers should care about fairness: the effects of aggregate justice perceptions on organizational outcomes. **Journal of Applied Psychology**, v. 88, n. 3, p. 432, 2003.

SIPONEN, M.; VANCE, A. Neutralization: new insights into the problem of employee information systems security policy violations. **MIS quarterly**, v. 34, n. 3, p. 487, 2010.

_____. An analysis of the traditional IS security approaches: implications for research and practice. **European Journal of Information Systems**, v. 14, n. 3, p. 303-315, 2005.

SKARLICKI, D. P.; FOLGER, R. Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. **Journal of applied Psychology**, v. 82, n. 3, p. 434, 1997.

SKINNER, B. F. O lugar do sentimento na análise do comportamento. Tradução de Al Néry. **Questões recentes na análise do comportamento**, Campinas: Papyrus, p. 13-24, 1995.

_____. **Sobre o behaviorismo**. Tradução de Maria da Penha Villalobos. São Paulo: Cultrix/EDUSP, 1982. Trabalho original publicado em 1974.

_____. **Reflections on behaviorism and society**. São Paulo: Prentice-Hall, 1978.

SMAHA, S. E. Haystack: An intrusion detection system. Aerospace Computer Security Applications Conference, **IEEE**, p. 37-44, 1988.

SMITH, P. K. et al. Cyberbullying: Its nature and impact in secondary school pupils. **Journal of Child Psychology and Psychiatry**, V. 49, n. 4, p. 376-385, 2008.

SMITTON, J. A. **Motivation and adjustment and story sequence analysis**. Vancouver: University of British Columbia, 1993.

- SOLMS, R. V.; NIEKERK, J. V. From information security to cyber security. **Computers & Security**, v. 38, p. 97-102, 2013.
- SON, J.-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. **Information & Management**, v. 48, n. 7, p. 296-302, 2011.
- SPAFFORD, E. H. Computer viruses as artificial life. **Artificial Life**, v. 1, n. 3, p. 249-265, 1994.
- STANTON, J. M. et al. Analysis of end user security behaviors. **Computers & Security**, v. 24, n. 2, p. 124-133, 2005.
- STEERS, R. M.; MOWDAY, R. T.; SHAPIRO, D. L. Introduction to special topic forum: the future of work motivation theory. **The Academy of Management Review**, v. 29, n. 3, p. 379-387, 2004.
- SUTHERLAND, E. H.; SCHUESSLER, K. **On analyzing crime**. Chicago: University of Chicago/Press Chicago, 1973.
- SYKES, G. M.; MATZA, D. Techniques of neutralization: A theory of delinquency. **American sociological review**, v. 22, n. 6, p. 664-670, 1957.
- SYMANTEC. **Internet security threat report**, v. 20, p. 119, 2015.
- SZOR, P. **The art of computer virus research and defense**. São Paulo: Pearson Education, 2005.
- TAYLOR, George R. **The transportation revolution, 1815-60**. New York: Harper Toachbooks, 1951.
- THEOHARIDOU, M. et al. The insider threat to information systems and the effectiveness of ISO17799. **Computers & Security**, v. 24, n. 6, p. 472-484, 2005.
- THORNBERRY, T. P. Toward an interactional theory of delinquency. **Criminology**, v. 25, p. 863, 1987.
- THORNDIKE, E. L. **Animal intelligence: experimental studies**. London: Macmillan, 1911.
- TITTLE, C. R.; BOTCHKOVAR, E. V. Self-control, criminal motivation and deterrence: an investigation using russian respondents. **Criminology**, v. 43, n. 2, p. 307-353, 2005.
- TODOROV, J. C.; MOREIRA, M. B. O conceito de motivação na psicologia. **Revista Brasileira de Terapia Comportamental e Cognitiva**, v. 7, n. 1, p. 119-132, 2005.
- TOGNETTA, L. R. P. Educação dos sentimentos: um caminho para a paz. **Revista de Educação do Cogeime**, v. 27, p. 23-32, 2005.
- TOURINHO, E. Z.; TEIXEIRA, E. D. R.; MACIEL, J. M. Fronteiras entre análise do comportamento e fisiologia: Skinner e a temática dos eventos privados. **Psicologia: Reflexão e Crítica**, v. 13, n. 3, p. 425-434, 2000.

TREND-MICRO. Cybersecurity challenges faced by a fast-growing market economy. **Organization of American States and Trend Micro Incorporated**, p. 35, 2013.

TUNLEY, M. Need, greed or opportunity? An examination of who commits benefit fraud and why they do it. **Secur J**, v. 24, n. 4, p. 302-319, 2011.

TZU, S. **A arte da guerra**. Traduzido por Sueli Barros Cassal, Porto Alegre, LPM, 2009.

VASHISTH, A.; KUMAR, A. Corporate espionage: the insider threat. **Business Information Review**, v. 30, n. 2, p. 83-90, 2013.

VIVO, M. de; VIVO, G. O. de; ISERN, G. Internet security attacks at the basic levels. **ACM SIGOPS Operating Systems Review**, v. 32, n. 2, p. 4-15, 1998.

WARKENTIN, M.; WILLISON, R. Behavioral and policy issues in information systems security: the insider threat. **European Journal of Information Systems**, v. 18, n. 2, p. 101-105, 2009.

WEBER, M.; BARBOSA, R.; BARBOSA, K. E. **Economia e sociedade: fundamentos da sociologia compreensiva**. Brasília: Universidade de Brasília, 1994.

WELLS, J. T. Why Employees Commit Fraud It's either greed or need. **Journal of Accountancy**, v. 191, n. 2, p. 89-92, 2001.

WIERZBICKA, A. Human emotions: universal or culture-specific? **American Anthropologist**, v. 88, n. 3, p. 584-594, 1986.

WILLISON, R. Considering the offender: addressing the procedural stages of computer crime in an organisational context. **Emerald Insight**, v. 19, n. 2, 2005.

_____. Understanding the offender/environment dynamic for computer crimes. **Information Technology & People**, v. 19, n. 2, p. 170-186, 2006.

_____.; SIPONEN, M. Overcoming the insider. **Communications of the ACM**, v. 52, n. 9, p. 133, 2009.

_____.; WARKENTIN, M. Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organisational justice. Proceedings of the IFIP TC8 International Workshop on Information Systems Security Research. **International Federation for Information Processing**, p. 127-144, 2009.

_____. Beyond deterrence: An expanded view of employee computer abuse. **Mis Quarterly**, v. 37, n. 1, p. 1-20, 2013.

WOMACK, J. P.; JONES, D. T. **A máquina que mudou o mundo**. Rio de Janeiro: Gulf Professional Publishing/Elsevier, 2004.

WU, P.; SHUPING, Y.; JUNHUA, C. Recognizing intrusive intention and assessing threat based on attack path analysis. **Multimedia Information Networking and Security, MINES'09**, p. 450-453, 2009.

_____.; ZHIGANG, W.;_____. Research on attack intention recognition based on graphical model. Information Assurance and Security, 2009. **IAS'09**. Fifth International Conference IEEE, p.360-363, 2009.

YAR, M. The novelty of 'cybercrime' - An assessment in light of routine activity theory. **European Journal of Criminology**, v. 2, n. 4, p. 407-427, 2005.

YEARWOOD, D. L.; KOINIS, G. Revisiting property crime and economic conditions: an exploratory study to identify predictive indicators beyond unemployment rates. **The Social Science Journal**, v. 48, n. 1, p. 145-158, 2011.

APÊNDICE A - TERMO DE SIGILO

Curso: MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS - FACE

Tema da Pesquisa: A INFLUÊNCIA DO AMBIENTE ORGANIZACIONAL NA MOTIVAÇÃO PARA PRÁTICA DE CRIMES CIBERNÉTICOS

Pesquisador Responsável: Plínio Silva de Garcia

Instituição: Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS

Orientadora: Profa. Dra. Marie Anne Macadar Moron

Telefone para contato: (51) 9259-8134 / **E-mail:** plinio@wwworking.com.br

Prezado (a) Sr (a):

Data: / /

O Sr (a) está participando de uma pesquisa científica. As informações fornecidas serão tratadas com total sigilo, sendo utilizadas apenas para fins acadêmicos. O pesquisador esclarecerá todas as dúvidas antes de iniciar.

No relatório final, serão apresentados dados gerais, análises e resultados, sem a identificação ou nomeação de pessoas, empresas, produtos ou marcas registradas. Materiais complementares (gravações, anotações) serão igualmente protegidos de qualquer divulgação sem a prévia autorização do respectivo entrevistado (a) participante da pesquisa.

Plínio Silva de Garcia
Mestrando 2014/16 - FACE / PUCRS

Entrevistado (a): _____
Ciente e de pleno acordo

APÊNDICE B - INSTRUMENTO DE PESQUISA

Data: ___ / ___ / 2016.

- Nome do Entrevistado (a): _____
- Experiência Profissional (em anos): _____
- Experiência com segurança cibernética (em anos): _____

ROTEIRO DE ENTREVISTA

No campo da segurança cibernética, as organizações necessitam adotar uma abordagem proativa. Analisar a conduta das pessoas, e não somente aspectos de TI, possibilita um melhor entendimento dos crimes cibernéticos. Sentimentos negativos, como é o caso do **descontentamento**, impactam na motivação das pessoas para o crime.

Eventuais ações retaliatórias que ocorrem no ambiente de trabalho produzem prejuízos financeiros, sociais e organizacionais. O que leva os trabalhadores a retaliar a sua empresa ou as pessoas que fazem parte dela através do crime cibernético?

Variados são os **sentimentos negativos** que uma pessoa pode adquirir no local de trabalho. Tais sentimentos se desenvolvem em consequência de fatos ocorridos (fatores estimuladores) que produzem impacto direto na vida dos indivíduos. Esses fatos estimulam os sentimentos negativos de forma decisiva (correspondem a causa desses sentimentos) ou de forma coadjuvante (fazem parte da causa desses sentimentos).

QUESTÕES PARA REFLEXÃO E DISCUSSÃO

- Você avalia que crimes cibernéticos possam ser motivados por **sentimentos negativos** no ambiente de trabalho?
 - ✓ Como? Justifique e inclua sua opinião e vivências como profissional.

- Você avalia que a ocorrência de crimes cibernéticos, no ambiente de trabalho, depende de **sentimentos negativos**?
 - ✓ De que forma? Justifique e inclua sua opinião e vivências como profissional.

- Quais os **tipos de sentimentos negativos** que você identifica como maiores causadores de crimes cibernéticos no ambiente de trabalho?
 - ✓ Cite os respectivos sentimentos negativos, elencando-os.
 - ✓ Apresente exemplos inerentes as suas vivências profissionais.

- Quais os **fatores estimuladores**, no ambiente de trabalho, que você identifica como elementos capazes de motivar a prática de crimes cibernéticos?
 - ✓ Cite exemplos conforme suas vivências profissionais.
 - ✓ Quais desses fatores são os mais relevantes?
 - ✓ Quais são os mais frequentes? Por que?

- É possível **identificar pessoas ou grupos**, no ambiente de trabalho, cujos sentimentos negativos sejam suficientes para motivar a prática de crimes cibernéticos?
 - ✓ Como? Justifique e inclua sua opinião e vivências como profissional.

- De que forma líderes e gestores podem contribuir para a redução desses **fatores estimuladores** e, conseqüentemente, os tais **sentimentos negativos** adquiridos ou experimentados no local de trabalho?
 - ✓ Quais estratégias que já funcionaram conforme a sua vivência profissional?
 - ✓ Quais deram errado? Por que?

APÊNDICE C - AMEAÇAS CIBERNÉTICAS

Conforme definições propostas por Szor (2005) e outros autores identificados na literatura prévia, uma coleção de ameaças cibernéticas predominantes nas ocorrências de crimes cibernéticos estão relacionadas abaixo:

- a) ***Virus*** é um código que recursivamente replica uma cópia de si mesmo, infectando arquivos ou sistemas hospedeiros.
- b) ***Worms*** correspondem a uma categoria de vírus que se desenvolve no ambiente da rede de computadores, multiplicando-se com ou sem a interferência dos usuários.
- c) ***Logic bombs*** são programações de código defeituosas normalmente inseridas em uma aplicação legítima, cuja função é realizar algum tipo de ação maliciosa assim que as aplicações legítimas forem executadas.
- d) ***Trojan Horses*** são programas que tentam despertar o interesse do usuário com algum apelo interessante de maneira que sejam executados e que produzam alguma consequência maliciosa complementar.
- e) ***Backdoors*** são ferramentas que abrem portas de acesso ao sistema através das quais atacantes podem realizar, maliciosamente, conexões remotas.
- f) ***Exploits*** são códigos desenvolvidos para conceder acessos indevidos ou mesmo produzir danos através da exploração de vulnerabilidades conhecidas e existentes em sistemas ou aplicações.
- g) ***Rootkits*** são construtores de vírus, tais como o VLC (*Virus Creation Laboratory*), cuja função é produzir novos vírus de computador de forma automatizada e amigável, inclusive para usuários iniciantes.
- h) ***Spammers*** são programas utilizados para enviar mensagens indesejadas para o serviço de correio eletrônico, grupos de notícias ou mensagens instantâneas. O conteúdo dessas mensagens pode variar entre propagandas, pornografia, boatos, download de vírus ou *backdoors*.
- i) ***Keyloggers*** coletam os dados digitados pelos usuários (nomes, senhas, códigos de acesso, números de cartões ou documentos, etc.) e remetem para atacantes remotos.

- j) ***Flooders*** são os ataques de negação de serviço, ou *denial of service* (DoS), são geradores de grandes volumes de tráfego de rede cujo objetivo é saturar a capacidade de processamento e encaminhamento de computadores, servidores e outros dispositivos de rede. Essa inundação de dados parte, simultaneamente, de dezenas, centenas ou milhares de computadores comprometidos (máquinas zumbi) que desempenham a função de um ataque coordenado e distribuído.
- k) ***Spywares* ou *adwares*** estão interessados no comportamento das pessoas na Internet. Usualmente patrocinados por empresas que desejam saber o que as pessoas estão fazendo, pesquisando ou comprando na rede, esses programas coletam informações, não raro sem a expressa permissão dos usuários, e remetem para empresas que as utilizam em suas estratégias de marketing e vendas.
- l) ***Phishing* e *vishing*** são definidos pelo grupo de trabalho *anti-phishing* (APWG) como "um ataque que usa tanto a engenharia social e como técnicas de subterfúgio para roubar dados de identidade pessoal dos consumidores e credenciais de contas financeiras" (SALEM; HOSSAIN; KAMALA, 2010). Conforme os autores, o primeiro está relacionado ao roubo de informações virtuais enquanto que o segundo foca no roubo de comunicações de voz na Internet. Em um ataque de *phishing* mais sofisticado, conhecido como *pharming*, o adversário subverte o sistema de nomes da Internet (DNS), redirecionando o acesso da vítima para um endereço controlado pelo atacante onde, provavelmente, ocorrerá a captura indevida de informações sensíveis (KARLOF et al., 2007).
- m) ***Spoofing***, em especial aquele relacionado a *World Wide Web*, permite que um invasor falsifique endereços de forma que os dados que a vítima envia para a Internet sejam, primeiramente, canalizados através de uma máquina ou dispositivo de rede controlado pelo invasor. Isso permite que o invasor tenha acesso e ciência de todas as atividades da vítima, coletando e analisando os dados que interessam (senhas, números de documentos, credenciais de acesso, etc) (FELTEN et al., 1997). Esse invasor também pode enviar dados falsos para a Internet em nome da vítima e vice-versa.
- n) ***Sniffing*** representa o uso de uma interface de rede (um acesso físico que determinado dispositivo tem em uma rede de computadores) em uma modalidade denominada promíscua para receber indevidamente dados que foram enviados, originalmente, para outros destinos (VIVO; VIVO; ISERN, 1998). Desta forma, é

possível capturar informações alheias, sem autorização e conhecimento prévios das pessoas ou dos equipamentos envolvidos na comunicação. Esses dados normalmente têm caráter privado e sigiloso, como é o caso das senhas de acesso a qualquer sistema. Especificamente no escopo das variadas formas de assédio, emerge com forte e contemporâneo impacto social e cultural o denominado *bullying* cibernético ou *cyberbullying*. Tal prática engloba a publicação ou distribuição virtual de comentários prejudiciais, ameaças, rumores, imagens ou vídeos sobre as vítimas dessa violência social.

- o) ***Cyberbullying*** descreve atos repetitivos e agressivos que são realizados por um indivíduo ou grupo, através da Internet, contra pessoas que não conseguem se defender (SMITH et al., 2008). Utilizando computadores, celulares ou outros dispositivos eletrônicos, agressores violam a lei e realizam, deliberada e repetidamente, crimes contra a pessoa mediante a prática de assédio, ameaça ou perseguição (HINDUJA; PATCHIN, 2010; 2014).