Rodrigo Sanches Miani

Um estudo sobre métricas e quantificação em segurança da informação

Campinas
2013

Universidade Estadual de Campinas

Faculdade de Engenharia Elétrica e de Computação

Rodrigo Sanches Miani

Um estudo sobre métricas e quantificação em segurança da informação

Tese de doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas para obtenção do título de Doutor em Engenharia Elétrica na área de Telecomunicações e Telemática.

Orientador: Prof. Dr. Leonardo de Souza Mendes
Co-orientador: Prof. Dr. Bruno Bogaz Zarpelão

Este exemplar corresponde à versão final da tese defendida pelo aluno Rodrigo Sanches Miani e orientada pelo Prof. Dr. Leonardo de Souza Mendes

---

Campinas
2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

M58e

Miani, Rodrigo Sanches, 1983-
Um estudo sobre métricas e quantificação em segurança da informação / Rodrigo Sanches Miani. – Campinas, SP : [s.n.], 2013.

Orientador: Leonardo de Souza Mendes.
Coorientador: Bruno Bogaz Zarpelão.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Pesquisa quantitativa. 2. Redes de computadores - Medidas de segurança. 3. Sistemas de segurança. I. Mendes, Leonardo de Souza,1961-. II. Zarpelão, Bruno Bogaz. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: On the use of metrics and quantification in information security
Palavras-chave em inglês:
Quantitative research
Computer networks - Security metrics
Security systems
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora:
Leonardo de Souza Mendes [Orientador]
Leonardo Barbosa e Oliveira
Ana Paula Resende Malheiro
Marco Aurélio Amaral Henriques
Paulo Cardieri
Data de defesa: 28-06-2013
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Rodrigo Sanches Miani

Data da Defesa: 28 de junho de 2013

Título da Tese: "Um Estudo Sobre Métricas e Quantificação em Segurança da Informação"

Prof. Dr. Leonardo de Souza Mendes (Presidente): _____

Prof. Dr. Leonardo Barbosa e Oliveira: _____

Dra. Ana Paula Resende Malheiro: _____

Prof. Dr. Marco Aurélio Amaral Henriques: _____

Prof. Dr. Paulo Cardieri: _____

Agradecimentos

A Deus.

A minha esposa e companheira Elisa. Obrigado pelos conselhos, pelo carinho, pela paciência e por compartilhar a sua vida comigo. Só nós sabemos o quanto tudo isso foi difícil mas também o quanto foi imensamente prazeroso. Que venham novos sonhos e projetos em nossa vida.

A toda a minha família. Em especial aos meus pais João e Rosa e a minha irmã Camila. Desde o primeiro ano de faculdade no momento em que saí de casa vocês sempre me apoiaram. Enfim a jornada terminou. Isso mostra que a dedicação e o sacrifício feito para educar os filhos é uma atitude exemplar, a qual serei eternamente grato e levarei como inspiração para a minha vida.

Ao meu orientador Prof. Dr. Leonardo de Souza Mendes pela confiança depositada, pelas inúmeras oportunidades e por todo o suporte dado ao longo do mestrado e doutorado.

Ao meu amigo, padrinho e co-orientador Prof. Dr. Bruno Bogaz Zarpelão pela oportunidade única de trabalhar com um profissional extremamente competente e dedicado. A direção do trabalho, assim como da carreira que escolhi trilhar foi influência direta de seus sempre pertinentes conselhos ao longo dos anos. Foi um grande privilégio trabalhar com você. Espero que a nossa parceria continue por muito tempo!

Aos amigos de Bauru por todos os bons momentos (churrascos!!) que de certa forma auxiliaram nessa caminhada: Vinícius, Rafael, Bruno, Marjory, Mika, Fábio e Erick.

Aos meus familiares de Bauru, em especial aos tios André e Silmara por todo o incentivo

e ajuda desde os primeiros anos da graduação.

Aos amigos e companheiros de república (G2): Cris, Paulinho e Bacalhau. Obrigado pela grande força e pelos momentos de descontração!

Aos amigos de São Carlos, turma Matemática 2002 - UFSCar. Em especial aos companheiros Fabrício (Tofu), Henrique (Xis) e Gustavo (Lobão). As conversas sobre estatística ajudaram muito no desenvolvimento do trabalho. Obrigado Lobo!

Aos grandes amigos de Campinas que por muito tempo foram minha segunda família durante o mestrado e doutorado: Henrique, Andreza, Jú, Andréa, Gean, Maurício, Felipe, Alexandre, Dherik, Éder, Liniquer, Alda, Régis e Ingrid.

Ao Prof. Michel Cukier pelo aprendizado e acolhimento no período de sanduíche nos EUA. Aos colegas de trabalho do CyQL: Yan e Danielle. Em especial ao amigo Bertrand pelo companheirismo e hospitalidade que ajudaram a diminuir a saudade das terras brasileiras.

Ao CAIS/RNP e à University of Maryland, pelo apoio e disposição com as informações disponibilizadas.

À FEEC/Unicamp pela estrutura e ótimo ambiente de trabalho que oferece aos estudantes e pesquisadores.

Aos membros da banca corretora pelas valiosas sugestões e dicas dadas durante o desenvolvimento deste trabalho.

À Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, pelo suporte financeiro que permitiu a realização deste trabalho (Processo número 09/02131-0).

Resumo

Com o aumento da frequência e diversidade de ataques, uma preocupação crescente das organizações é garantir a segurança da rede. Para compreender as ações que conduziram os incidentes e como eles podem ser mitigados, pesquisadores devem identificar e medir os fatores que influenciam os atacantes e também as vítimas. A quantificação de segurança é, em particular, importante na construção de métricas relevantes para apoiar as decisões que devem ser tomadas para a proteção de sistemas e redes. O objetivo deste trabalho foi propor soluções para auxiliar o desenvolvimento de modelos de quantificação de segurança aplicados em ambientes reais. Três diferentes abordagens foram usadas para a investigação do problema: identificação de limitações nos métodos existentes na literatura, investigação de fatores que influenciam a segurança de uma organização e a criação e aplicação de um questionário para investigar o uso de métricas na prática. Os estudos foram conduzidos usando dados fornecidos pela University of Maryland e pelo Centro de Atendimento a Incidentes de Segurança (CAIS) vinculado a Rede Nacional de Pesquisa (RNP). Os resultados mostraram que as organizações podem se beneficiar de análises mais rigorosas e eficientes a partir do uso de métricas de segurança e que a continuidade das pesquisas nessa área está intimamente ligada ao desenvolvimento de estudos em sistemas reais.

Palavras-chave: Pesquisa quantitativa, Métricas de segurança, Estudo empírico, Sistemas de prevenção de intrusão, Incidentes de Segurança.

Abstract

With the increase in the number and diversity of attacks, a critical concern for organizations is to keep their network secure. To understand the actions that lead to successful attacks and also how they can be mitigated, researchers should identify and measure the factors that influence both attackers and victims. Quantifying security is particularly important to construct relevant metrics that support the decisions that need to be made to protect systems and networks. In this work, we aimed at proposing solutions to support the development of security quantification models applied in real environments. Three different approaches were used to investigate the problem: identifying issues on existing methods, evaluating metrics using empirical analysis and conducting a survey to investigate metrics in practice. Studies were conducted using data provided by the University of Maryland and also by the Security Incident Response Team (CAIS) from the National Education and Research Network (RNP). Our results showed that organizations could better manage security by employing security metrics and also that future directions in this field are related to the development of studies on real systems.

Keywords: Cybersecurity quantification, Security metrics, Empirical study, Intrusion prevention systems, Security incidents.

Sumário

1 Introdução **1**

1.1 Abordagem 4

1.2 Contribuições 6

1.3 Organização da tese 8

2 Terminologia e Definições Básicas **9**

2.1 Segurança 9

2.2 Terminologia 11

2.3 Análise quantitativa de segurança da informação 13

2.3.1 Métricas de segurança 14

2.3.2 Modelos para medir segurança 19

2.3.3 Estudos empíricos sobre quantificação de segurança 25

2.3.4 Uso de questionários em segurança da informação 27

3 Investigação e Análise Crítica de Métodos para Quantificar Segurança **31**

3.1 Análise de trabalhos anteriores 31

3.2 Abordagem proposta 37

3.2.1 Método de coleta dos trabalhos 40

3.2.2 Classificação proposta 41

3.2.3 Resultados e discussão 43

4 Análise de Fatores que Influenciam a Segurança **51**

4.1 Relacionamento entre IPS e incidentes de segurança 51
4.1.1 Dados do sistema de prevenção de intrusão e de incidentes de segurança 54
4.1.2 Metodologia 58
4.1.3 Resultados 67
4.1.4 Discussões e implicações práticas 71
4.1.5 Resumo dos resultados 84
4.2 Outros fatores que influenciam a ocorrência de incidentes de segurança . . 85
4.2.1 Dados - CAIS/RNP 86
4.2.2 Metodologia 90
4.2.3 Exemplos 104
4.2.4 Resumo dos resultados 110
4.3 Limitações 111
4.3.1 University of Maryland 111
4.3.2 CAIS/RNP 112
4.4 Modelo para a identificação de métricas de segurança relevantes 112

5 Questionário para a Avaliação do Uso de Métricas 117
5.1 Metodologia 117
5.2 Resultados 122
5.3 Análise e discussão 129
5.3.1 Resultados agrupados 129
5.3.2 Relação entre o tipo de empresa e as métricas 132
5.3.3 Relação entre a experiência em segurança e as métricas 137
5.4 Resumo dos resultados 140

6 Conclusões e Trabalhos Futuros 141

Bibliografia 147

Apêndice A 159

Apêndice B 163

Apêndice C **165**

Apêndice D **171**

Lista de Figuras

2.1 Exemplo de uma configuração de rede e seu respectivo grafo de ataque. Extraída de (Wang et al., 2008) 20
2.2 Uso do AHP para avaliação da segurança da informação. Adaptado de (Bengtsson, 2007) 24

3.1 Categorias de métricas proposta por Rudolph e Schwarz. Extraída de (Rudolph e Schwarz, 2012) 37
3.2 Diagrama para extração de informações relativas a processos ou sistemas de qualquer natureza. Adaptado de (Trzesniak, 1998) 39
3.3 Distribuição dos trabalhos analisados de acordo com o alvo da medida . . . 46

4.1 Visão geral da abordagem proposta 54
4.2 Distribuição dos incidentes reportados entre os anos de 2007 e 2010. 60
4.3 Evolução de métricas relevantes - Bot 74
4.4 Distribuição de incidentes Bot 75
4.5 Teste de Laplace - Incidentes Bot 78
4.6 Teste de Laplace - Incidentes Hacking 79
4.7 Teste de Laplace - Incidentes Spam 80
4.8 Valores do teste de Laplace entre 10/04/2007 e 12/05/2007. 81
4.9 Valores do teste de Laplace entre 05/10/2010 e 13/11/2010. 82
4.10 Valores do teste de Laplace entre 01/11/2009 e 12/12/2009. 83
4.11 Número cumulativo de incidentes de segurança por semana 84
4.12 Incidentes Bot - 2011/2012 (CAIS/RNP) 90

4.13 Incidentes - 2011/2012 (CAIS/RNP) 93
4.14 Correlograma - incidentes reportados entre 2011 e 2012 95
4.15 Incidentes reportados somente no domingo e quinta-feira 97
4.16 Correlograma - incidentes reportados entre 2007 e 2012 (University of Maryland) 98
4.17 Número de incidentes de segurança por mês (CAIS/RNP) 99
4.18 Número cumulativo de incidentes de segurança por mês (CAIS/RNP) . . . 100
4.19 Índice mensal de sazonalidade - 2011/2012 101
4.20 Teste de Laplace para o número de incidentes por mês 102
4.21 Índice de sazonalidade - Março, Abril, Maio e Dezembro 107
4.22 Número cumulativo de incidentes Bot por instituição 110
4.23 Visão geral do processo de identificação de métricas relevantes 114

5.1 Respostas - Questão 1 123
5.2 Respostas - Questão 2 124
5.3 Respostas - Questão 3 126
5.4 Respostas - Questão 4 126
5.5 Experiência dos participantes em segurança da informação - Box plot . . . 127
5.6 Experiência dos participantes em segurança da informação - Frequências . 128

6.1 Levantamento bibliográfico dos trabalhos analisados - Parte 1 159
6.2 Levantamento bibliográfico dos trabalhos analisados - Parte 2 160
6.3 Taxonomia dos incidentes reportados pela University of Maryland 163
6.4 Tela inicial 165
6.5 Primeira parte do questionário - Área de atuação da organização e atividade desempenhada. 166
6.6 Segunda parte do questionário - Caracterização do local de trabalho e experiência profissional. 167
6.7 Terceira parte do questionário - Seleção das métricas. 167
6.8 Quarta parte do questionário - Avaliação da importância das métricas. . . 168
6.9 Quinta parte do questionário - Avaliação da complexidade das métricas. . . 169
6.10 Sexta parte do questionário - Espaço para citar outras métricas. 169

6.11 Resultados da questão 7 172
6.12 Resultados da questão 8 173
6.13 Resultados da questão 9 174

Lista de Tabelas

2.1 Exemplos de métricas de segurança 17
2.2 Tabela comparativa - Modelos para medir segurança 25

3.1 Trabalhos anteriores sobre análise e classificação de métricas de segurança . 38
3.2 Como as diferentes metodologias para quantificar segurança são aplicadas nos sistemas ou processos 44
3.3 Relação entre os dados utilizados e o processo medido 47
3.4 Relação entre os dados utilizados e a metodologia 48

4.1 Incidentes de segurança investigados 61
4.2 Alertas do sistema de prevenção de intrusão 61
4.3 Estatística descritiva das variáveis (209 observações) 62
4.4 Resultados dos modelos de regressão - coeficiente e valor p 68
4.5 Resultados dos modelos de regressão de acordo com o tipo de incidente - coeficiente e valor p 69
4.6 Métricas relevantes ao longo do tempo 73
4.7 Evolução das métricas relevantes por tipo de incidente 82
4.8 Resumo dos incidentes (2011/2012) - CAIS/RNP 88
4.9 Resumo dos incidentes por tipo (2011/2012) - CAIS/RNP 91
4.10 Resumo dos incidentes por estado (2011/2012) - CAIS/RNP 92
4.11 Incidentes reportados por dia da semana 96
4.12 Instituições investigadas 105
4.13 Resultados - número de incidentes por dia 106

4.14 Resultados - número de incidentes por mês 107
4.15 Resultados - grau de associação entre os tipos de incidentes 108
4.16 Grau de associação entre os incidentes Bot por instituição 108
4.17 Grau de associação entre os incidentes Spam por instituição 109

5.1 Métricas avaliadas na pesquisa 120
5.2 Questões presentes na pesquisa 121
5.3 Taxas de respostas de pesquisas sobre segurança 123
5.4 Estatística descritiva das respostas - Questões 5 e 6 124
5.5 Questões 7, 8 e 9 - Cinco primeiros resultados 125
5.6 Questões 7, 8 e 9 - Cinco últimos resultados 125
5.7 Tabela ANOVA - Influência dos grupos 131
5.8 Tipos de empresa - Correlação entre as perguntas 133
5.9 Tabela ANOVA - Influência do tipo de empresa 133
5.10 Tabela ANOVA - Influência do tipo da empresa 134
5.11 Questão 7 - Diferenças entre TIC e Educação 135
5.12 Questão 9 - Diferenças entre TIC e Educação 135
5.13 Experiência do participante - Correlação entre as perguntas 137
5.14 Tabela ANOVA - Influência da experiência em segurança da informação . . 138
5.15 Tabela ANOVA - Influência da experiência em segurança da informação por tipo de métrica 139

Lista de Acrônimos

AHP	Analytic Hierarchy Process (Processo de análise hierárquico)
CAIS	Centro de Atendimento a Incidentes de Seguraça
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CIS	Center for Internet Security
CSIRT	Equipe de Resposta a Tratamento de Incidentes de Segurança
CVSS	Common Vulnerability Scoring System
DIT	Division of Information Technology
IDS	Intrusion Detection System (Sistema de detecção de intrusão)
IPS	Intrusion Prevention System (Sistema de prevenção de intrusão)
LARS	Least Angle Regression
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OLS	Ordinary Least Squares
RNP	Rede Nacional de Pesquisa
SANS	SysAdmin, Audit, Networking, and Security
SFR	Stepwise Forward Regression
TIC	Tecnologias da Informação e Comunicação

Notação

X_k	Conjunto de k variáveis independentes em um modelo de regressão
Y	Variável independente em um modelo de regressão
β_j	Coeficiente de regressão da j-ésima variável independente
p	Nível de significância observado
$G1$	Conjunto de métricas para os ataques direcionados a organização
$G2$	Conjunto de métricas para os ataques originados dentro da organização
s_t	Conjunto referente ao intervalo de tempo em que as variáveis da regressão foram coletadas
Xr_t	Conjunto de variáveis independentes relevantes
$u(t)$	Coeficiente do teste de Laplace no tempo t
C_j	Coeficiente de associação entre um tipo de incidente j e um conjunto de métricas relevantes
r_k	Coeficiente de autocorrelação em um determinado intervalo de observação k
μ	Média aritmética de uma população
σ	Desvio padrão de uma população
S_i	Índice de sazonalidade mensal do i-ésimo mês
r	Coeficiente de correlação de *Pearson*
s_{xy}	Coeficiente de correlação cruzada
H_0	Hipótese nula
H_a	Hipótese alternativa

Lista de publicações

Artigos publicados

- MIANI, R. S. ; CUKIER, M. ; ZARPELÃO, B. B. ; MENDES, L. S. . Relationships between information security metrics. The Eighth Annual Cyber Security and Information Intelligence Research Workshop, 2013, Oak Ridge. Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13. New York: ACM Press.

- MIANI, R. S. ; CUKIER, M. ; ZARPELAO, B. B. ; BREDA, G. D. ; MENDES, L. S. . An Empirical Study of Connections Between Measurements and Information Security. The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), 2012, Rome. Proceedings of the Sixth International Conference on Emerging Security Information, Systems and Technologies, 2012. p. 104-111.

- VIEIRA, L. ; MIANI, R. S. ; ZARPELAO, B. B. ; BREDA, G. D. ; MENDES, L. S. . An Architecture Based on Agent-manager Model for Automated Data Collection of Security Metrics. The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), 2012, Rome. Proceedings of the Sixth International Conference on Emerging Security Information, Systems and Technologies, 2012. p. 85-91.

- MIANI, R. S. ; ZARPELAO, B. B. ; MENDES, L. S. . Application of Security Metrics in a Metropolitan Network : A Case Study. International Telecommunica-

tions Symposium 2010, Manaus. Proceedings of International Telecommunications Symposium 2010.

Capítulo 1

Introdução

Os recentes ataques de negação de serviço direcionados a instituições financeiras e governamentais realizados pelo grupo *Anonymous*, a descoberta de códigos maliciosos capazes de espionar e controlar sistemas industriais como o *Stuxnet* e o vazamento de informações sigilosas liderado pelo grupo *Wikileaks* fazem com que haja uma preocupação crescente com as questões relacionadas à segurança da informação. Um relatório disponibilizado pelo departamento de segurança nacional dos Estados Unidos (Department of Homeland Security, 2011), mostra que os ataques a computadores estão crescendo não somente em frequência, mas também em impacto.

Esta tendência é reforçada pela publicação de diversas estatísticas sobre incidentes de segurança. As principais fontes de dados sobre incidentes de segurança do Brasil são o Centro de Atendimento a Incidentes de Segurança (CAIS), vinculado à Rede Nacional de Pesquisa (RNP) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Dados de ambas as instituições mostram que, desde o fim dos anos 90, os incidentes de segurança apresentam uma forte tendência de crescimento. A revolução digital e o crescimento das vendas de dispositivos com acesso à Internet são alguns dos fatores que podem explicar este crescimento. Uma das consequências do aumento no número de incidentes de segurança é o aumento de investimentos em soluções de segurança. De acordo com o estudo da Frost & Sullivan (Sullivan), empresa internacional de consultoria, o mercado de segurança da informação na América Latina movimentou US$ 186,1 milhões em 2007 e alcançará US$ 598,4 milhões em 2013.

Os desafios enfrentados pelas organizações com relação ao tratamento e prevenção de

incidentes de segurança são grandes e exigem muitos cuidados. Com esse intuito, diversos meios para analisar e representar a segurança de sistemas de informação são propostos. Nesse trabalho, será usada uma abordagem quantitativa para descrever a segurança de sistemas, em particular, a segurança de ambientes operacionais, como a rede de uma organização. A quantificação é um paradigma de investigação científica baseado na contagem e mensuração de observações e aplicado em diversas áreas do conhecimento humano Church e Rogers (2006). À partir do uso de métricas bem definidas, a quantificação permite a descrição precisa e consistente de diferentes objetos de pesquisa.

A ideia de quantificação aplicada a segurança da informação é objeto de discussões dos pesquisadores da área ao longo das últimas duas décadas, seja para o desenvolvimento de métricas de segurança, estudos sobre impactos econômicos, avaliação de risco ou modelos para medir segurança (Verendel, 2010). O emprego de métricas de segurança e suas aplicações em cenários de Tecnologia da Informação e Comunicação (TIC), em especial, é um tópico fundamental para investigar as motivações dos ataques e também para avaliar a eficiência dos controles implementados.

Uma métrica pode ser vista como um padrão de medida. O objetivo primário de uma métrica é transformar dados brutos em informações passíveis de análise. Grandes organizações ligadas à segurança da informação como o *Computer Emergency Response Team* (CERT), *SysAdmin, Audit, Network, Security* (SANS) e *National Institute of Standards and Technology* (NIST) recomendam a implementação de métricas nas corporações, pois elas podem indicar o nível atual de certa meta de segurança e também direcionar as ações tomadas pela organização (Payne, 2006), (Miani et al., 2010). Alguns exemplos de métricas de segurança incluem: número de vulnerabilidades de segurança conhecidas sem correções, número de estações com privilégios administrativos liberados para qualquer usuário e período de tempo não planejado em que um recurso computacional não está disponível.

Contudo, grande parte da literatura sobre o assunto é teórica e direcionada ao desenvolvimento de listas de métricas de segurança (Boyer e McQueen, 2008), (Chew et al., 2008), (The Center for Internet Security, 2010), (Jaquith, 2007), (Herrmann, 2007), (W. Krag Brotby, 2009). Poucos trabalhos mostram o lado prático e a utilidade das métricas de segurança. Um estudo conduzido por Verendel (2009) mostra que até o momento, não

existem evidências empíricas sobre os benefícios e a relevância de tais métricas. Diversas questões ainda permanecem sem uma resposta adequada: Quais métricas escolher? As métricas realmente representam o que deveriam medir? Quais métricas podem ser utilizadas para avaliar o nível de segurança da informação? A eficiência das métricas varia ao longo do tempo? Como analisar o relacionamento entre um conjunto de métricas e o objeto que está sendo medido?

Em outras áreas da ciência, como a Economia, Ciências Sociais e Biologia, o emprego da quantificação é um assunto consolidado. Produto Interno Bruto (PIB), Índice de Desenvolvimento Humano (IDH) e Índice Gerais de Preços (IGP) são exemplos do uso da quantificação para a descrição de um processo ou sistema. Levando esses fatos em consideração, um caminho natural de pesquisa para a quantificação de segurança consistiria em adotar uma abordagem inspirada em tais áreas. Entretanto, diversos problemas dificultam o prosseguimento desses estudos na área de segurança da informação.

Um problema é associado a ausência de dados sobre segurança. O compartilhamento e disponibilidade desse tipo de informação ainda é visto com desconfiança pelos envolvidos (Geer et al., 2003). Muitas organizações acreditam que a exposição de informações sobre segurança, mesmo anonimamente, pode eventualmente prejudicar os negócios (Jaquith, 2007). Alguns exemplos de dados disponíveis para o estudo da segurança da informação incluem: relatórios de incidentes de segurança (Richardson, 2011), (Verizon, 2012), (PriceWaterHouseCoopers, 2011), bases de dados de vulnerabilidades, tais como a *National Vulnerability Database* (NVD) (NIST, 2013) e o PREDICT (*Protected Repository for the Defense of Infrastructure against Cyber Threats*) (Department of Homeland Security, 2013) que é um repositório de dados centralizados de operações de rede do mundo inteiro. Porém, esses dados são na maioria das vezes, simples e não incluem características sobre a organização (cultura de segurança da organização ou tamanho da equipe de TIC), detalhes sobre os usuários ou sobre a coleta dos dados, como a configuração do sistema de detecção de intrusão que coletou o dado.

Outro problema está ligado à natureza da segurança da informação. Medir segurança é uma tarefa complexa, diferente e muitas vezes mais difícil do que outros tipos de medida. Pfleeger e Cunningham (2010) investigaram nove possíveis razões para esse fato. Uma das razões citadas pelos autores é a de que a segurança é multidimensional, ou seja, é com-

posta por diversos atributos. Mesmo decompondo a segurança em diversos atributos, a combinação ou composição das medidas em um único número que represente a segurança de todo o sistema não é uma tarefa trivial. Outra razão citada é a de que o próprio adversário (atacante) modifica o ambiente. Os adversários alteram o ambiente utilizando novas estratégias e criando novas classes de ataques, levando a um aumento da complexidade e da quantidade de variáveis envolvidas no processo de medir segurança. Além disso, como os objetivos de segurança das organizações podem variar, as métricas também podem variar de acordo com a organização, tornando um problema o estabelecimento de métricas de segurança eficientes para sistemas e ambientes distintos.

Portanto, é possível afirmar que a ausência de estudos que exploram os aspectos práticos e a importância da abordagem quantitativa em segurança é um problema relevante para o avanço dessa área de pesquisa. Com esse intuito, o presente trabalho propõe uma investigação sobre os benefícios e a relevância da quantificação de segurança usando dados coletados em ambientes reais. O objetivo é fornecer o embasamento teórico adequado para a discussão do problema, além de apresentar soluções que auxiliem o emprego da abordagem quantitativa para a avaliação da segurança em uma organização.

1.1 Abordagem

Com base nas dificuldades descritas na seção anterior, o problema da tese será abordado da seguinte forma: i) identificação das razões que envolvem a ausência de validação nos métodos empregados para a quantificação da segurança, ii) investigação de fatores que influenciam a segurança de uma organização usando dados coletados em ambientes reais e iii) criação e aplicação de um questionário para investigar o uso da quantificação de segurança na prática.

O primeiro passo consiste em entender o estágio atual da área de pesquisa. Diversos trabalhos propõem métodos para medir segurança. Conforme notado por Verendel (2009), os modelos propostos, na maioria dos casos, não são confiáveis devido a ausência de validação. Um dos objetivos desta tese é tentar entender as razões desse fato. A compreensão dessas razões pode ser o ponto de partida para o desenvolvimento de métodos quantitativos mais robustos e eficientes para a comunidade de segurança. Será trabalhada a hipótese

de que a ausência de validação nos modelos propostos pode estar relacionada a problemas conceituais de quantificação de dados. Com esse intuito, 57 trabalhos científicos na área de quantificação de segurança da informação foram estudados e classificados de acordo com três critérios (Trzesniak, 1998): o alvo da medida, ou seja, o sistema de interesse, a metodologia de obtenção da medida e os dados utilizados.

A segunda parte deste trabalho consiste em propor soluções para quantificar a relação entre as métricas e o objeto que está sendo medido. O estudo em questão envolve a investigação de fatores que influenciam a frequência de incidentes de segurança reportados em uma organização. Conforme discutido anteriormente, um grande problema ligado a esse tipo de estudo é a ausência de dados. No entanto, duas instituições colaboraram com o fornecimento de dados para as pesquisas: University of Maryland, EUA e CAIS/RNP. Com o auxílio desses dados, dois estudos foram conduzidos e serão descritos com detalhes nesta tese:

1. Investigação da relação entre métricas de segurança obtidas à partir de dados do sistema de prevenção de intrusão (IPS - *Intrusion Prevention System*) da University of Maryland e o número de incidentes de segurança reportados pela mesma entidade - o número de ataques bloqueados ou o a quantidade de alertas disparados influenciam o modo com que os incidentes são reportados?

2. Investigação de fatores que influenciam a ocorrência de incidentes de segurança reportados pelo CAIS/RNP - variação de acordo com determinadas características temporais e conforme os tipos de incidentes detectados.

A intenção desse caminho de pesquisa é buscar uma forma de avaliação e validação de métricas de segurança usando dados coletados em ambientes reais.

Após a identificação dos problemas presentes na literatura e o desenvolvimento de soluções para a avaliação empírica de métricas de segurança, a última etapa deste trabalho de doutorado consiste em analisar o uso da quantificação de segurança na prática. Com esse intuito, foi escolhido um método amplamente empregado pela comunidade científica para a coleta de informações iniciais sobre um determinado assunto, chamado de pesquisa de avaliação, ou *survey*. Esse tipo de pesquisa consiste em recolher dados através de questio-

nários enviados a um determinado número de pessoas e produzir descrições quantitativas dessa população.

Foi proposto um questionário com o objetivo de compreender como as diferentes métricas de segurança propostas na literatura são aplicadas no cotidiano das empresas. Em particular, a intenção do questionário é obter opiniões de especialistas sobre os seguintes itens: 1) quais métricas são usadas para avaliação da segurança, 2) qual a importância das métricas, quando comparadas entre si e 3) qual é a complexidade de implementação das métricas em ambientes reais, quando comparadas entre si.

1.2 Contribuições

O objetivo deste trabalho é propor uma investigação detalhada sobre a relevância e os benefícios da quantificação de segurança usando três abordagens: identificação das razões que envolvem a ausência de validação nos métodos empregados para a quantificação da segurança, investigação de fatores que influenciam a segurança de uma organização usando dados coletados em ambientes reais e o desenvolvimento e aplicação de um questionário para investigar o uso da quantificação de segurança na prática. As principais contribuições desta tese são:

- **Proposta de uma nova classificação para a categorização e comparação de modelos de quantificação de segurança baseada em teorias de construção de indicadores quantitativos:** a nova classificação procura complementar as anteriores (Villarrubia et al., 2004), (Verendel, 2009), (Rudolph e Schwarz, 2012), usando critérios inspirados na teoria de indicadores quantitativos;

- **Levantamento bibliográfico atualizado de trabalhos que propõem modelos de quantificação de segurança:** investigação e análise crítica de 57 trabalhos sobre quantificação de segurança publicados entre 2004 e 2012. Essa compilação do estado da arte pode ser utilizada como ponto de partida para novas pesquisas pela comunidade científica;

- **Desenvolvimento de soluções para quantificar segurança:** a combinação de métodos estatísticos como modelos de regressão linear múltipla, testes de tendência

de Laplace e análise de séries temporais possibilitam encontrar a correlação entre a métrica e o objeto de medida e assim identificar a relevância de métricas de segurança;

- **Quantificação da associação entre métricas obtidas à partir do sistema de prevenção de intrusão e a frequência de incidentes de segurança reportados:** levando em consideração que os sistemas de prevenção de intrusão mantém em seus registros as tentativas de ataques bloqueadas e os incidentes de segurança são, na maioria das vezes, os registros dos ataques realizados com sucesso, é possível inferir a existência de uma relação entre esses conjuntos de dados. Essa ideia pode ser estendida para outros conjuntos de dados, como os registros do *firewall* e dados do sistema de detecção de intrusão, entre outros. Os dados utilizados nesse estudo foram fornecidos pela University of Maryland e obtidos durante o período de estágio realizado em tal instituição;

- **Análise quantitativa sobre outros tipos de fatores que podem influenciar a ocorrência de incidentes de segurança:** são avaliados o impacto de fatores relacionados a características do ambiente (tempo e associação entre os diferentes tipos de incidentes) na ocorrência de incidentes de segurança em uma organização. Esse tipo de estudo fornece informações que podem ser utilizadas para o desenvolvimento de políticas de prevenção e mitigação de incidentes. Os dados utilizados nesse estudo foram fornecidos pelo CAIS/RNP;

- **Criação de um fluxo de atividades para auxiliar o processo de validação e comparação de métricas de segurança:** com base nos estudos conduzidos para analisar a influência de fatores na frequência de incidentes de segurança, foi sugerido um conjunto de ações para guiar a identificação de métricas relevantes;

- **Investigação sobre o uso da abordagem quantitativa em segurança, usando dados obtidos em um questionário respondido por profissionais da área de TIC:** o uso de questionários para a investigação de problemas relacionados à segurança da informação é uma prática importante para a validação de modelos e investigação de hipóteses. A ideia principal do questionário é a identificação de

métricas de segurança relevantes para os profissionais de segurança. Devido a ausência de estudos empíricos e padronizações sobre o tema, essa abordagem pode ser usada para elucidar as estratégias utilizadas, identificar as preocupações das organizações e iniciar validações empíricas à partir das respostas. Foi possível encontrar correlação entre as métricas mais utilizadas e mais importantes e somente diferenças sutis nas métricas utilizadas por respondentes que trabalham em diferentes setores econômicos.

1.3 Organização da tese

Esta tese é organizada da seguinte forma: o capítulo 2 descreve os conceitos básicos sobre segurança da informação e quantificação de segurança, além de apresentar a terminologia usada ao longo do trabalho e discutir os modelos usadas para medir segurança encontrados na literatura. O capítulo 3 apresenta um levantamento bibliográfico sobre trabalhos que propõem modelos de quantificação de segurança e mostra a abordagem desenvolvida, que consiste em analisar os métodos presentes na literatura usando critérios baseados na construção de indicadores quantitativos. O capítulo 4 traz os detalhes dos estudos desenvolvidos para avaliar os fatores que influenciam a frequência de incidentes de segurança. Além das duas análises propostas, também será apresentado um modelo para auxiliar a identificação de métricas relevantes e as limitações dos conjuntos de dados utilizados. O capítulo 5 detalha o questionário proposto, assim como os resultados obtidos. Por fim, o capítulo 6 mostra as considerações finais e as perspectivas para trabalhos futuros.

Capítulo 2

Terminologia e Definições Básicas

Este capítulo descreve os conceitos básicos relacionados à segurança da informação e à quantificação de segurança. Primeiramente, serão apresentadas algumas definições básicas sobre segurança da informação. A seguir, será introduzida a terminologia usada ao longo do trabalho, com a distinção dos termos métrica e indicador. As premissas básicas sobre métodos de quantificação de segurança serão apresentadas, assim como exemplos de propostas baseadas em Grafos de Ataque, Avaliação de Risco, Superfície de Ataque e Processo de Análise Hierárquico (AHP - *Analytic Hierarchy Process*). Por fim, serão mostradas as definições e requisitos de uma métrica de segurança, um levantamento sobre investigações empíricas em quantificação de segurança e trabalhos relacionados sobre o uso de questionários em segurança da informação.

2.1 Segurança

De acordo com a norma ISO/IEC 27004 (International Organization for Standardization, 2009), a informação é um ativo que tem um valor para a organização e consequentemente necessita ser adequadamente protegida. A segurança da informação busca minimizar os impactos das ameaças no sistema [1] e assim garantir a continuidade dos negócios.

[1] Ao longo deste trabalho, um sistema de informação ou sistema será definido como um computador ou sistema de informação computacional. Formalmente, um sistema de informação é um conjunto discreto de recursos de informação organizado para a coleta, processamento, manutenção, uso, compartilhamento ou disseminação da informação (Chew et al., 2008).

A segurança da informação é frequentemente definida em termos de Bishop (2002):

- Sigilo - a informação deve ser acessível somente às entidades autorizadas pelo proprietário da informação;
- Integridade - garantia de que a informação manipulada mantenha as características originais estabelecidas pelo proprietário da informação;
- Disponibilidade - usuários autorizados devem obter acesso à informação sempre que necessário.

O ponto de vista das entidades, usuários e suas ações junto aos sistemas é um outro meio de abordar a segurança da informação, também conhecido como *Authentication, Authorization, and Accounting* (AAA) Metz (1999). Os seguintes conceitos são definidos:

- Autenticação (*Authentication*): garantia de que a identidade física de um usuário ou sistema esteja relacionada a sua respectiva identidade digital;
- Autorização (*Authorization*): determinar quais ações podem ser executadas por um usuário ou entidade;
- Não repúdio (*Accounting*): garantia de que ações e acessos de usuários e entidades sejam associadas de forma inquestionável.

Geus e Nakamura (2007) citam exemplos de falhas que, se exploradas corretamente, podem comprometer a segurança de sistemas:

- Exploração de vulnerabilidades em sistemas operacionais, aplicativos, protocolos e serviços. Exemplos: execução remota de códigos maliciosos em sistemas operacionais como o Windows;
- Exploração dos aspectos humanos dos envolvidos. Exemplos: uso de engenharia social para a obtenção de informações sigilosas;
- Falha no desenvolvimento e implementação da política de segurança. Exemplos: elaboração de política de segurança que não prevê o uso cópias de segurança;

- Falha na configuração de serviços e de sistemas de segurança. Exemplo: utilização da configuração padrão que é conhecida por todos, inclusive pelos invasores.

Eventos relacionados a exploração com sucesso de tais falhas e ao ato de violar, de maneira implícita ou explícita uma determinada política de segurança são conhecidos como incidentes de segurança. Um aumento no número de incidentes pode representar que:

- A organização está mais vulnerável aos ataques;
- Mais recursos (tempo, funcionários e tecnologia) foram alocados para a detecção de incidentes.

Já uma diminuição do número de incidentes de segurança pode representar que:

- A organização está mais resistente aos ataques;
- Poucos recursos (tempo, funcionários e tecnologia) foram alocados para a detecção de incidentes.

A análise de incidentes pode revelar importantes comportamentos em uma organização, e ser usada para diversos fins, como por exemplo a alocação eficiente de recursos de TIC, a avaliação do impacto de medidas preventivas ou ainda alterações em políticas de segurança vigentes. Um dos objetivos desta tese é o estudo de métricas associadas a ocorrência de incidentes de segurança.

2.2 Terminologia

O conceito de métrica, quando não definido de maneira correta, pode causar imprecisão e dificultar a compreensão do assunto. Na literatura é possível encontrar várias definições para esse termo. Conforme discutido em (Miani, 2009), autores da área trabalham com duas abordagens:

1. Definir o conceito de medida e a partir dele definir métrica;

2. Não diferenciar os conceitos de medida e métrica.

Alguns trabalhos que utilizam o primeiro modo para definir o conceito de métrica são: (Sademies, 2004) e (Payne, 2006). Payne (2006) utiliza a seguinte definição: medidas são geradas através de contagem enquanto métricas são geradas por meio de análises. Em outras palavras, medidas são dados brutos e métricas são interpretações humanas, objetivas ou subjetivas de tais dados. Os seguintes exemplos ilustram a diferença entre métrica e medida: o número de vulnerabilidades encontrados é um tipo de medida, enquanto que a relação entre as vulnerabilidades encontradas em cada mês representa uma métrica.

Já o segundo modo de definição de métricas é empregado em (Jaquith, 2007), (Chew et al., 2008) e (W. Krag Brotby, 2009). Jaquith (2007) afirma que a simples quantificação de um problema e seus resultados em um valor numérico pode ser considerado uma métrica. Logo, não é feita uma diferenciação entre os conceitos de métrica e medida. Com o objetivo de simplificar o texto e as notações, os conceitos de métrica e medida não serão diferenciados ao longo desta tese. Assim como os autores citados anteriormente, as definições serão mantidas em um formato mais simples, para focar no aspecto mais importante, que é a discussão sobre como as métricas podem auxiliar no cotidiano das organizações.

A seguir serão definidos os seguintes termos utilizados ao longo desta tese: métrica de segurança e indicador de segurança. Os termos foram definidos com base nos trabalhos desenvolvidos por (Chew et al., 2008), (Jaquith, 2007) e (Rudolph e Schwarz, 2012).

Definição 1. Métrica de segurança

Uma métrica de segurança representa o resultado de um processo de quantificação em algum aspecto da segurança da informação.

Definição 2. Indicador de segurança

Um indicador de segurança representa uma métrica correlacionada a uma determinada propriedade de segurança.

É importante notar que, na maioria das métricas propostas na literatura, a correlação entre a métrica e uma determinada propriedade de segurança não é formalmente estabe-

lecida. De acordo com a definição proposta nesse trabalho, o número de vírus detectados em estações de trabalho é uma métrica de segurança. Porém, para ser considerado um indicador de segurança, a correlação da métrica com alguma propriedade de segurança deve ser verificada. Se as análises mostram que o número de vírus detectados em estações de trabalho está correlacionado com as tentativas de ataque contra a organização, então essa métrica pode ser utilizada como um indicador para tentativas de ataque contra a organização.

2.3 Análise quantitativa de segurança da informação

Dacier et al. (1996) e Wang e Wulf (1997), propuseram os primeiros modelos com o intuito de medir segurança. Um dos principais problemas encontrados pelos pesquisadores foi a própria definição de segurança. Esta questão ainda é motivo de discussão entre a comunidade científica, devido as diferentes percepções de segurança que um indivíduo ou grupo podem possuir. Problemas de segurança considerados essenciais para um ambiente acadêmico, como a Universidade Estadual de Campinas são certamente diferentes das prioridades de segurança para a agência de inteligência norte-americana (CIA - *Central Intelligence Agency*). Um outro exemplo envolve as prioridades de segurança. A rede que controla as transações de uma bolsa de valores pode ter como prioridade de segurança a disponibilidade em tempo real e a privacidade das informações, enquanto que um portal de notícias concentra as atenções na integridade das informações. Assim, uma única definição de segurança nem sempre é o suficiente Wang e Wulf (1997).

O modelo proposto por Wang e Wulf (1997) consiste na seleção de unidades e escalas e na definição de uma metodologia para estimar e validar as métricas. O principal objetivo do trabalho é elucidar como ferramentas analíticas podem ser utilizadas para medir segurança. Uma possível métrica de segurança no modelo é calculada por meio da combinação de elementos de confidencialidade, integridade e disponibilidade do sistema que está sob medição. Além disso, são tratadas questões como: decomposição de propriedades de segurança, relações funcionais entre fatores de segurança e validação baseada em teoria de medida, relações empíricas e uso de experimentos formais. As ideias seminais apresentadas neste trabalho auxiliaram o desenvolvimento de métricas de segurança baseadas

em elementos de confidencialidade, integridade e disponibilidade, como o CVSS (*Common Vulnerability Score System*) (Mell et al., 2007), a criação de métodos para decomposição de segurança como o uso do AHP entre outros avanços na área.

Já o trabalho de Dacier et al. (1996) consiste em primeiramente modelar o sistema como um grafo de privilégios, exibindo as vulnerabilidades de segurança do sistema. O próximo passo é transformar esse grafo de privilégios em uma cadeia de Markov para todos os possíveis cenários de ataque. Os possíveis cenários de ataque são quantificados utilizando o tempo e o esforço usado para o atacante alcançar um alvo. O conceito de modelagem apresentado por Dacier et al. usando grafos para visualizar as vulnerabilidades de segurança do sistema, originou a criação de modelos de quantificação de segurança conhecidos como Grafos de Ataque.

Dificuldades em calcular os valores de confidencialidade, integridade e disponibilidade para uma métrica e o emprego de vulnerabilidade de segurança como o único vetor de ataque em um sistema foram as principais limitações nos primeiros modelos para medir segurança. Assim, à partir desses dois trabalhos, os estudos sobre quantificação de segurança se concentraram em três principais tópicos (Verendel, 2009): a criação de novos modelos formais para quantificar segurança (como o proposto por Dacier et al.), o desenvolvimento de métricas de segurança e a criação de métodos genéricos para análise quantitativa de segurança (não necessariamente modelos formais ou métricas) e mecanismos de quantificação.

Nas próximas seções serão apresentados trabalhos relacionados ao desenvolvimento de métricas de segurança, modelos para quantificar segurança e estudos empíricos sobre quantificação de segurança.

2.3.1 Métricas de segurança

De acordo com W. Krag Brotby (2009), métrica é um termo utilizado para denotar uma medida baseada em uma referência. Como a segurança, em seu significado mais básico, pode ser representada pela proteção contra as ameaças ou a ausência de ameaças, as métricas devem refletir o nível de segurança relativo a um certo objetivo e auxiliar a tomada de decisão para tratar ou evitar ameaças. O autor ainda afirma que as métricas

de segurança atuais não obtiveram sucesso para fazer isso devido a ausência de objetivos em sua definição. A definição de objetivos para as métricas é crucial para o sucesso das mesmas. Sem eles, é impossível determinar progressos ou ainda avaliar se o programa está na direção correta.

Jaquith (2007), afirma que qualquer quantificação de um problema e seus resultados em um valor numérico pode ser considerado uma métrica. Segundo o autor, embora diversas definições sobre métrica possam ser encontradas, inclusive em dicionários e em outros contextos, como física e matemática, o mais importante é a discussão sobre como as métricas podem auxiliar no cotidiano das organizações. Jaquith também afirma que o principal objetivo de uma métrica é a quantificação de dados brutos para fundamentar a tomada de decisões. Já Chew et al. (2008), define métrica como uma ferramenta projetada para facilitar a tomada de decisões e melhorar a performance do sistema, através da coleta, análise e divulgação de dados.

Um ponto chave nas discussões sobre o uso de métricas de segurança é relacionado a qualidade das métricas a se empregar. Caso métricas mal planejadas ou inadequadas sejam aplicadas a certo objetivo, os resultados podem trazer falsa sensação de segurança e até perda de capital de investimentos mal aplicados. Contudo, o que é necessário para que uma métrica seja adequada? Quais atributos uma métrica deve possuir? Conforme mencionado anteriormente, as métricas de segurança existem para fornecer suporte à tomada de decisões. Este suporte é realizado por meio da geração de informação. Levando em consideração tal fato, W. Krag Brotby (2009) define uma série de atributos que as informações geradas por uma métrica adequada deve possuir:

- Gerenciáveis: as informações fornecidas pelas métricas devem ser concisas e acessíveis;
- Significativas: a informação deve ser fácil de entender e importante, além de fornecer uma base para a tomada de decisões;
- Inequívoca: informação ambígua pode ser enganosa, de pouco uso ou extremamente perigosa;
- Confiável: a capacidade de confiar nos instrumentos é condicionada na confiabilidade

das medidas;

- Precisas: um sensato e conhecido nível de precisão é essencial;
- Apropriadas: informações que avisam sobre um desastre depois de ocorrer, não são úteis;
- Preditivas: é importante que algumas informações geradas possam sinalizar problemas iminentes.

Jaquith (2007) propõe o seguinte conjunto de atributos para métricas de segurança.

- Definida de maneira consistente, sem critérios subjetivos;
- Fácil de coletar, de preferência de modo automatizado;
- Expressa em números cardinais ou porcentagem, não de maneira qualitativa com rótulos como “alto”, “médio” e “baixo”;
- Expressa utilizando ao menos uma unidade de medida, tais como “defeitos”, “horas” ou “dólares”;
- Suficientemente relevante a fim de que as decisões possam ser tomadas com base nos resultados das métricas.

Note que as definições são complementares, pois, enquanto Jaquith propõe um conjunto de atributos para uma métrica adequada, Brotby apresenta um conjunto de atributos que as informações geradas por uma métrica adequada deve possuir. De acordo com as definições, é possível afirmar que se uma métrica possui os atributos citados por Jaquith, então a informação gerada por ela deverá respeitar o conjunto de atributos de Brotby. Uma métrica definida de maneira consistente e sem critérios subjetivos é inevitavelmente inequívoca, assim como uma métrica expressa utilizando números cardinais e ao menos uma unidade de medida será precisa. Dessa forma, é possível construir um conjunto consistente de atributos que definem as características de uma métrica de segurança adequada.

A Tabela 2.1 apresenta algumas métricas de segurança. Elas foram escolhidas a fim de ilustrar os conceitos mostrados até aqui.

Tabela 2.1: Exemplos de métricas de segurança

Métrica	**Documento de referência**
Taxa de atualizações de segurança aplicadas por período ou por nó da rede	(Jaquith, 2007)
Downtime, período de tempo em que um recurso computacional não está funcionando ou operacional, não planejado	(Jaquith, 2007)
Porcentagem total de sistemas para os quais os controles de segurança foram testados em um determinado período de tempo	(Chew et al., 2008)
Porcentagem de notebooks com capacidade de cifração para arquivos confidenciais	(Chew et al., 2008)
Tempo médio entre incidentes de segurança	(The Center for Internet Security, 2010)
Porcentagem de sistemas sem vulnerabilidades críticas conhecidas	(The Center for Internet Security, 2010)
Porcentagem de funcionários de TIC com qualificações específicas em segurança da informação	(Torres et al., 2006)

A implementação de métricas de segurança proporciona diversos benefícios às organizações (Chew et al., 2008). O processo de coleta dos dados e apresentação dos resultados permite identificar controles técnicos, operacionais ou de gestão que não estão sendo implementados ou são implementados incorretamente. Utilizando os resultados da análise das métricas, os gerentes e proprietários do sistema podem isolar os problemas, usar os dados coletados para justificar os pedidos de investimentos e assim direcionar os investimentos para as áreas que necessitam de melhorias.

Apesar dos benefícios citados, um grande problema relacionado às métricas de segurança é o chamado problema fundamental da medição (Hinson, 2006). Considere uma métrica que tenha como objetivo medir o número e a severidade dos incidentes de segurança em um determinado sistema. O problema fundamental da medição recai no seguinte questionamento: o que os números obtidos com a medição podem nos indicar? Como interpretar corretamente os dados? A situação a seguir ilustra esse problema.

Considere as medições obtidas por uma métrica com relação à ataques em páginas da

web (*web defacements*). Esse tipo de ataque não é tão comum quanto foi há alguns anos atrás. Os servidores agora são mais protegidos ou os atacantes estão escolhendo outros tipos de alvos? Em outras palavras, os controles de segurança estão funcionando ou as falhas passaram desapercebidas? Esse tipo de problema requer um grande cuidado na elaboração da métrica e também na filtragem e interpretação dos resultados obtidos.

Um outro problema relacionado a implementação de métricas de métricas de segurança é o uso excessivo de métricas (W. Krag Brotby, 2009). A organização pode gastar recursos implementando muitas métricas e não usá-las de fato. W. Krag Brotby (2009) propõe as seguintes diretrizes que auxiliam evitar tal erro: i) não coletar métricas se não existirem objetivos pré-definidos sobre como os resultados serão utilizados, ii) propor objetivos factíveis e pragmáticos, iii) distinguir entre o que pode ser medido e o que precisa ser medido e iv) estabelecer uma relação de custo-benefício entre as vantagens e o custo da implementação.

A proliferação de propostas de métricas de segurança e os problemas relacionados ao uso prático das mesmas, motivou a agência federal norte-americana de padronização e tecnologia (NIST) a desenvolver um relatório (Jansen, 2010) sobre o estado da arte e possíveis áreas de pesquisa sobre o tema métricas de segurança.

O relatório mostra que, em geral, o estado atual das métricas de segurança envolve indicadores de segurança ambíguos, avaliados de modo subjetivo e que não necessariamente coincidem com os objetivos de segurança da organização. Além disso, poucos trabalhos da área mostraram a utilidade das métricas de segurança na prática. Dessa forma, os esforços em pesquisa na área de métricas de segurança devem envolver os seguintes fatores:

- Determinar bons estimadores para a segurança do sistema;
- Reduzir a dependência do elemento humano nas medidas e consequentemente diminuir a subjetividade;
- Oferecer modos mais rápidos e sistemáticos para obter métricas significativas;
- Compreensão sobre os mecanismos de composição de segurança.

Em especial, o relatório aponta como um possível ponto de partida, cinco possíveis áreas de pesquisa:

1. Modelos formais de métricas de segurança;
2. Coleta e análise de dados históricos;
3. Técnicas de avaliação utilizando Inteligência Artificial;
4. Métodos de medida concretos e praticáveis;
5. Componentes intrinsecamente mensuráveis.

Esta tese se baseia em duas dessas áreas de pesquisa: coleta e análise de dados históricos fornecidos pela University of Maryland e CAIS/RNP e métodos de medida concretos e praticáveis usando modelos estatísticos. Além disso, a presente pesquisa também envolve dois dos fatores sugeridos em (Jansen, 2010): o desenvolvimento de bons estimadores para a segurança do sistema e modos mais rápidos e sistemáticos para obtenção de métricas significativas.

2.3.2 Modelos para medir segurança

Diferentes modelos para medir segurança podem ser encontrados na literatura. Verendel (2009) propõe a seguinte classificação para esses métodos: i) métodos voltados para medir questões econômicas de segurança, ii) métodos que envolvem o desenvolvimento e seleção de métricas de segurança, iii) modelagem de componentes de um sistema e a relação com a segurança, iv) métodos para modelar as ameaças, motivações dos ataques e possíveis ações e v) modelos que tratam das vulnerabilidades de segurança do sistema. A seguir, alguns modelos são apresentados, assim como as principais deficiências e o relacionamento de tais modelos com a nossa proposta.

A primeira abordagem apresentada trata da avaliação quantitativa da segurança de um sistema baseada no relacionamento entre as vulnerabilidades de um computador que pode ser modelada por meio de grafos de ataque. A principal ideia dessa abordagem é o estudo sobre como as vulnerabilidades em um determinado nó da rede podem ser combinadas para a realização de um ataque.

A Figura 2.1 ilustra um grafo de ataque. O lado esquerdo representa a configuração da rede. O lado direito da Figura 2.1 mostra o respectivo grafo de ataque. São dois os tipos de

vértices, os círculos representam as explorações de vulnerabilidades (*exploits*) e os textos sem círculos representam as condições. Por exemplo, *rsh*(0,1) representa um login remoto da máquina 0 para a 1 e *trust*(0,1) significa que uma relação de confiança está estabelecida entra as máquinas 0 e 1. Os valores numéricos dentro e acima dos círculos representam a probabilidade de um ataque explorar a vulnerabilidade quando todas as condições exigidas são satisfeitas e a probabilidade de um ataque explorar a vulnerabilidade nesta rede em particular.

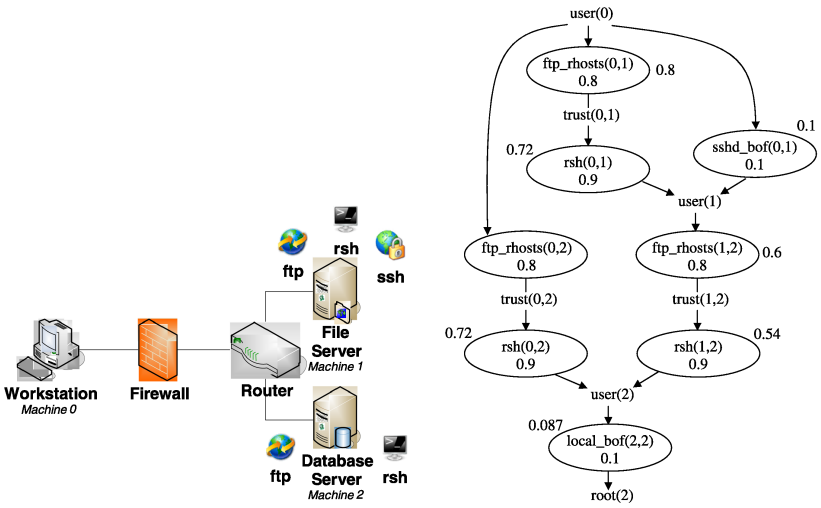


Figura 2.1: Exemplo de uma configuração de rede e seu respectivo grafo de ataque. Extraída de (Wang et al., 2008)

Diversos trabalhos usam grafos de ataques com o objetivo de medir a segurança de uma rede (Wang e Singhal, 2007), (Wang et al., 2008), (Feng e Jin-Shu, 2008) e (Kotenko, 2006). Apesar das vantagens proporcionadas pela análise da rede do ponto de vista dos grafos e da combinação de vulnerabilidades, os problemas computacionais relacionados à geração dos grafos (Frigault e Wang, 2008), o aumento exponencial do tamanho dos grafos segundo o tamanho da rede (Xie et al., 2009) e a ausência de validações do método utilizando dados reais, dificultam a adoção desse método em larga escala.

Outro método que avalia as vulnerabilidades de segurança presentes em um sistema é conhecido como CVSS (Mell et al., 2007). O método consiste em analisar o impacto da vulnerabilidade de acordo com três grupos de métricas (fundamentais, temporais e relacionadas ao ambiente) e gerar um valor entre 0 e 10, que avalia a severidade da vul-

nerabilidade. O CVSS atualmente está na versão 2, mas um grupo de pesquisa já está trabalhando em melhorias para uma terceira versão.

A exploração de vulnerabilidades é uma das principais fontes de ataques à segurança da informação. Existem diversas ferramentas no mercado, como o *Nessus Vulnerability Scanner*, desenvolvidas com o intuito de detectar vulnerabilidades em sistemas. Dessa forma, a facilidade de detecção de vulnerabilidades, aliada à criação de um método para quantificá-las, abre caminhos de pesquisa para a avaliação da segurança utilizando as vulnerabilidades presentes em um sistema.

Scarfone e Grance (2008) propõem um modelo para quantificar a segurança de computadores baseado no índice CVSS das vulnerabilidades, perfil de ataques ao longo do tempo e nos controles de segurança implementados (o uso de antivírus e firewall). Bhatt et al. (2011) apresentam uma abordagem para quantificar e calcular o perfil de risco de uma organização utilizando CVSS. Como a abordagem proposta leva em consideração a topologia da rede, os autores mostram, usando experimentos, que o método pode ser utilizado para a priorização de *patches* de segurança e componentes vulneráveis em uma rede. A abordagem proposta por (Jajodia et al., 2011) recomenda o uso do CVSS para a criação de um indicador de segurança para um computador. Porém, não fica claro como os autores tratam a questão da agregação dos valores do CVSS quando o computador possui mais de uma vulnerabilidade. Outra aplicação interessante do CVSS pode ser encontrada em (Wang et al., 2011). Os autores definem uma métrica de similaridade para comparar e classificar vulnerabilidades de segurança. Encontrar similaridades em um grupo de vulnerabilidades pode acelerar o processo de mitigação da vulnerabilidade, já que vulnerabilidades similares provavelmente exigem soluções similares.

As principais limitações nas abordagens que usam o CVSS como o principal método para quantificar a segurança de uma rede ou computador são relacionadas aos seguintes fatores: a dificuldade em agregar os valores encontrados com o cálculo do CVSS de modo eficiente e de acordo com as políticas de segurança da organização, e o fato de que a presença de vulnerabilidades de segurança em um sistema não necessariamente significa presença de ataques (Cukier e Panjwani, 2009).

Outra abordagem relacionada a criação de métodos para medir segurança é a aplicação de modelos probabilísticos para a estimação de risco. O trabalho desenvolvido por (Ahmed

et al., 2008), estima o risco de acontecer um ataque e o risco desse ataque ser propagado dentro da rede. Os modelos são construídos a partir da hipótese de que se um serviço possui um histórico de muitas vulnerabilidades ao longo do tempo, então a probabilidade do serviço se tornar vulnerável novamente no futuro é bem maior. O risco do ataque é calculado utilizando as vulnerabilidades de segurança presentes nos serviços através da modelagem das vulnerabilidades históricas e da criação da função de probabilidade do risco esperado. Já o risco do ataque ser propagado é calculado usando duas métricas extraídas de dados do *firewall* e de vulnerabilidades: propagação do ataque e imunidade do serviço. Os autores validaram os modelos e a hipótese principal usando experimentos com redes de diversos tamanhos e vulnerabilidades presentes na NVD.

Ryan e Ryan (2008) desenvolveram um método para medir a eficiência dos controles de segurança baseado na análise do tempo de falha (*time-failure analysis*). Esse é um conceito utilizado para modelar as falhas de um sistema ao longo do tempo. No caso da segurança da informação, o tempo de falha é o tempo que um sistema leva para ser atacado por um indivíduo ou grupo. A partir disso, são propostas métricas relacionadas ao gerenciamento de risco. Cada métrica representa uma função de probabilidade de falha do sistema sob diferentes condições. Analogamente, a pesquisa desenvolvida por (Leversage e James, 2008) sugere o uso do tempo médio para comprometimento (MTTC - *mean time-to-compromise*) como uma estimativa do tempo que um atacante com um determinado nível de habilidade leva para atacar com sucesso um sistema. Os autores modelam as transições de estados usando modelos predadorpresa e cadeias de Markov. Uma das limitações do trabalho é a de que somente os ataques remotos originados da Internet são considerados no modelo proposto.

A quantificação da segurança de redes usando probabilidades e cadeias de Markov também é descrita em (Wang et al., 2010). Os autores trabalham com a hipótese de que a quantificação da segurança de uma rede deve passar pela quantificação da segurança de cada computador, assim como, as métricas de segurança de uma rede serão formadas por métricas para cada computador.

Os autores criam um modelo de transição para cada um dos estados definidos de um computador (*Bom*, *Vulnerável*, *Atacado* e *Comprometido*). Os estados são monitorados a partir do uso de um sistema de prevenção de intrusões na rede em que se encontra

os computadores. A transição de estados é modelada usando um processo de Markov e métricas baseadas nessa transição, como a disponibilidade do computador no estado considerado *Bom* e o tempo entre a transição de estados como *Atacado* e *Comprometido*. Apesar de ser essencial para o desenvolvimento do modelo, a estado *Bom* do computador não é definido de maneira objetiva pelos autores.

Em linhas gerais, os modelos para medir segurança baseado no cálculo de probabilidades fornecem a teoria necessária para a investigação do assunto, contudo, a ausência de validação e comparação entre os modelos propostos na literatura dificulta a aplicação de tais modelos na prática.

É importante citar que validação é definida por Balci (1998) como o ato de verificar se o modelo, dentro de seu domínio de aplicação, se comporta de maneira satisfatória de acordo com os objetivos do estudo. Em outras palavras, a validação consiste em verificar se o modelo construído é o correto para a situação (Chrun, 2011). Dois tipos de informações são usadas para auxiliar a validação de modelos: especialistas no assunto e dados. Ao longo do texto serão apresentados exemplos de validações de modelos para quantificar segurança usando os diferentes tipos de informações.

Outro método empregado para analisar e agrupar os diferentes componentes de uma rede é o processo de análise hierárquica ou AHP. O AHP é um método de tomada de decisão multi-critério criado por Saaty (1990), no qual as decisões são tomadas em diferentes níveis e organizadas de maneira hierárquica. As entradas do método são números relacionados às decisões, como o tamanho de um objeto, notas escolares ou valores de métricas de segurança. As saídas do método são valores que representam o peso de cada decisão.

A aplicação do AHP para a avaliação da segurança da informação funciona da seguinte forma. A primeira fase consiste na seleção de um conjunto de métricas adequado para a descrição de um determinado objetivo de segurança. As soluções propostas na literatura recomendam o auxílio de especialistas para auxiliar em tal escolha. A próxima fase consiste na comparação paritária, isto é, par a par, das métricas, também com a ajuda de especialistas. Por meio dessa comparação são determinadas as importâncias relativas de cada métrica. O processo AHP através do cálculo do auto-vetor de prioridades, fornece o peso p_i da métrica, com $i = 1, 2, ..., n$ e n = número de métricas presentes no conjunto. De posse dos valores padronizados v_i das métricas selecionadas, é possível obter um índice

da seguinte forma:

$$I = \sum_{i=1}^{n} p_i \cdot (v_i) \tag{2.1}$$

A Figura 2.2 ilustra uma árvore de decisão em que o objetivo é a avaliação de segurança da informação com base em cinco diferentes critérios e seis alternativas (métricas de segurança). O índice é calculado primeiramente para cada critério. Com os valores para cada um dos critérios, é possível criar um novo índice para o topo do árvore (objetivo). O emprego de média aritmética ou o uso de pesos são duas possíveis alternativas. Construções do AHP para avaliação de segurança são encontrados em: (Bengtsson, 2007), (Zhen-yuan et al., 2009), (Alkussayer e Allen, 2011) e (Thalia et al., 2011).

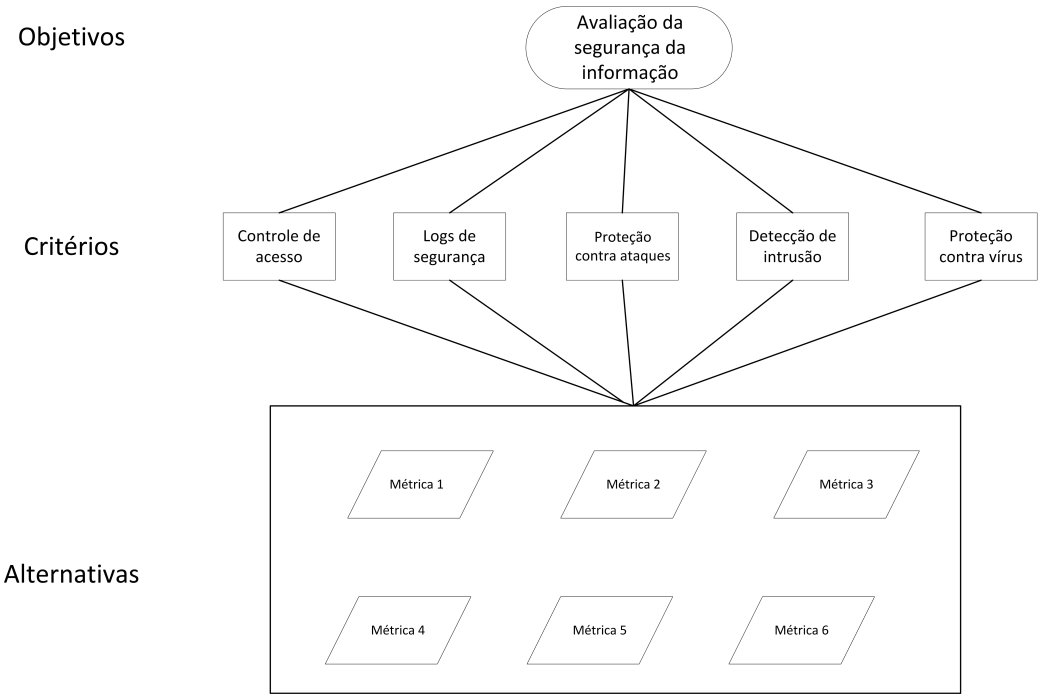


Figura 2.2: Uso do AHP para avaliação da segurança da informação. Adaptado de (Bengtsson, 2007)

Os métodos de quantificação de segurança usando AHP podem se tornar alternativas atraentes aos outros modelos, devido a simplicidade e o grande número de exemplos em outras áreas disponível na literatura. Contudo, a construção de tais modelos exige a padronização de escalas das métricas envolvidas, definição clara dos pesos iniciais dos critérios e alternativas e uma interpretação coerente dos resultados, pois a agregação de

valores pode ofuscar os detalhes do sistema investigado. Além disso, não é possível assumir que a segurança de um sistema possa ser sempre decomposta de maneira hierárquica, em termos de seus componentes mais simples.

A Tabela 2.2 apresenta um comparativo entre os modelos para medir segurança discutidos anteriormente.

Tabela 2.2: Tabela comparativa - Modelos para medir segurança

Abordagem	**Limitações**	**Referências**
Grafos de ataque	i) aumento exponencial do tamanho dos grafos segundo o tamanho da rede, ii) ausência de validações usando dados reais	(Kotenko, 2006), (Wang e Singhal, 2007), (Wang et al., 2008), (Feng e Jin-Shu, 2008), (Frigault e Wang, 2008) e (Xie et al., 2009)
Avaliar as vulnerabilidades de segurança usando CVSS	i) dificuldade em agregar os valores do CVSS, ii) presença de vulnerabilidades em um sistema pode não ser um indicativo de ataques	(Mell et al., 2007), (Scarfone e Grance, 2008), (Bhatt et al., 2011), (Jajodia et al., 2011) e (Wang et al., 2011)
Modelos probabilísticos	i) a ausência de validação e comparação entre os modelos propostos na literatura	(Ahmed et al., 2008), (Ryan, JJC and Ryan, 2008), (Leversage e James, 2008) e (Wang et al., 2010)
Processo de análise hierárquico (AHP)	i) padronização de escalas das métricas envolvidas, ii) definição clara dos pesos iniciais dos critérios, iii)hipótese de que a segurança pode ser decomposta de maneira hierárquica	(Bengtsson, 2007), (Zhen-yuan et al., 2009), (Alkussayer e Allen, 2011) e (Thalia et al., 2011)

2.3.3 Estudos empíricos sobre quantificação de segurança

Um dos objetivos deste trabalho é a identificação de métricas de seguranças relevantes. Alguns estudos similares foram propostos nesta área. A principal diferença entre tais

trabalhos e esta tese, reside no abordagem empírica introduzida e nos dados usados.

Cukier e Panjwani (2007) mostram que não é correto assumir que as atividades maliciosas registradas de ataques originados da Internet serão a única fonte de tráfego malicioso em direção a rede de uma organização. Dados coletados localmente são igualmente importantes para a caracterização dos ataques sofridos pela organização.

Com relação a predição de ataques, Panjwani et al. (2005) demonstraram que a varredura de portas não é um bom indicador de um futuro ataque. Porém, a varredura de portas combinada com a varredura de vulnerabilidades pode ser um indicador relevante de ataque. *Honeypots* [2] são usados como principal fonte de dados nesse trabalho. Outro trabalho que utiliza uma abordagem baseada em *honeypots* (Cukier e Panjwani, 2009) revela que a presença de um alto número de vulnerabilidades em serviços não necessariamente implica um alto número de conexões maliciosas. Além disso, os autores também encontraram evidências empíricas de que um alto número de vulnerabilidades em computadores não necessariamente significa um grande número de ataques em tais computadores.

Usando dados de uma competição internacional de defesa contra ataques à redes de computadores envolvendo mais de cem participantes, Holm et al. (2012) avaliaram dezoito métricas relacionadas à vulnerabilidades de segurança. Os autores mostram que as métricas que utilizam mais dados do CVSS possuem uma correlação maior com o tempo em que um sistema leva para ser atacado. Outro resultado encontrado é que os modelos que utilizam somente a vulnerabilidade mais crítica para compor a métrica são menos promissores do que os modelos que consideram todas as vulnerabilidades do sistema.

Neste trabalho, a avaliação empírica entre os fatores que afetam a ocorrência de incidentes de segurança será construída utilizando métodos estatísticos, como modelos de regressão linear múltipla. Abordagens semelhantes foram adotadas em diferentes estudos sobre segurança da informação. Arora et al. (2006) usam dados de *honeypots* e modelos de regressão para mostrar que em média ambas as vulnerabilidades não publicadas e publicadas atraem menos ataques do que as vulnerabilidades publicadas e com correções (*patches*). Em outro estudo, mas com uma abordagem semelhante, Arora et al. (2004) fornecem evidência empírica de que a divulgação de vulnerabilidades aumenta a frequência de ataques. Porém, a frequência dos ataques relacionada a tais vulnerabilidades diminui

[2] É um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido.

ao longo do tempo.

Wang et al. (2010), propõem uma abordagem baseada na criação de um modelo de regressão dinâmica para investigar as características das buscas que direcionam a procura por conhecimento em segurança da informação usando ferramentas de busca. Os autores mostram que a ocorrência de ataques influência a busca por conhecimento, já a divulgação de vulnerabilidades não afeta a busca.

Zhang et al. (2012a) avalia diversas percepções comuns sobre os fatores que influenciam o comprometimento de contas de usuários em duas universidades norte-americanas. Os autores utilizam regressão logística para entender e explicar o relacionamento entre os fatores e o comprometimento das contas de usuários.

Um dos tópicos de pesquisa tratados nesta tese é a investigação da relação entre métricas de segurança obtidas a partir de dados do IPS e o número de incidentes de segurança. Condon et al. (2008), (2007) descrevem a aplicação de séries temporais e modelos de confiabilidade de software em incidentes de segurança. Os resultados indicam que determinados incidentes são causados por vulnerabilidades bem definidas e podem ser facilmente corrigidos, porém, outros tipos de incidentes possuem um comportamento de propagação similar ao comportamento de doenças contagiosas, o que dificulta o tratamento.

Chrun et al. (2008a) apresentaram um método para extrair informações usando métricas obtidas de dados de um sistema de prevenção de intrusão. Os autores discutem uma abordagem que consiste em analisar a evolução das métricas de segurança por grupo de ataque com foco nos valores atípicos ou *outliers*. Usando um método similar, os mesmos autores (Chrun et al., 2008b) desenvolveram uma técnica baseada em dados de IPS para identificar e classificar potenciais computadores corrompidos.

2.3.4 Uso de questionários em segurança da informação

O uso de questionários para a investigação de problemas relacionados à segurança da informação é uma prática importante para a validação de modelos e investigação de hipóteses.

Alguns trabalhos nessa área incluem: (Kotulic e Clark, 2004), (Kajava e Savola, 2005), (Chrun, 2011), (Sademies, 2004), (Baker e Wallace, 2007) e (Bayuk, 2011). Conforme

mostrado em tais trabalhos, um problema comum dessa abordagem é a baixa taxa de resposta dos participantes. A sensação de insegurança gerada pela possibilidade de exposição da informação é um dos principais motivos para esse comportamento. Um meio de amenizar tal fenômeno é o uso de questionários online que permitem respostas anônimas. Estes questionários podem ser disseminados por meio de canais específicos de comunicação como listas de discussão.

Sademies (2004) propõe um estudo, em forma de questionário, sobre o uso de métricas de segurança em empresas finlandesas. O objetivo do trabalho foi revelar como o desenvolvimento e implementação das métricas era feito nas organizações. Os resultados mostraram que métricas técnicas e métricas relacionadas à avaliação de riscos são comumente utilizadas, mas sem o uso de automação e critérios para identificar as medidas mais importantes para a organização. Outro resultado indica que a maioria das organizações não usa as métricas de segurança como um processo, mas sim em aplicações isoladas. Outra pesquisa conduzida em empresas finlandesas (Kajava e Savola, 2005) teve como objetivo identificar como a segurança da informação é medida e avaliada. Os resultados mostraram que apesar de o uso de métricas de segurança estar ainda no começo, as empresas veem com bons olhos o uso de tais técnicas. Outro importante estudo foi conduzido por Baker e Wallace (2007). O objetivo do trabalho foi identificar como as organizações implementam controles de segurança. Foram compilados oitenta controles de segurança (uso de antivírus, *backup*, monitoração, entre outros) e os participantes indicaram quais dos controles foram implementados e também como foram implementados.

Chrun (2011) utilizou questionários online como uma das abordagens para validar um modelo de tomada de decisão para segurança. O modelo desenvolvido ao longo de seu trabalho exigia dois tipos de validações: i) se a decomposição escolhida para segurança (usuário, organização, ameaça e bens) representava a opinião da comunidade de segurança e ii) opinião da influência da segurança em cada uma das características definidas. Bayuk (2011) também usa questionários como forma de validação de modelos de segurança. A autora propõe que a segurança de um sistema não pode ser medida somente através da quantificação de atributos de seus componentes. Atributos relacionados a postura da organização, como missão e objetivos, detecção e resposta à incidentes e validação das entradas do sistema também devem fazer parte dos modelos para medir segurança. A

validação das hipóteses foi feita com base na análise de um questionário respondido por profissionais e pesquisadores da área de segurança.

A ideia principal do questionário desenvolvido nesta tese é a identificação de possíveis indicadores de segurança. A pergunta principal que irá guiar a construção do nosso questionário é: *"Quais métricas são utilizados para avaliar o nível de segurança de uma organização?"*

Com base nessa pergunta, outras investigações podem ser realizadas, como em que são baseados tais critérios? Qual é a diferença entre as organizações, perante o conjunto de indicadores utilizados? Devido a ausência de estudos empíricos e padronizações sobre o tema, essa abordagem pode ser usada para elucidar as estratégias utilizadas, identificar as preocupações das organizações e iniciar validações empíricas à partir das respostas.

Capítulo 3

Investigação e Análise Crítica de Métodos para Quantificar Segurança

Este capítulo apresenta uma análise crítica sobre trabalhos que propõem modelos de quantificação de segurança. Primeiramente, são discutidos três trabalhos anteriores sobre a análise e classificação da abordagem quantitativa para descrição da segurança de sistemas. O ponto chave da discussão desses trabalhos é a ausência de validação nos modelos propostos. A seguir, será mostrado um estudo para compreender algumas razões que influenciam esse fato, e que consiste em analisar os métodos presentes na literatura usando os seguintes critérios: o alvo da medida, ou seja, o sistema de interesse, a metodologia de obtenção da medida e os dados utilizados.

3.1 Análise de trabalhos anteriores

Vaughn et al. (2002) criaram a primeira classificação de métricas de segurança durante um simpósio realizado em Williamsburg, Virginia, EUA no ano de 2001. Os dois níveis principais, sugeridos durante o encontro ainda são utilizados em diversos trabalhos: métricas gerenciais e métricas para avaliação técnica. Porém, o trabalho desenvolvido por Villarubia et al. (2004) foi a primeira pesquisa voltada para a análise e classificação de métricas de segurança presentes na literatura. O principal objetivo dos autores é a criação de uma série de características para a classificação de métricas de segurança.

Antes de analisar as métricas existentes, Villarubia apresenta a seguinte classificação

usada no trabalho:

- Objetivo de segurança: os objetivos podem ser atrelados a confidencialidade, integridade, disponibilidade e autenticação;
- Área de controle: gerenciamento, operacional ou técnica;
- Dimensão temporal: métricas preventivas, de detecção, corretivas e relacionadas a recuperação do sistema;
- Público alvo: corpo técnico, gerentes e responsáveis pela organização e autoridades externas.

A partir desta classificação, os autores propõem um conjunto de seis características para uma determinada métrica. As três primeiras características são propriedades básicas de qualquer métrica. Já as três características restantes determinam se uma métrica foi ou não validada, o tipo de validação usada (teórica ou empírica) e se a métrica possui alguma ferramenta para automação de seu processo de coleta.

1. Objetividade / Subjetividade - define se a métrica é calcula por formulas matemáticas ou fornecidas pela interação humana;
2. Direta / Indireta - uma métrica direta não depende de qualquer outro atributo. Uma métrica indireta é obtida por meio de dados de um ou mais atributos;
3. Tempo de execução / Estática - define o momento em que a métrica pode ser calculada;
4. Validação teórica - se a validação é baseada em abordagens de teoria da medida ou abordagens axiomáticas ou baseada em propriedades do sistema;
5. Validação empírica - busca demonstrar se existe evidência real de que as métricas cumprem os objetivos definidos. A validação empírica pode ser baseada em experimentos, estudos de caso e pesquisas;
6. Automação - indica se a métrica possui suporte ou não a ferramentas de automação.

O próximo passo dos autores foi a seleção de um conjunto de métricas para a análise. De acordo com os autores, diversas métricas foram descartadas da pesquisa, pois não tinham informação suficiente para contemplar as características definidas. Ao final, 57 métricas de 8 trabalhos diferentes foram selecionadas. A lista completa pode ser encontrada em (Villarrubia et al., 2004). Os detalhes sobre a metodologia e os critérios de escolha dos trabalhos analisados foram omitidos.

Os resultados encontrados mostram que a maioria das métricas são diretas, formadas por somente um atributo. As métricas indiretas geralmente fornecem mais informação e são o ponto de partida para o desenvolvimento de indicadores de segurança. Outro resultado interessante é a ausência de validação (teórica e empírica) e automação nas métricas analisadas. Nenhuma métrica investigada foi validada de maneira teórica e somente uma foi validada de maneira empírica. Com relação a automação, somente uma métrica possui algum tipo de suporte para essa atividade. Esse resultado evidencia que o cenário das métricas de segurança em 2004 envolvia o desenvolvimento de pesquisa em validação teórica, empírica e suporte a automação.

Em 2009, Verendel (2009) apresentou um levantamento bibliográfico sobre a análise e representação quantitativa de segurança. O trabalho é uma extensão do trabalho anterior, desenvolvido por Villarrubia et al. (2004), pois trata de vários tipos de modelos de quantificação de segurança, não somente o uso de métricas. A hipótese discutida pelo autor é se a segurança pode ser representada corretamente utilizando métodos quantitativos.

Para avaliar essa hipótese, o autor analisou 90 trabalhos entre os anos de 1981 e 2008 e os classificou com relação a perspectivas de segurança, alvos de quantificação, suposições básicas e os tipos de validações.

A metodologia empregada para a seleção dos trabalhos incluiu:

- Coleta inicial de artigos, usando diversas fontes de dados e palavras chaves da área. O material inicial possuía 140 artigos;
- A data de publicação dos trabalhos foi limitada entre 1981 e 2008;
- Foram incluídos somente trabalhos relacionados a segurança de sistemas em ambientes reais (também conhecida como segurança operacional), como por exemplo a

infraestrutura de uma organização. Análises quantitativas sobre algoritmos criptográficos, fluxos de informação e questões de privacidade foram excluídas da análise;

- Diversos trabalhos foram descartados por apresentarem ideias similares ou aparecerem em mais de uma publicação;

Com base na análise dos trabalhos, o autor propõe a seguinte classificação:

- Perspectiva - são quatro as perspectivas definidas: CIA (confidencialidade, integridade e autenticidade), econômica, baseada em teorias de confiabilidade e dependabilidade e outras;

- Alvo - os cinco possíveis alvos para os métodos de quantificação são, econômico, *frameworks* sobre como desenvolver e selecionar métodos de quantificação, componentes e sua estrutura no sistema em consideração, ameaças e a existência de vulnerabilidades;

- Suposições - independência de eventos, assumir que o sistema em questão é invariante ao longo do tempo ou entre diferentes ambientes e por fim, supor que a decomposição do do sistema é feita de maneira simples, utilizando somente a descrição de seus componentes;

- Validação - uso de hipóteses, validação empírica, simulações e validação teórica.

O primeiro resultado significativo obtido pelos autores trata das suposições que foram consideradas nos trabalhos. A maioria dos métodos emprega suposições não coerentes com o sistema avaliado e também sem base empírica. Utilizar tais suposições sem a validação necessária pode comprometer a aplicação dos modelos.

Outro resultado, similar ao já encontrado em (Villarrubia et al., 2004), comprova que a minoria dos trabalhos emprega o método empírico de validação. Além disso, o foco desses métodos reside em demonstrar como eles podem ser aplicados ao invés de validar como a segurança é representada pelos atributos de interesse. De acordo com os autores, os trabalhos relacionados à modelagem de vulnerabilidades foram os únicos que apresentaram resultados empíricos convincentes. A ausência de comparação entre os métodos que usam o

mesmo tipo de metodologia ou experimentos com os mesmos dados também foi destacado pelo autor.

Com base nos resultados, Verendel faz diversas sugestões para melhorar a compreensão dos métodos quantitativos aplicados à segurança da informação: comparar os métodos usando os mesmos conjuntos de dados, melhorar a colaboração entre os diversos tópicos de pesquisa, exigir melhores requisitos de validação e estabilizar a coleta e disponibilidade de diferentes conjuntos de dados.

Outro trabalho que investiga a literatura sobre métodos de quantificação de segurança é apresentado em (Rudolph e Schwarz, 2012). Os autores analisam o estado da arte dos trabalhos dessa área, com o objetivo de caracterizar as estratégias de quantificação, o nível de maturidade das métricas e os obstáculos técnicos ou conceitais que eventualmente prejudicam o progresso da área.

A pesquisa estende a classificação definida em (Verendel, 2009), incluindo atributos como escopo de quantificação, procedimento de quantificação, ciclo de vida e suporte a ferramentas. Diferentemente do trabalho de Verendel que é restrito a trabalhos relacionados a segurança de sistemas em ambientes reais, em (Rudolph e Schwarz, 2012) os autores incluem áreas como o desenvolvimento de software seguro nos critérios de busca de artigo. Além disso, a classificação proposta pelos autores auxilia a escolha de uma determinada métrica de segurança para um determinado cenário.

A metodologia empregada para a seleção dos 43 trabalhos analisados consiste em:

1. Criar uma base inicial de trabalhos, usando os portais acadêmicos Google Scholar e IEEE Xplore;

2. Aumentar a base inicial por meio da inserção de artigos encontrados em listas de publicações relacionadas;

3. Filtrar os trabalhos pré-selecionados usando como referência o título, resumo e conclusão;

4. Investigar cuidadosamente os trabalhos selecionados encontrados no passo 3) - excluir trabalhos não relacionados ou em fase inicial de desenvolvimento.

A partir da análise dos trabalhos selecionados, os autores desenvolveram a seguinte classificação para as métricas de segurança:

- Custo (*Cost*) - envolve métricas que estimam o custo exigido para um ataque, os custos para a prevenção de ataques e os custos de remediação;
- Probabilidade (*Probability*) - contém métricas que estimam a probabilidade de um ataque acontecer;
- Eficiência (*Efficiency and Rigor*) - métricas que possuem o objetivo de medir ou estimar a taxa de sucesso das medidas tomadas contra os ataques;
- Conformidade (*Compliance*) - lista as métricas que avaliam o nível em que os requisitos de segurança são cumpridos sob o ponto de vista de um determinado sistema ou processo;
- Cobertura do alvo (*Target coverage*) - inclui as métricas para medir a fração (ou o número absoluto) de alvos de segurança que satisfazem um determinado critério de segurança.

A Figura 3.1 ilustra a árvore de classificação proposta pelos autores. Note que as categorias principais possuem sub-categorias e em alguns casos três níveis de classificação (*cost -> attack cost -> required time*) antes das métricas propriamente ditas. Isso demonstra a grande diversidade de trabalhos na área e a dificuldade em padronizar determinados métodos, conforme já discutido em (Verendel, 2009).

Esta classificação permitiu aos autores algumas conclusões importantes sobre os trabalhos investigados. Novamente foi possível mostrar que não há resultados empíricos que confirmem a correlação entre as métricas de segurança e os alvos da medida, ou seja, a maioria das métricas propostas não foi aplicada, testada ou sequer aceita na prática. Desta forma, trabalhos que discutam a significância das métricas em ambientes reais são um ponto de partida importante para esse objetivo. Outros resultados encontrados incluem: a ausência de métricas com suporte à ferramentas de automação de coleta de dados e a maioria das métricas não trata de maneira adequada a oscilação dos objetivos de segurança

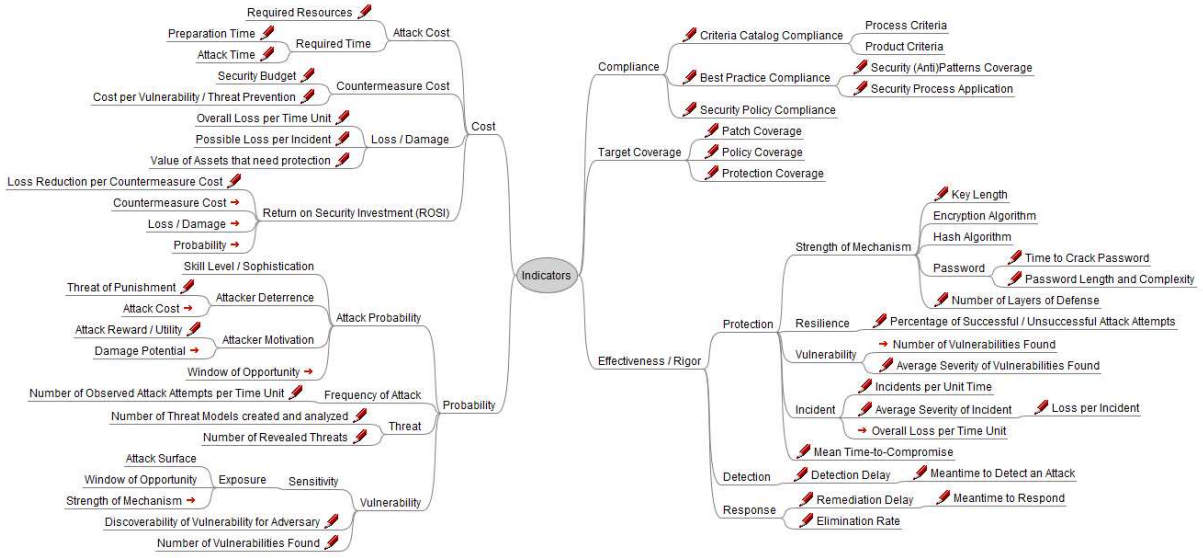


Figura 3.1: Categorias de métricas proposta por Rudolph e Schwarz. Extraída de (Rudolph e Schwarz, 2012)

definidos pelas organizações e também as variações das ameaças de segurança, de acordo com vários fatores, como o tempo ou motivações para o ataque.

A Tabela 3.1 sumariza as principais características dos três trabalhos estudados. Note que os trabalhos apresentam conclusões similares sobre o uso de métricas de segurança. O grande problema ainda é a ausência de validação dos métodos propostos usando dados empíricos. Em outras palavras, porque tais métodos não são validados? Porque existem poucas pesquisas usando dados empíricos? A compreensão desses problemas pode auxiliar o desenvolvimento de trabalhos futuros na área. Porém, como os três trabalhos investigados não fornecem subsídios suficientes para responder estas questões, na próxima seção será apresentada uma pesquisa que busca entender possíveis origens para esses problemas. Essa análise é uma das contribuições deste trabalho.

3.2 Abordagem proposta

Conforme descrito na seção anterior, o objetivo desse estudo é investigar as razões que envolvem a ausência de validação dos métodos para quantificar segurança. A abordagem consiste em avaliar os diversos modelos propostos na literatura de acordo com os conceitos básicos de quantificação de informação.

Tabela 3.1: Trabalhos anteriores sobre análise e classificação de métricas de segurança

Trabalho	Ano	Trabalhos analisados	Metodologia	Objetivo	Classificação proposta	Principais resultados
Villarrubia et al.	2004	8	Criação da classificação e depois a análise dos trabalhos	Propor uma classificação para métricas de segurança	i) Objetividade ii) Direta / Indireta iii) Tempo de execução iv) Validação teórica v) Validação empírica vi) Automação	i) maioria das métricas são diretas ii) ausência de validação (teórica e empírica) iii) ausência de suporte à automação
Verendel	2009	90	Classificação criada a partir da análise dos trabalhos	Análise crítica de trabalhos sobre quantificação de segurança	i) Perspectiva ii) Alvo iii) Suposições iv) Validação	i) maioria dos métodos emprega suposições não coerentes com o sistema avaliado e sem base empírica ii) ausência de validações empíricas iii) ausência de comparação entre os métodos que usam o mesmo tipo de metodologia ou dados
Rudolph e Schwarz	2012	43	Classificação criada a partir da análise dos trabalhos	Propor uma nova classificação para métrica de segurança	i) Custo ii) Probabilidade iii) Eficiência iv) Conformidade v) Cobertura do alvo	i) ausência de resultados empíricos que confirmem a correlação entre as métricas e os alvos da medida ii) a ausência de métricas com suporte à ferramentas de automação iii) maioria das métricas não trata as variações das ameaças de segurança e objetivos de segurança

Métricas de segurança nada mais são do que o resultado de um processo de quantificação de algum aspecto da segurança da informação. Esse processo de quantificação possui certas características e deve obedecer a determinadas regras a fim de operar de maneira correta. Porém, quais são essas regras e características? Como avaliar se o processo está no caminho certo? A teoria sobre construção de indicadores quantitativos pode ser usada para entender como as informações relativas a processos ou sistemas de qualquer natureza podem ser extraídas eficientemente.

Indicadores consistem de informação que indicam mudança. Um indicador é um fator ou variável quantitativa ou qualitativa que fornece um modo simples e confiável para exibir as alterações vinculadas a uma determinada intervenção. Indicadores permitem a percepção de diferenças, melhorias ou desenvolvimentos relacionados a uma alteração desejada em um certo contexto. O uso de indicadores é muito comum, seja nas ciências exatas ou sociais. Na economia, indicadores como a taxa de desemprego e o produto interno bruto são utilizados para avaliar a situação econômica de um país.

A Figura 3.2 ilustra parte da metodologia relacionada ao desenvolvimento de indica-

dores quantitativos. O sistema ou processo de interesse se encontra no centro e é a partir dele que as informações serão geradas. A observação do processo, envolve, sob o ponto de vista do pesquisador, questionamentos sobre o funcionamento, regras, organização ou comportamento do sistema em questão. Esta observação faz parte da primeira fase de extração de informações. A segunda fase consiste em como obter os dados que serão utilizados para gerar as informações. Nessa fase, é importante que a metodologia seja estável, bem definida e reprodutível, de modo que, quando repetida em circunstâncias semelhantes, os dados coletados sejam coerentes entre si. Por fim, a fase de obtenção da informação é baseada na reelaboração dos dados brutos para a visualização da informação (por exemplo, reordenando-os de diversos modos, efetuando algum tipo de cálculo ou aplicando alguma análise estatística), interpretação e compreensão da informação obtida e, em alguns casos, o refinamento em uma ou mais das etapas anteriores.

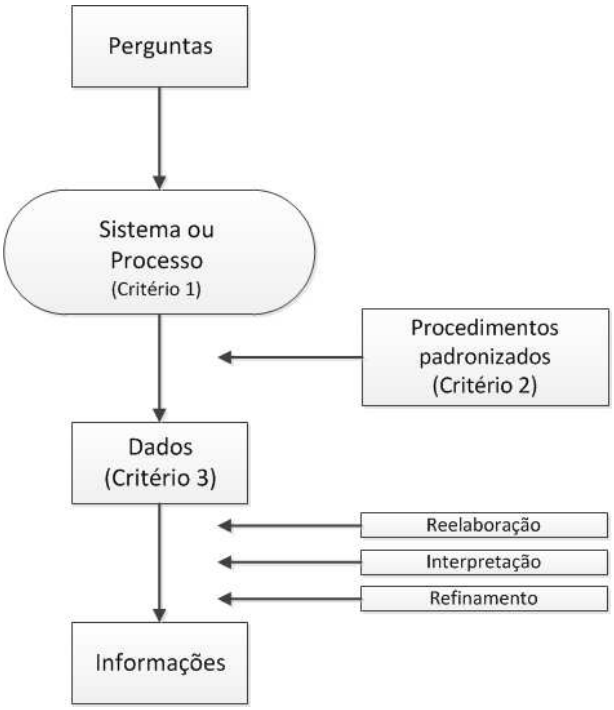


Figura 3.2: Diagrama para extração de informações relativas a processos ou sistemas de qualquer natureza. Adaptado de (Trzesniak, 1998)

Desta forma, três critérios devem ser devidamente definidos: o alvo da medida, que representa, o sistema ou processo de interesse, a metodologia de obtenção da medida, representado pelos procedimentos padronizados e, por fim, os dados utilizados. Suponha

que o processo de interesse seja os ataques direcionados à organização. Uma possível metodologia de obtenção dos dados seria o cálculo do número de ataques detectados pela organização. Os dados utilizados poderiam ser obtidos através dos registros do sistema de detecção de intrusão da organização. Note que o exemplo ilustra a clareza e coerência dos critérios definidos. Porém, isso não garante que as informações obtidas são correlacionadas com o processo ou ainda são suficientes para medi-lo. Validações devem ser feitas para investigar tais fatos. Dessa forma, a grande vantagem em analisar os modelos de segurança usando os três critérios básicos de quantificação de informação é a possibilidade de detectar se as características mínimas de um determinado método de quantificação foram respeitadas.

As seguintes questões serão investigadas em um conjunto de 57 trabalhos relacionados:

1. Relação entre as metodologias empregadas para quantificar segurança e o sistema em questão.

2. Relação entre os dados utilizados e o sistema em questão.

3. Relação entre as metodologias empregadas para quantificar segurança e os dados utilizados.

3.2.1 Método de coleta dos trabalhos

O material inicial consistia de 92 documentos publicados em revistas científicas, anais de congressos internacionais e nacionais, livros e relatórios técnicos. Esse material era composto pelas referências bibliográficas utilizadas ao longo do mestrado e dos dois primeiros anos de estudo do doutorado. O principal critério utilizado para guiar as modificações na base de dados inicial foi o seguinte: "Analisar os trabalhos que propõem métricas para avaliar a segurança de uma organização ou que ao menos estimem parte da segurança organizacional utilizando métodos quantitativos".

Com base nesse critério foi feita uma inspeção no resumo, palavras-chave e conclusão de cada um dos 92 documentos iniciais. Além disso, foram realizadas pesquisas nos principais portais acadêmicos (*IEEE Xplore*, *ACM Digital Library*, *SpringerLink*, *Science Direct*, *Wiley* e *Google Scholar*) usando várias combinações de palavras-chave ligadas ao critério de

busca inicial, como "(Security Metrics OR Information Security Metrics) AND (Enterprise Security Metrics OR Enterprise Level Security Metrics)".

Assim como no levantamento realizado por Verendel (2009), somente trabalhos relacionados a segurança operacional foram incluídos. Além disso, como o critério central envolve a seleção de trabalhos que apresentam métricas para avaliar a segurança de uma organização ou que no mínimo descrevam parte da segurança organizacional empregando uma abordagem quantitativa, excluímos documentos relacionados a quantificação do impacto econômico, métricas de segurança de software e artigos redundantes. Também foram excluídos documentos sobre modelos de descoberta de vulnerabilidades, pois, conforme observado por Verendel (2009), a validação e comparação usando diferentes conjuntos de dados é uma prática comum neste tipo de trabalho.

Finalmente, após os refinamentos citados e cuidadosa inspeção manual, 57 documentos, publicados entre 2001 e 2012, foram selecionados para a investigação. A tabela com todos os trabalhos investigados pode ser encontrada no Apêndice A.

Conforme discutido em (Verendel, 2009), esse tipo de seleção de material, apesar de ser baseada em diversos critérios, depende também do julgamento do responsável em selecionar os trabalhos, assim como dos limites de esforço dos envolvidos na busca. Logo, acreditamos que os principais trabalhos da área foram selecionados para a pesquisa.

3.2.2 Classificação proposta

Os trabalhos foram classificados de acordo com os seguintes critérios: alvo da medida, que representa, o sistema ou processo de interesse, a metodologia de obtenção da medida e os dados utilizados. Após a análise dos trabalhos, foi criada uma taxonomia para cada um dos critérios. É importante frisar que devido a multidisciplinaridade que envolve a segurança da informação, os trabalhos podem pertencer a mais de uma categoria dentro da mesma classificação.

A classificação do sistema ou processo de interesse é dada por:

- **Segurança da rede (NET):** inclui trabalhos que avaliam a segurança da rede como um todo. Tipicamente mais de um componente é analisado.

- **Segurança da organização ou sistema (ORG):** similarmente, inclui trabalhos que avaliam não só a rede, mas a segurança da organização em geral.

- **Risco (RSK):** trabalhos que avaliam certos tipos de risco associados à segurança. Por exemplo, um processo de interesse pode ser o risco associado ao valor esperado das perdas (financeiras ou de outros tipos) relacionadas aos ataques à organização.

- **Eficiência (EFF):** quando o processo de interesse está relacionado a quantificação da eficiência de controles de segurança. Por exemplo, a avaliação da eficiência de medidas comuns de segurança, como atualizações, virtualização e remoção de softwares não utilizados.

- **Outros (SPE):** sistemas ou processos específicos, mas diferente dos anteriores, como o comprometimento de contas de usuários.

A classificação da metodologia inclui:

- **Modelos probabilísticos (PRO):** modelagem da segurança através de processos estocásticos para estudar a propagação de ataques, modelar as falhas de um sistema ao longo do tempo, estimar o tempo que um atacante com um determinado nível de habilidade leva para atacar com sucesso um sistema entre outros.

- **Estatística (STA):** análise e interpretação de dados usando técnicas estatísticas, como modelos de regressão linear, correlação e séries temporais.

- **Métricas simples (MET):** utilização de métricas de segurança que envolvem cálculos simples, como por exemplo, porcentagem de incidentes de segurança investigados e número de usuários com privilégios de administrador por máquina.

- **Grafos (GRA):** aplicação de grafos de ataque e variações para modelar como as vulnerabilidades de um determinado nó da rede podem ser combinadas para a realização de um ataque.

- **Técnicas estruturadas - (STR):** decomposição hierárquica ou estruturada de fatores, como o AHP.

- **Outros - (OTH):** Outros métodos matemáticos, como por exemplo o uso de cálculo diferencial e integral e álgebra linear.

A classificação dos dados é composta por:

- **Exemplos fictícios (EXE):** exemplos criados com o propósito de ilustrar a viabilidade da proposta.
- **Sistemas em funcionamento (REA):** dados extraídos de ambientes reais, como *honeypots*, registros de incidentes de Universidades e etc.
- **Vulnerabilidades (VUL):** bases de dados de vulnerabilidades de segurança, como por exemplo o NVD.
- **Opiniões de especialistas / Questionários - (QUE):** dados coletados de questionários ou da opinião de especialistas na área.
- **Teóricos (THE):** modelos teóricos que não usam quaisquer tipos de dados.

3.2.3 Resultados e discussão

Para avaliar se a ausência de validação dos métodos para medir segurança está relacionada aos três critérios básicos da quantificação de informação, é necessário analisar, em cada um dos trabalhos, o relacionamento dos critérios entre si.

A análise da relação entre as metodologias empregadas para quantificar segurança e o processo medido é o primeiro passo da investigação. A ideia principal consiste em compreender como os diferentes métodos são usados em cada um dos processos identificados. A relação entre os dados utilizados e o processo medido também deve ser estudada. Em outras palavras, os tipos de dados usados são suficientes para extrair as informações relativas ao objetivo da medida? A última análise desenvolvida contempla a relação entre as metodologias empregadas para quantificar segurança e os dados utilizados. Os tipos de dados usados nos trabalhos variam de acordo com a metodologia de quantificação? Esse estudo pode esclarecer se determinadas metodologias tendem a usar certos tipos de dados, por exemplo, quais tipos de dados são empregado pelos métodos probabilísticos?

O levantamento bibliográfico realizado fornece uma perspectiva simples sobre quais metodologias para quantificar segurança são aplicadas nos diferentes sistemas ou processos de interesse. A Tabela 3.2 mostra o relacionamento entre esses dois critérios.

Tabela 3.2: Como as diferentes metodologias para quantificar segurança são aplicadas nos sistemas ou processos

	PRO	STA	MET	GRA	STR	OTH	Total
NET	3	0	5	8	3	3	22
ORG	11	2	7	4	3	6	33
RSK	0	1	3	1	0	0	5
EFF	1	2	4	0	0	0	7
SPE	5	9	15	3	2	3	37

As abordagens relacionadas a risco (RSK) e eficiência (EFF) foram as menos representativas no estudo. Grande parte da literatura associada a análise de risco envolve o estudo de fatores econômicos como o cálculo de métricas como o *Return on Investment* (ROI) e *Return on Security Investment* (ROSI). Mesmo considerando a exclusão dos trabalhos com viés econômico do levantamento bibliográfico, ainda existe espaço para pesquisa quando o alvo é a quantificação de risco, mas sem considerar a perspectiva econômica. Dos três trabalhos investigados, um deles propõem um conjunto de métricas para minimizar os riscos de ataques à organização (Boyer e McQueen, 2008), o outro trabalho estima o risco baseado em melhorias no CVSS (Bhatt et al., 2011) e o outro propõe um modelo para auxiliar as tomadas de decisões relacionadas à TIC (Chrun, 2011). O objetivo da avaliação da eficiência de controles de segurança é fornecer recursos para um profissional de segurança comparar as diversas medidas propostas na literatura e assim decidir quais implementar. Os resultados encontrados na Tabela 3.2, mostram que, apesar de importante, essa área ainda é pouco explorada pelos pesquisadores. Dois trabalhos, em especial, se destacam por apresentar estudos sobre a eficiência de medidas comuns de segurança como o uso de ferramentas de virtualização, senhas de administrador seguras, aplicação de atualização de segurança, entre outros (Harrison e White, 2010) e métricas para caracterizar a eficiência de políticas de segurança da informação (Goel e Chengalur-Smith, 2010).

Dessa forma, com relação ao alvo da medida ou sistema de interesse, os trabalhos

ficaram polarizados entre as seguintes áreas: segurança da rede (NET), segurança da organização (ORG) e alvos específicos (SPE). De acordo com a Tabela 3.2, os seguintes resultados, para tais áreas, podem ser notados:

- NET: quase 60% dos trabalhos envolvem o uso de métricas simples ou grafos. Como o alvo da medida é a segurança da rede, muitos trabalhos usam grafos de ataque para modelar a rede e estudar como as vulnerabilidades de um determinado nó podem ser combinadas para a realização de um ataque.

- ORG: mais de 54% dos trabalhos usam modelos probabilísticos ou métricas simples. Quando o objetivo é medir a segurança da organização, o uso de somente grafos de ataque não é suficiente. Dessa forma, outros métodos são utilizados e em especial o uso de modelos probabilísticos para a avaliação da vulnerabilidade, confiabilidade, ameaças e consequências se destaca.

- SPE: mais de 64% dos trabalhos utilizam métodos estatísticos ou métricas simples. Nenhum método estatístico foi usado nos trabalhos em que o alvo é a segurança da rede. Já para a segurança da organização, somente dois trabalhos usavam tais métodos. Esse número aumentou para nove nos trabalhos em que o sistema a ser medido é um alvo específico de segurança da informação. Isso pode ser considerado um bom sinal, já que a aplicação de métodos estatísticos, como regressão linear, séries temporais e testes de correlação indica um esforço dos pesquisadores no uso de dados empíricos para quantificação de segurança.

Conforme discutido anteriormente, a definição adequada do alvo da medida, da metodologia e dos dados utilizados é um passo importante para a construção de processos de quantificação. No levantamento realizado, os trabalhos sobre segurança da rede, compreendem, de maneira geral, a quantificação da segurança de uma rede como um todo. Essa abordagem envolve inúmeros aspectos desde os técnicos (equipamentos, políticas e controles de segurança), gerenciais (contratação de pessoal e orçamento) e o fator humano. Consequentemente, a criação de um modelo que visa quantificar a segurança da rede como um todo pode ser complexo demais e não refletir a segurança como deveria.

Vários trabalhos discutem e fundamentam essa questão: (Bayuk, 2011), (Jansen, 2010), (Paul E. Black e Souppaya, 2008), (Pfleeger, 2009), (Pfleeger e Cunningham, 2010) e (Stolfo et al., 2011). De acordo com essa linha de pensamento, o mais sensato seria avaliar processos ou sistemas mais simples e específicos e deste ponto em diante tirar conclusões sobre a segurança da rede. A economia é quantificada dessa forma. Existem diversos indicadores econômicos e cada um deles descreve um determinado aspecto do todo. Uma análise econômica é feita com o auxílio de diversos indicadores. Portanto, espera-se que a análise sobre a segurança de toda uma rede ou organização envolva também vários fatores. Os principais problemas consistiriam então em como identificar, validar e correlacionar estes fatores. A Figura 3.3 mostra que 21 dos 57 trabalhos analisados são relacionados a quantificação de alvos específicos de segurança.

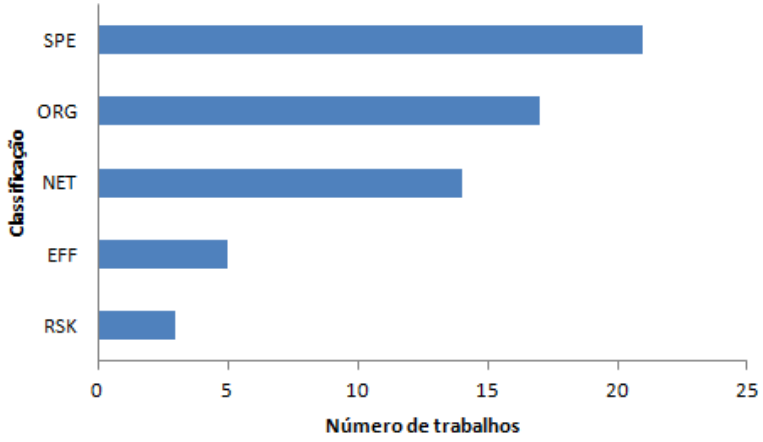


Figura 3.3: Distribuição dos trabalhos analisados de acordo com o alvo da medida

A Tabela 3.3, mostra o relacionamento entre os tipos de dados utilizados e o processo medido. Importantes observações podem ser feitas a partir da análise dessa tabela. Os trabalhos relacionados à quantificação da segurança da rede (NET) usam em sua grande maioria dados oriundos de exemplos fictícios (EXE) ou são completamente teóricos (THE). Nenhum trabalho utilizou dados reais (REA) ou de questionários (QUE). Isso pode indicar problemas na validação dos modelos propostos. Analogamente, os trabalhos sobre quantificação da segurança da organização (ORG) também usam na maioria das vezes (72%) dados de exemplos fictícios ou nenhum tipo de dado. Somente três trabalhos envolvem o uso de dados reais. Porém, dentre esses trabalhos, dois deles (Weissmann, 2005) e

(Khan e Hussain, 2010) não fornecem uma descrição clara dos conjuntos de dados usados, comprometendo a reprodução e comparação dos métodos.

Diferentemente dos trabalhos sobre segurança de rede e segurança da organização, os resultados presentes na Tabela 3.3 também apontam que os alvos de medida relacionados a eficiência, risco e alvos específicos possuem uma incidência maior de estudos com dados reais e questionários. A análise mostra uma tendência de utilização de dados reais nos trabalhos analisados quando os alvos da medida não incluem sistemas genéricos como segurança da rede ou segurança da organização. Esses resultados sugerem que a definição do processo ou sistema de segurança que será medido influencia nos tipos de dados utilizados. Uma definição abrangente ou imprecisa pode implicar na dificuldade de obtenção de dados, gerando trabalhos sem nenhum suporte à dados ou somente com exemplos fictícios. Conforme notado em (Verendel, 2009), apesar da importância do desenvolvimento de trabalhos teóricos na área de quantificação de segurança, o uso de dados reais é crucial para permitir novos avanços nessa área.

Tabela 3.3: Relação entre os dados utilizados e o processo medido

	EXE	REA	VUL	QUE	THE	Total
NET	10	0	1	0	3	14
ORG	8	3	1	1	5	18
RSK	0	2	1	1	1	5
EFF	1	2	0	2	1	6
SPE	5	9	2	0	6	22

A Tabela 3.4, apresenta a relação entre os tipos de dados utilizados e a metodologia de quantificação empregada. É possível notar quais métodos estão relacionados a determinados tipos de dados, como ao uso de dados reais. De acordo com o levantamento feito neste trabalho, o uso de métricas simples (MET) e métodos estatísticos (STA) são os alvos de medida que possuem a maior incidência do uso de dados reais e questionários. Metodologias que envolvem o uso de grafos (GRA) e decomposição hierárquica de fatores (STR) não utilizaram dados reais em suas propostas. Além disso, modelos probabilísticos (PRO) e baseados em grafos costumam adotar somente exemplos fictícios em seus modelos de quantificação.

Ainda de acordo com a Tabela 3.4, apesar do baixo número, os dados relacionados a vulnerabilidades (VUL) aparecem ao menos uma vez em todas metodologias. As diversas bases de vulnerabilidades (NVD (NIST, 2013), CVE (Mitre, 2013)) disponibilizadas para o público, aliado ao uso do CVSS certamente contribuiu para esse resultado. Assim, o baixo número de trabalhos encontrados em nosso estudo e a alta disponibilidade de informações relacionadas a vulnerabilidade de segurança mostram que as pesquisas nessa área ainda podem ser expandidas. Trabalhos puramente teóricos (THE), sem nenhum uso de dados, também aparecem ao menos uma vez em todos as metodologias. Em especial, métodos probabilísticos, métricas simples e grafos não usam quaisquer tipos de dados na maioria das vezes.

Tabela 3.4: Relação entre os dados utilizados e a metodologia

	EXE	REA	VUL	QUE	THE	Total
PRO	11	2	1	0	6	20
STA	0	10	2	1	1	14
MET	9	12	4	2	8	35
GRA	9	0	1	0	6	16
STR	6	0	1	0	1	8
OTH	7	1	2	0	2	12

O principal objetivo do levantamento e análise crítica desses trabalhos é estudar as razões que envolvem a ausência de validação dos métodos para quantificar segurança. A compreensão dessas razões pode indicar os próximos caminhos de pesquisa na área de quantificação de segurança. Os resultados encontrados ao longo da análise mostram que:

1. Grande parte dos modelos investigados para quantificar segurança buscam medir alvos genéricos e complexos, como medir a segurança da rede ou a segurança da organização;

2. Na maioria das vezes, os modelos que buscam medir a segurança da rede ou a segurança da organização estão vinculados a metodologias que não utilizam dados reais (modelos probabilísticos, grafos e técnicas estruturadas) em sua construção;

3. Dentre os modelos estudados, a aplicação de métodos estatísticos e uso de dados reais aparece com maior frequência nos trabalhos que propõem a quantificação de alvos específicos. Porém, a pesquisa nessa área ainda está no começo, visto que muitos trabalhos ainda utilizam exemplos fictícios ou propõem novos modelos, sem o uso de qualquer tipo de dado;

4. Poucos trabalhos investigados usam dados das bases públicas de vulnerabilidades de segurança. A maioria dos trabalhos que usam esses dados são voltados para predição de vulnerabilidades em software ou comportamentos relacionados a divulgação de vulnerabilidades;

5. Outra área pouco explorada foi a avaliação da eficiência de controles de segurança. Trabalhos como (Harrison e White, 2010) e (Goel e Chengalur-Smith, 2010) que propõem a investigação da eficiência de medidas comuns de segurança poderiam ser estendidos e validados por outros pesquisadores;

6. A maioria dos dados reais são provenientes de universidades e *honeypots*. Poucos trabalhos usaram conjuntos de dados de maneira compartilhada ou realizaram comparações. O estudo conduzido por (Zhang et al., 2012a), no qual dados de contas de usuários corrompidas em duas universidades norte-americanas são investigados, é uma exceção.

7. Muitas vezes, a escolha de um certo alvo de medida seguida de uma determinada metodologia, pode resultar em modelo com sérias restrições para obtenção de dados e consequentemente com problemas de validações. Por exemplo, o modelo definido em (Jonsson e Pirzadeh, 2011), sugere medir a segurança da organização usando um modelo probabilístico composto por diversos atributos do sistema e do ambiente em que a organização está inserida. Contudo, a quantidade e complexidade de atributos dificulta a aplicação do modelo em ambientes reais.

Com base em tais resultados, é possível afirmar que um dos caminhos viáveis de pesquisa em quantificação de segurança é o estudo e discussão de alvos mais simples e específicos e o uso de metodologias capazes de suportar dados reais para eventuais verificações e validações. Assim, o próximo capítulo mostra dois estudos em alvos específicos (relação

entre métricas obtidas a partir de dados do sistema de prevenção de intrusão e fatores que influenciam a ocorrência de incidentes de segurança) usando técnicas estatísticas (modelos de regressão, testes de correlação, testes de Laplace, séries temporais) e métricas simples, além de dados reais fornecidos por duas instituições: University of Maryland e CAIS/RNP.

Capítulo 4

Análise de Fatores que Influenciam a Segurança

Este capítulo traz os detalhes acerca do desenvolvimento de soluções para quantificar a relação entre as métricas e o objeto que está sendo medido. A pesquisa em questão envolve a investigação de fatores que influenciam a frequência de incidentes de segurança reportados em uma organização. Conforme discutido anteriormente, dois problemas ligados a esse tipo de estudo são: a falta de uma metodologia que permita a aplicação dos modelos em ambientes reais e a ausência de dados. A ideia é usar uma abordagem quantitativa combinada com dados reais para auxiliar a avaliação da segurança em uma organização. Primeiramente, será mostrado um estudo sobre a relação entre métricas de segurança obtidas usando dados do IPS e incidentes de segurança reportados pela University of Maryland. A seguir, será apresentada a análise complementar sobre outros tipos de fatores que podem influenciar a ocorrência de incidentes de segurança, usando dados do CAIS/RNP.

4.1 Relacionamento entre IPS e incidentes de segurança

Devido ao aumento do número de problemas em segurança da informação, organizações tendem a gastar mais recursos para mitigar os riscos e proteger a sua infra-estrutura. Dois

exemplos importantes são as atividades de tratamento de incidentes de segurança e os sistemas de detecção/prevenção de intrusão.

A prática conhecida como tratamento de incidentes de segurança consiste em conceder suporte ao processo de recuperação e análise de ataques de sistemas comprometidos. Um benefício secundário ligado a essa atividade é a análise das estatísticas associadas a tais ataques. Os dados podem ser usados para a correlação de eventos e determinação de tendências, melhorando a percepção acerca dos problemas de segurança da organização. Dispositivos como IDS e IPS também aparecem com frequência nas organizações e são ferramentas importantes para monitorar (ou bloquear) as atividades maliciosas de uma rede. Ao longo dessa seção, será apresentado um estudo sobre a relação entre os dados de um IPS e os incidentes de segurança.

Um IPS pode ser considerado como uma extensão de um IDS, pois além de detectar intrusos, ele também age em tempo real bloqueando possíveis ataques. Devido a essas características, tais sistemas podem ser vistos como monitores de atividades maliciosas no perímetro de rede da organização. De acordo com o CERT, um incidente de segurança representa a violação de uma política de segurança, seja ela implícita ou explícita. Usualmente, todo incidente de segurança reportado é gravado em uma base de dados. Em outras palavras, usando dados de incidentes de segurança e dados de um IPS, é possível investigar a relação entre as atividades maliciosas bloqueadas e as violações das políticas de segurança no perímetro da rede.

O processo de estudo, resposta e tratamento de incidentes é baseado em diversas origens de eventos: sensores instalados na organização (IDS), notificação de usuários e notificação de outros administradores do sistema. A partir dessas fontes, é possível obter as seguintes informações sobre um incidente de segurança (Richardson, 2008): endereço IP de origem, endereço IP de destino, tipo de ataque e informações sobre a data do ataque. Porém, outros importantes detalhes sobre o incidente, como as falhas de segurança envolvidas ou as diversas tentativas antes do ataque bem sucedido são difíceis de serem obtidos sem uma análise mais profunda. As informações presentes nos sistemas de prevenção de intrusão podem melhorar a compreensão da segurança da organização, e também desenvolver novas políticas de prevenção de ataques.

Essa suposta correlação entre as informações coletadas pelo IPS e os incidentes de se-

gurança foi sugerida, porém não avaliada em (Chrun et al., 2008a) e (Chrun et al., 2008b). Nesses trabalhos, algumas métricas de segurança baseadas em dados de um sistema de prevenção de intrusão foram definidas. A partir da análise da evolução das métricas de segurança por grupo de ataque com foco nos valores atípicos ou *outliers*, os autores desenvolvem um método para identificar e classificar potenciais computadores corrompidos.

Usando essa hipótese como ponto de início para as análises, diversas investigações podem ser realizadas. Neste trabalho, as seguintes questões serão abordadas:

1. Métricas de segurança obtidas a partir de dados do IPS são relacionadas aos incidentes de segurança?

2. Métricas relacionadas a posição do atacante perante a rede da organização influenciam os incidentes de segurança?

3. Métricas relevantes variam de acordo com o tipo de incidente?

4. Quais as implicações práticas para a segurança da organização?

Primeiramente, foram definidos dois grupos de dados relacionados ao IPS, de acordo com a perspectiva do atacante: i) computadores fora da organização direcionando ataques para dentro da organização e ii) computadores dentro da organização direcionando ataques para fora da organização.

O próximo passo foi a extração de métricas de segurança para cada um dos grupos. Baseado nos trabalhos de Chrun et al. (2008a) e (2008b) as seguintes métricas foram definidas: número de alertas, número de atacantes, número de assinaturas de ataques, número de alvos, número de alertas por alvo, número de atacantes por alvo, número de alertas por atacante e número de alvos por atacantes.

Após a definição das métricas, os incidentes de segurança foram agrupados nos seguintes grupos: Hacking, Bot e Spam. Desse ponto em diante, é possível estudar o relacionamento entre as métricas de segurança e a ocorrência de incidentes nos diferentes grupos. Para isso, foi aplicado um modelo de regressão linear híbrido conhecido como LARS/OLS (*Least Angle Regression/ Ordinary Least Square*) nos dados fornecidos pela University of Maryland. A Figura 4.1 mostra uma visão geral da análise proposta.

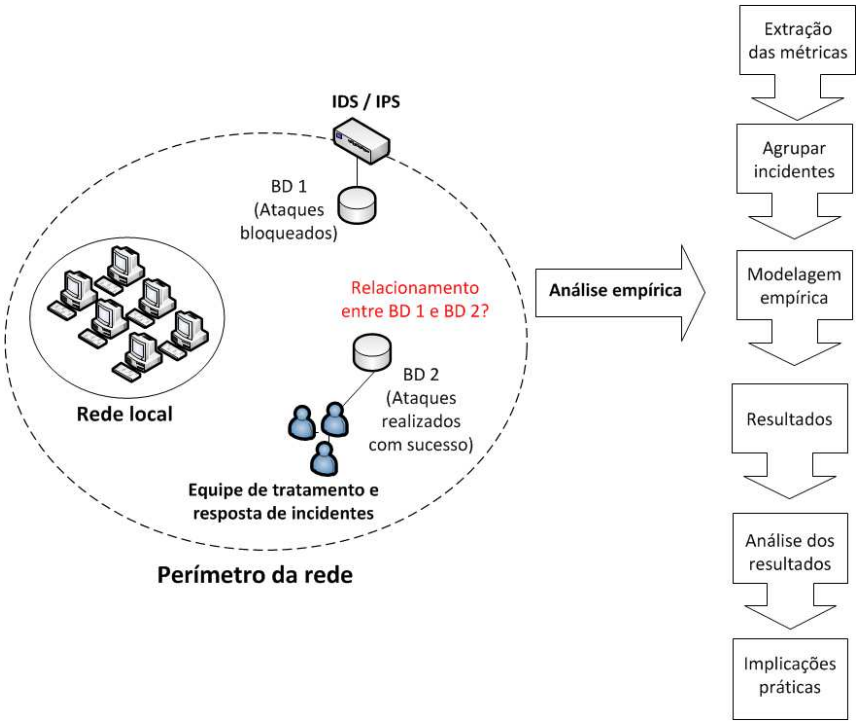


Figura 4.1: Visão geral da abordagem proposta

Os detalhes sobre as métricas, os dados utilizados, o modelo de regressão e os resultados obtidos serão apresentados nas próximas seções.

4.1.1 Dados do sistema de prevenção de intrusão e de incidentes de segurança

Conforme definido anteriormente, um IPS é um dispositivo que possui todas as funcionalidades de um IDS e também bloqueia determinados ataques. Assim como um IDS, é comum o IPS atuar no caminho de um meio físico, com o intuito de capturar, analisar e devolver o tráfego para rede. Neste modo, o IPS é frequentemente instalado na borda da rede, seguido de um *firewall*, ou mesmo um roteador com acesso a uma rede externa (Nagahama et al., 2008). Portanto, a captura e a análise se restringem ao tráfego que passa através do IPS. Consequentemente, o tráfego malicioso em um segmento interno da rede não chega a ser capturado e, consequentemente, não pode ser bloqueado.

O modo mais comum usado pelos sistemas de prevenção de intrusão para detectar/bloquear possíveis atacantes é conhecido como detecção baseada em assinaturas. Nesse

método, as decisões dependem de um conjunto de assinaturas que são regularmente atualizadas pelos fabricantes de IPS assim que novos ataques são descobertos. Quando as características de um certo ataque correspondem com as características de uma determinada assinatura, o ataque é bloqueado e um alerta é gravado nos registros do IPS. Esse tipo de método é muito similar ao utilizado nos softwares antivírus. Um exemplo de assinatura seria a tentativa de conectar em um servidor *telnet* usando o usuário "root"; se o IPS detectar esse tipo de padrão no tráfego, a possível ameaça seria bloqueada.

A detecção baseada em assinaturas é extremamente eficiente para detectar ameaças já conhecidas. A principal limitação desse método é a detecção de ameaças novas e ainda desconhecidas. Novas metodologias de detecção, como as baseadas no comportamento da rede e dos protocolos, surgiram para tentar minimizar esse problema. Porém, a maioria dos IPSs ainda usam a detecção baseada em assinatura como o método primário de detecção de intrusos. Os dispositivos instalados na University of Maryland são baseados em assinaturas. Outros detalhes sobre os sistemas de prevenção de intrusão, como as diversas opções de posicionamento na rede e descrição das metodologias de detecção/prevenção de intrusos podem ser encontradas em (Scarfone e Mell, 2007), (Nakamura e Geus, 2007) e (Patel et al., 2010).

O conteúdo dos registros de um IPS pode variar de acordo com os dispositivos, porém, alguns atributos podem ser encontrados na maioria dos sistemas: alertas, data, horário, identificação da assinatura, ação tomada (bloqueio, alerta), endereço IP de origem, endereço IP de destino, porta de origem, porta de destino, entre outros. Usando alguns desses atributos, (Chrun et al., 2008a) propõe métricas baseadas nas seguintes perspectivas: 1) computadores fora da organização direcionando ataques para dentro da organização e 2) computadores dentro da organização direcionando ataques para fora da organização. Desta forma, os alertas serão diferenciados de acordo com o tipo de ataque: quando o alvo é a organização ou quando os computadores da própria organização são os responsáveis pelo ataque.

As métricas a seguir, específicas para os ataques direcionados a organização foram propostas em (Chrun et al., 2008a). No decorrer desta tese, tal conjunto de métricas será chamado de G1.

- *Número de alertas:* ilustra o número de tentativas de ataque direcionadas a organização. É calculado a partir do endereço IP do computador que foi a origem do ataque. Se em um determinado dia, foram bloqueados x_1 tentativas de ataque originados de máquinas fora do perímetro da universidade, então o número de alertas para aquele dia é x_1;

- *Número de atacantes (distintos):* mostra a atividade dos atacantes que direcionam a organização. É calculado a partir do endereço IP do computador que foi a origem do ataque. Se em um determinado dia, foram bloqueados x_2 atacantes originados de máquinas fora do perímetro da universidade, então o número de atacantes para aquele dia é x_2;

- *Número de alvos (distintos)*: indica o número de alvos dos ataques e potenciais computadores corrompidos. É calculado a partir do endereço IP do computador que foi o alvo do ataque (destino). Se em um determinado dia, x_3 computadores dentro da organização foram alvos de ataque, então o número de alvos para aquele dia é x_3;

- *Número de assinaturas (distintas)*: revela a variedade dos ataques que direcionam a organização. Cada alerta disparado é relacionado a uma assinatura de ataque e cada assinatura possui um número de identificação único. Se em um determinado dia foi detectado que x_4 assinaturas diferentes foram usadas para os ataques originados fora da organização, então o número de assinaturas para aquele dia é x_4;

- *Número de alertas por alvo:* indica o quanto alguns computadores são atacados;

- *Número de atacantes por alvo:* revela possíveis ataques coordenados a alvos específicos.

As métricas a seguir, específicas os ataques originados dentro da organização e direcionados a computadores fora do perímetro da rede também foram propostas em (Chrun et al., 2008a). No decorrer desta tese, tal conjunto de métricas será chamado de G2.

- *Número de alertas:* indica o número de tentativas de ataques realizadas a partir de computadores dentro do perímetro da organização, direcionadas a computadores fora

do perímetro. É calculado a partir do endereço IP do computador que foi a origem do ataque. Se em um determinado dia foram bloqueados y_1 tentativas de ataque originados de máquinas dentro do perímetro da universidade, então o número de alertas para aquele dia é y_1;

- *Número de atacantes (distintos):* ilustra a atividade dos ataques originados de dentro da organização e também os potenciais computadores corrompidos. É calculado a partir do endereço IP do computador que foi a origem do ataque. Se em um determinado dia foram bloqueados y_2 ataques originados de máquinas dentro do perímetro da universidade, então o número de atacantes para aquele dia é y_2;

- *Número de alvos (distintos):* reflete o número de alvos externos ao perímetro da organização que sofreram ataques originados de dentro do perímetro. É calculado a partir do endereço IP do computador que foi o alvo do ataque (destino). Se em um determinado dia y_3 computadores fora da organização foram alvos de ataque, então o número de alvos para aquele dia é y_3;

- *Número de assinaturas (distintas):* revela a variedade dos ataques originados a partir de computadores de dentro do perímetro da organização. Cada alerta disparado é relacionado a uma assinatura de ataque e cada assinatura possui um número de identificação único. Se em um determinado dia foi detectado que y_4 assinaturas diferentes foram usadas para os ataques originados dentro da organização, então o número de assinaturas para aquele dia é y_4;

- *Número de alertas por atacante:* mostra o quanto os computadores da organização estão atacando computadores fora da organização. Um alto valor pode indicar a persistência do atacante em disparar ataques contra computadores fora da organização.

- *Número de alvos por ataque:* auxilia a caracterização da atividade maliciosa originada a partir de computadores da organização. Uma varredura de portas pode ser caracterizada por um alto número de alvos por atacante.

Após a definição das métricas de segurança baseadas em dados do IPS, os dados de incidentes devem ser caracterizados. O *Center of Internet Security* (CIS), uma organização sem fins lucrativos que desenvolve soluções para aumentar a segurança da Internet,

criou uma lista de atributos que devem ser populados, da melhora maneira possível, para cada incidente de segurança reportado. A lista inclui: identificação do incidente, data de ocorrência, data de recuperação, data de descoberta, nível de esforço, escopo do incidente, sistemas afetados, classificação do incidente, causa principal, prioridade e localização geográfica.

Alguns dos atributos listados anteriormente podem ser usados para agrupar os incidentes. A classificação de um incidente é utilizada com frequência para fornecer contexto ao registros coletados. Ela pode incluir diversas categorias, como: ataques de Negação de Serviço, Códigos Maliciosos, Acessos Não-autorizados e Uso Inapropriado. Relatórios sobre incidentes de segurança, como os publicados pela Verizon (2012), Symantec (2012) e *Computer Security Institute* (CSI) (2011) usam diferentes classificações para melhorar a compreensão acerca dos ataques.

Conforme discutido no capítulo 2, a análise de incidentes pode revelar importantes comportamentos em uma organização. Uma métrica importante nesse quesito é o número de incidentes de segurança encontrados em um determinado período de tempo (The Center for Internet Security, 2010). De posse das métricas extraídas dos dados de um IPS e do número de incidentes de segurança encontrados em um determinado período de tempo, é possível estabelecer relações quantitativas entre os conjuntos de dados: um aumento no número de ataques bloqueados pelo IPS indica um aumento no número de incidentes de segurança reportados. A próxima seção exibe os detalhes sobre a metodologia utilizada para investigar essa relação.

4.1.2 Metodologia

A primeira parte da metodologia proposta consiste em tratar os dados que serão analisados. A segunda parte trata da análise de regressão.

Tratamento dos dados

O conjunto de dados fornecido pela University of Maryland consiste de 1794 incidentes de segurança e 7.665.085 alertas do IPS, durante um período de quatro anos (entre 1º de Janeiro de 2007 até 31 de Dezembro de 2010). Com base em discussões com o *Division*

of Information Technology (DIT) da University of Maryland, que é o departamento que cuida de toda a infraestrutura de TIC do campus, os dados de incidentes (e também dos alertas do IPS) foram agrupados em semanas ($t = 209$ semanas), com a segunda-feira como o primeiro dia da semana. Coincidentemente, o dia 1º de Janeiro de 2007 foi uma segunda-feira.

O agrupamento dos incidentes em uma certa janela de tempo é uma técnica utilizada para minimizar os efeitos do atraso entre a ocorrência de um evento e o cadastro dele como um incidente. Nos incidentes em que a detecção não é feita de maneira automatizada, é normal que exista um tempo entre a notificação, análise e o cadastro do incidente na base de dados. Como na base de dados disponibilizada não existem registros sobre quando o incidente foi descoberto, mas sim quando ele foi reportado, essa aproximação, sugerida pelo DIT, foi adotada. Assim, ambos os grupos de dados (métricas obtidas usando dados do IPS e os incidentes de segurança) serão analisados semanalmente.

O conjunto de dados de incidentes inclui sete categorias criadas pelo DIT: Abuso (conflitos de endereço IP, uso de proxy aberto para burlar as políticas de segurança), Bot, Hacking (varredura de porta, ataques de negação de serviço, invasões), Spam, Vírus, Spyware e Worm. Cada categoria contém diversos tipos de incidentes, em um total de 52 tipos. A classificação e cada um dos tipos de incidentes pode ser vista no Apêndice B.

Os incidentes reportados e gravados na base de dados da University of Maryland foram baseados em três fontes de eventos: 1) um IDS usando uma combinação de regras regulares e regras definidas pelos administradores de segurança, 2) notificações de usuários e 3) notificações de outros administradores do sistema. Como a ocorrência do incidente implica no bloqueio do endereço IP do computador suspeito, a DIT da universidade verifica a autenticidade de cada incidente. Isso significa que todos os incidentes obtidos a partir dessas três fontes são revisados manualmente. A DIT usa ferramentas como varredura de portas e analisadores de pacotes para validar o comportamento suspeito dos computadores.

Cada fonte de evento possui características próprias sobre a confirmação do incidente. Em geral, 60% dos alertas gerados pelo IDS são inconclusivos. Entre os 40% restantes, aproximadamente a metade é bloqueada diretamente pelo DIT e a outra metade exige uma confirmação. Entre as notificações, poucas são feitas por usuários. Já as notificações realizadas por outros administradores de sistemas são definidas e reportadas como

incidentes em cerca de 75% dos casos, baseado na relação de confiança que a DIT possui com cada administrador. Devido a questões de sigilo, esse tipo de dado não foi revelado, e portanto, o evento que originou o incidente não é conhecido.

Foram examinados os três tipos de incidentes que ocorreram com a maior frequência no conjunto de dados: Bot, Hacking e Spam. A Figura 4.2 apresenta a distribuição dos incidentes reportados entre os anos de 2007 e 2010. A soma desses três incidentes representa 92,5% do conjunto de dados analisado. Já a Tabela 4.1 mostra outras informações sobre os incidentes investigados. A "Data inicial" indica o data em que o primeiro incidente de tal categoria foi reportado. Já a "Data final" representa a data em que o último incidente foi reportado. "# de dias" mostra o número de dias em que ao menos um incidente de determinada categoria foi reportado durante a "Data inicial" e "Data final".

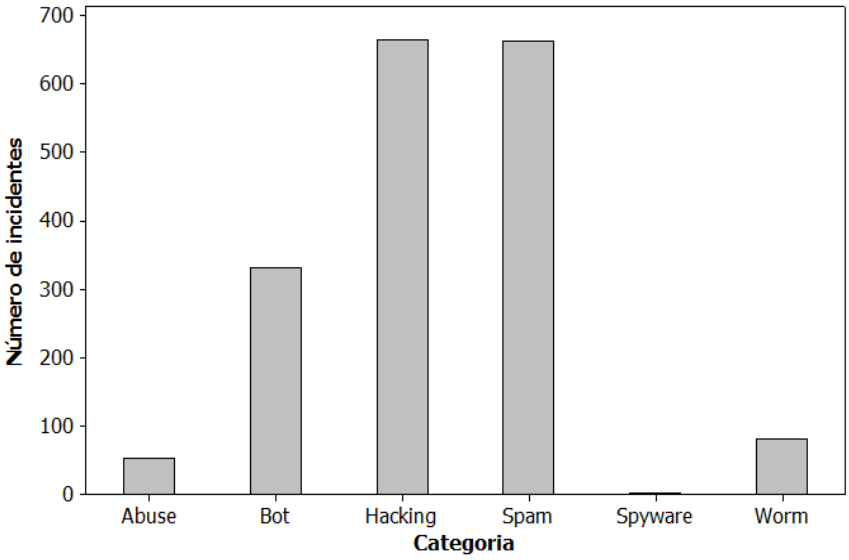


Figura 4.2: Distribuição dos incidentes reportados entre os anos de 2007 e 2010.

A Tabela 4.2 apresenta as tentativas de ataque bloqueadas pelo IPS. "# de atacantes", "# de alvos" and "# de assinaturas" representam, respectivamente, o número cumulativo de atacantes, alvos e assinaturas. Todos os alertas tiveram início em 01/01/2007 e terminaram em 31/12/2010. O dispositivo IPS investigado foi comprado pela University of Maryland e instalado em 01/09/2006. Ele localiza-se na borda da rede, bloqueando ataques externos à organização e também ataques originados dentro do perímetro da rede, mas destinados

Tabela 4.1: Incidentes de segurança investigados

Categoria	Data inicial	Data final	# de incidentes	# de dias
Todos	02/01/2007	31/12/2010	1776	581
Hacking	02/01/2007	31/12/2010	665	308
Spam	04/01/2007	31/12/2010	663	233
Bot	02/01/2007	14/12/2010	332	144

Tabela 4.2: Alertas do sistema de prevenção de intrusão

Grupo	# de alertas	# de atacantes	# de alvos	# de assinaturas
Todos	7.665.085	1.837.321	368.100	24.354
G1	7.293.795	1.815.492	304.068	18.265
G2	371.290	21.829	64.032	6089

a computadores fora da organização.

A diferença entre o número de alertas do grupo G1 e do grupo G2 chama a atenção. São aproximadamente 20 vezes mais alertas originados de ataques externos com destino a computadores dentro da organização. Levando em consideração todos os alertas, mais de 95% são relacionados ao grupo G1. Em termos de segurança, duas possíveis justificativas podem ser usadas para compreender esse resultado: 1) dispositivo IPS investigado possui uma capacidade maior de detectar ataques externos à organização e 2) ataques externos à organização são mais frequentes do que os ataques originados dentro do perímetro e com alvos fora da organização. Nas próximas seções será investigada a relação entre as métricas de cada um dos grupos e o número de incidentes de segurança.

O número total de incidentes de segurança será denotado por I_t, o número de incidentes do tipo Bot será denotado por IB_t, o número de incidentes do tipo Hacking será denotado por IH_t e o número de incidentes do tipo Spam por IS_t onde t é o número de semanas e $t = 1, \ldots, 209$. As métricas de IPS serão denotadas por: número de alertas = Al_t, número de atacantes = At_t, número de alvos = T_t, número de assinaturas = S_t, número de alertas por alvo = AlT_t, número de atacantes por alvo = AtT_t, número de alertas por atacante = $AlAt_t$ e número de alvos por atacante = TAt_t. A Tabela 4.3 apresenta a descrição

Tabela 4.3: Estatística descritiva das variáveis (209 observações)

Métrica	Média	Desvio padrão	Mínimo	Q1	Mediana	Q3	Máximo
I_t - # total de incidentes	8,617	10,538	0	2	5	10	64
IB_t - # de incidentes Bot	1,589	3,409	0	0	0	2	26
IH_t - # de incidentes Hacking	3,182	6,093	0	0	2	4	64
IS_t - # de incidentes Spam	3,167	8,386	0	0	1	2	84
Al_t - # de alertas (G1)	34.899	86.230	187	7.766	14.585	24.917	910.940
A_t - # de atacantes (G1)	8.687	59.487	31	757	1.355	2.220	822.698
T_t - # de alvos (G1)	1454,9	676,5	78	1.013	1.210	1.728,5	3.662
S_t - # de assinaturas (G1)	87,39	128,98	15	62	72	82	1.347
AlT_t - # de alertas por alvo (G1)	24,55	54,70	2,40	5,26	11,64	18,57	447,83
AtT_t - # de atacantes por alvo (G1)	5,01	28,05	0,34	0,65	0,97	1,34	361,31
Al_t - # de alertas (G2)	1.777	2.267	98	446	944	2.180	14.755
A_t - # de atacantes (G2)	104,44	78,91	11	55,50	84	133,50	504
T_t - # de alvos (G2)	306,4	310,7	15	68,5	152	523,5	1.585
S_t - # de assinaturas (G2)	29,13	33,38	7	19,50	24	29	426
$AlAt_t$ - # de alertas por atacante (G2)	21,13	42,71	2,43	5,92	11,52	19,74	534,77
TAt_t - # de alvos por atacante (G2)	3,139	3,127	0,326	1,087	1,952	3,985	25,423

estatística do conjunto de dados analisado.

Até o presente momento, foram exibidas as métricas de segurança que serão investigadas, os grupos de incidentes, a forma com que os dados serão analisados e também algumas informações sobre o ambiente em que se encontra os dados. A seguir, será detalhado o método usado para investigar a relação entre as métricas de IPS e os incidentes de segurança.

Análise de regressão

Um método usado extensamente pela comunidade científica para investigar a relação entre duas ao mais variáveis é conhecido como análise de regressão. O principal objetivo desse tipo de análise é obter informações sobre uma das variáveis, por meio dos valores conhecidos da(s) outra(s) variáveis. A variável cujo valor é fixado pelo pesquisador é usualmente representada por x e conhecida como variável independente, previsão ou explicativa. A outra variável é conhecida como dependente ou resposta e frequentemente denotada por y.

O modelo de regressão linear, em especial, pressupõe que o valor esperado de uma determinada variável dependente y é uma função linear da variável independente x. Já um modelo de regressão linear múltiplo relaciona uma variável dependente y a mais de uma variável independente. Por exemplo, ao tentar prever os ataques em um computador (variável dependente), é possível ter o seguinte conjunto de variáveis independentes: $x_1 =$ número de vulnerabilidades de segurança encontradas no computador, $x_2 =$ presença de antivírus atualizado e $x_3 =$ número de dias desde a última verificação se há atualização para o sistema operacional.

A notação geral de um modelo de regressão é escrita da seguinte forma:

$$Y = \beta_0 + \sum_{k=1}^{j} \beta_k X_k + \epsilon_t \tag{4.1}$$

onde β_0 é o termo constante, β_1 a β_j são os coeficientes das $j-$ésimas variáveis independentes, j é o número total de variáveis independentes, ϵ_t é chamada de desvio aleatório ou erro aleatório e X_k representa o conjunto de variáveis independentes. Os coeficientes β_j representam a mudança média na variável dependente Y, associada com um aumento de 1 unidade na variável independente X.

Neste trabalho, será usado um modelo de regressão linear múltipla para investigar o relacionamento entre as métricas de IPS (variáveis independentes) e o número de incidentes de segurança (variáveis dependentes). Nosso conjunto de variáveis dependentes é composto por: I_t, IB_t, IH_t e IS_t. O conjunto de variáveis independentes X_k é formado por: Al_t (G1 e G2), At_t (G1 e G2), T_t (G1 e G2), S_t (G1 e G2), AlT_t, AtT_t, $AlAt_t$ e TAt_t. A regressão linear múltipla foi escolhida por ser simples, eficiente e amplamente utilizada na literatura

para a realização de análises empíricas. Porém, outros modelos também poderiam ser usados, como: regressão logística, modelos auto regressivos, regressão dinâmica e regressão robusta.

Uma abordagem utilizada com frequência para auxiliar essa investigação é conhecida como seleção de variáveis. De modo geral, esse método consiste em verificar a significância estatística de cada uma das variáveis envolvidas no modelo com o auxílio da análise do valor p, também conhecido como *nível de significância observado*. O valor p é calculado para cada um dos coeficientes β_j, com o objetivo de verificar a hipótese nula H_0 de que o coeficiente em questão seja igual a zero. Um coeficiente igual a zero, significa que a variável associada a ele não possui nenhum efeito no modelo de regressão. O valor p é calculado a partir da razão entre o coeficiente e o desvio padrão estimado do coeficiente. Outras informações sobre o cálculo do valor p para seleção de variáveis em modelos de regressão linear pode ser obtido em: (Devore, 2012), (Montgomery et al., 2012) e (Mendenhall e Sincich, 1989). Valores p pequenos sugerem que a respectiva variável é um valor significativo para o modelo. Ao longo deste trabalho será adotado um nível de confiança de 95%. Em outras palavras, uma métrica (variável) será considerada significativa ou relevante se o seu coeficiente de regressão β_j possuir um valor $p < 0,05$.

Não existe uma teoria que caracterize a relação entre as métricas obtidas dos dados de IPS (variáveis independentes) e o número de incidentes de segurança (variáveis dependentes). Uma hipótese sobre a relação entre essas variáveis foi formulada devido a uma possível ligação entre os ataques bem sucedidos e os ataques bloqueados. Consequentemente, todas as doze métricas selecionadas para a investigação precisam ser devidamente testadas. Em tais casos, o uso de somente um modelo com todas as variáveis disponíveis pode não ser suficiente para obter o melhor conjunto de variáveis e ainda pode ser custoso para o pesquisador (Wright e London, 2009). Com o intuito de auxiliar o processo de seleção das variáveis independentes em um modelo de regressão, foram desenvolvidos diversos métodos, como: regressão por análise dos melhores subconjuntos (*best regression subsets*), regressão passo a passo (*stepwise regression*), regressão por componentes principais (*principal component regression*) e regressão de ângulo mínimo (LARS).

Cada método possui características próprias e limitações, como restrições a determinados tipos de conjuntos de dados e alta complexidade computacional. Diversos trabalhos

investigam a eficiência dos diversos métodos de seleção de variáveis em regressão linear múltipla (Thompson, 1978), (Halinski e Feldt, 1970) e (Budescu, 1993). Como o objetivo deste trabalho é identificar quais métricas estão relacionadas aos incidentes de segurança, o seguinte método, dividido em duas partes, foi adotado 1) refinar o conjunto inicial, selecionando um subconjunto de métricas e 2) aplicar a regressão linear nas variáveis obtidas no passo 1). Com relação a segurança, esse modelo traria vantagens, pois facilitaria o desenvolvimento de critérios para a análise da métrica. Esse tipo de situação ficará mais evidente nas análises à seguir.

Um modelo que atende o processo descrito é conhecido como modelo híbrido LARS/OLS (Tibshirani et al., 2004a). Neste método, o algoritmo LARS é usado para encontrar um subconjunto de variáveis independentes e, então, a partir desse subconjunto, um modelo de regressão linear é usado para estimar os coeficientes. Alguns exemplos do uso dessa técnica podem ser encontrados em (Hecker et al., 2009) e (Liu, 2012).

O LARS (Tibshirani et al., 2004a), é um algoritmo para seleção de variáveis baseado nos métodos tradicionais de seleção progressiva (*SFR - stepwise forward regression*) (Devore, 2012). O processo de seleção de variáveis independentes do algoritmo LARS funciona de maneira semelhante ao método SFR usando a correlação absoluta entre a variável independente e a variável dependente. A correlação absoluta é definida como a correlação entre a variável independente e os resíduos (diferença entre o valor observado e o valor estimado pelo modelo de regressão linear). O primeiro passo consiste em encontrar a variável independente x_{j1} que melhor descreva a variável dependente, pelo cálculo de modelos de regressão linear com somente uma variável independente. No próximo passo, são testados os modelos que contêm a variável independente x_{j1} até encontrar a primeira variável independente x_{j2} com valor de correlação absoluto maior que uma certa razão t. Ao invés de continuar a busca a partir dos outros modelos que contém a variável independente x_{j1}, como é feito pelo SFR e que demanda um esforço computacional maior, o LARS propõe uma otimização nessa busca, com base nas variáveis independentes já selecionadas. Outros detalhes sobre o método de seleção de variáveis empregado pelo LARS podem ser encontrados em: (Tibshirani et al., 2004a), (Tibshirani et al., 2004b), (McCann e Welsch, 2007) e (Khan et al., 2007).

Assim como todos os métodos automáticos usados para a seleção de variáveis, as variá-

veis selecionadas podem não representar as reais variáveis significativas do modelo (Wright e London, 2009). O pesquisador deve ser capaz de diferenciar os modelos gerados e também adicionar ou excluir possíveis variáveis de controle quando necessário.

Para contornar essa situação, foi definida a seguinte estratégia com relação a seleção de variáveis: nos casos em que o LARS não selecionou nenhuma variável ou quando as variáveis selecionadas são muito diferentes das variáveis significativas encontradas no modelo de regressão linear padrão (com todas as variáveis), será usado o modelo de regressão linear padrão, ao invés do LARS.

Também é importante ressaltar que o resultado obtido com os modelos de regressão não necessariamente implica em uma relação de causa e efeito entre as variáveis. Mesmo que exista uma evidência empírica forte entre duas variáveis, somente isso não pode ser usado para estabelecer uma relação de causalidade. Para isso, é preciso criar uma fundamentação do estudo fora do escopo da análise dos dados. O uso de modelos estatísticos para a investigação da relação entre variáveis pode confirmar um certo relacionamento entre elas, mas não pode ser a única base para tal afirmação.

Assim, com base nas perguntas definidas no início da seção 4.1, primeiramente, será investigado se existe alguma evidência empírica que métricas IPS são relacionadas aos incidentes de segurança. Para isso, foram propostos quatro diferentes modelos de regressão. Cada modelo contém um determinado subconjunto das doze métricas definidas anteriormente:

1. Modelo I formado pelas métricas do grupo G1: Al_t, At_t, T_t, S_t, AlT_t e AtT_t;
2. Modelo II formado pelas métricas do grupo G2: Al_t, At_t, T_t, S_t, $AlAt_t$ e TAt_t;
3. Modelo III proposto em (Chrun et al., 2008a) e formado pelas métricas: T_t (G1), A_t (G2), AlT_t, AtT_t, $AlAt_t$ e TAt_t;
4. Modelo IV formado pelas métricas T_t (G1), T_t (G2), AlT_t e $AlAt_t$, referentes ao resultado da aplicação do LARS nas doze métricas;

Usar modelos alternativos de regressão com diferentes configurações de métricas aumenta a confiança sobre os resultados obtidos. Quanto maior o número de métricas relevantes presentes nos modelos propostos, maior a convicção sobre a existência de um

relacionamento entre os dados de IPS e os incidentes de segurança. A ausência de métricas relevantes nos modelos investigados enfraquece a suposição sobre a existência de um relacionamento entre tais conjuntos. A abordagem proposta neste trabalho foi inspirada no trabalho realizado por (Wang e Xiao, 2010), em que são usados seis modelos diferentes de regressão para investigar se a busca por informações sobre segurança é relacionada aos ataques às redes de computadores e a divulgação de vulnerabilidades de segurança.

A análise proposta em (Chrun et al., 2008a) não trata da relação explícita das métricas de IPS com os incidentes de segurança, mas sim do uso de observações atípicas (*outliers*) para identificar certos problemas de segurança nos computadores de uma rede, como *worms* e varreduras de portas. Isso mostra que algumas métricas presentes no conjunto podem não ser relevantes para o estudo proposto. Um exemplo é o número de alertas (T_t), pois um atacante pode lançar um ataque contra um alvo diversas vezes e em diferentes janelas de tempo. De acordo com os autores, essa persistência poderia ser representada pela métrica número de alertas por alvo (AlT_t). Similarmente, o número de atacantes (A_t (G1)) e o número de alvos (T_t (G2)) foram excluídos da análise de acordo com essa ideia, já que a persistência poderia ser representada pelas métricas número de atacantes por alvo (AtT_t) e número de alvos por atacante (TAt_t), respectivamente.

4.1.3 Resultados

A Tabela 4.4 apresenta os modelos de regressão e cada um dos resultados. Nenhuma métrica foi considerada significativa no modelo I. Considerando somente o modelo II, a métrica T_t (G2) foi considerada relevante. No modelo III, das seis métricas incluídas na regressão, três delas (A_t (G2), TAt_t e AlT_t) impactaram significativamente o número de incidentes de segurança. Já no modelo IV, entre as quatro métricas presentes na regressão, a métrica T_t (G2), assim como no modelo II, foi a única variável significativa.

Em cada um dos modelos investigados, ao menos uma métrica foi considerada relevante, com exceção do modelo I. Essa evidência empírica sugere que o conjunto de métricas investigado possui uma relação com o número de incidentes de segurança reportados, confirmando a resposta positiva para a pergunta 1:

1. Métricas se segurança obtidas a partir de dados do IPS são relacionadas aos inciden-

Tabela 4.4: Resultados dos modelos de regressão - coeficiente e valor p

Variáveis (Métricas)	Modelo I	Modelo II	Modelo III	Modelo IV
Al_t (G1)	-0,0002 (0,0001)	-	-	-
Al_t (G2)	-	-0,0003 (0,0006)	-	-
At_t (G1)	0,0003 (0,0002)	-	-	-
At_t (G2)	-	-0,0038 (0,0154)	0,0345 ** (0,009)	-
T_t (G1)	0,0025 (0,0014)	-	0,001314 (0,001)	0,00144 (0,001)
T_t (G2)	-	0,01517 * (0,0059)	-	0,0135 ** (0,0022)
S_t (G1)	-0,0053 (0,0057)	-	-	-
S_t (G2)	-	-0,0071 (0,0214)	-	-
AlT_t (G1)	0,2636 (0,1824)	-	-0,029 (0,01632)	-0,0123 (0,0125)
AtT_t (G1)	-0,3031 (0,2326)	-	0,024 (0,032)	-
TAt_t (G2)	-	0,0047 (0,5398)	1,1038 ** (0,2723)	-
$AlAt_t$ (G2)	-	-0,01645 (0,0348)	-0,0459 * (0,02)	0,0213 (0,0162)

* $p < 0,05$ ** $p < 0,01$ ( ): erro padrão do coeficiente

tes de segurança?

Também foi possível notar algumas diferenças entre as seleções de variáveis em cada um dos modelos de regressão. A métrica T_t (G2) foi excluída do modelo III, mas foi considerada significativa nos modelos II e IV. Assim como no modelo IV, em que as métricas A_t (G2) e TAt_t foram excluídas da seleção pelo algoritmo LARS, mas no modelo III apareceram como significativas. Isso mostra a importância da análise acerca dos modelos gerados. Dessa forma, o pesquisador deve ser capaz de inserir ou excluir determinadas variáveis do modelo quando necessário.

Em termos práticos, se o conhecimento da relação entre um determinado conjunto de variáveis independentes (métricas de IPS) e a variável dependente (incidentes de segurança) é restrito e sustentado por hipóteses que necessitam de validação, é recomendável que todas as métricas presentes no conjunto sejam avaliadas, seja com o auxílio de algoritmos de seleção ou incluindo o conjunto inteiro de variáveis independentes no modelo de regressão. Este é o caso descrito nesta tese.

O resultado positivo para a pergunta 1 pode ser usado como ponto de partida para a investigação das perguntas 2 e 3 definidas anteriormente:

2. Métricas relacionadas a posição do atacante perante a rede da organização influenciam os incidentes de segurança?

Tabela 4.5: Resultados dos modelos de regressão de acordo com o tipo de incidente - coeficiente e valor p

Variáveis (Métricas)	Bots	Hacking	Spam
Al_t (G1)	-0,000002 (0,0000023)	-	-
Al_t (G2)	-	-	-
At_t (G1)	-	-	-
At_t (G2)	-	0,0333 ** (0,005974)	-0,024 (0,012)
T_t (G1)	0,0023 ** (0,0003)	-	-0,00124 (0,00084)
T_t (G2)	-0,001 (0,00087)	0,00139 (0,00151)	0,0107 ** (0,0039)
S_t (G1)	-0,00087 (0,00157)	-	-
S_t (G2)	-	-	-
AlT_t (G1)	-	-0,0141 * (0,007)	-
AtT_t (G1)	-	-	-
TAt_t (G2)	0,427 ** (0,1053)	-	-0,1597 (0,317)
$AlAt_t$ (G2)	-0,018 ** (0,0061)	-	-

* $p < 0,05$ ** $p < 0,01$ ( ): erro padrão do coeficiente

3. Métricas relevantes variam de acordo com o tipo de incidente?

Os resultados dos modelos apresentados na Tabela 4.4 podem diferir de acordo com a classificação do incidente. Na maioria dos casos, a análise de acordo com o tipo de incidente é mais útil do que a análise do conjunto dos incidentes acumulados, pois cada incidente possui características próprias que devem ser levadas em consideração em seu processo de tratamento e prevenção. Se a equipe de tratamento e resposta de incidentes da organização detecta um aumento no número de incidentes em comparação com o mês passado, poucas decisões podem ser tomadas a partir dessa informação. Se o aumento foi no número de Spam e Vírus, as atitudes podem ser direcionadas de maneira mais eficiente.

A Tabela 4.5 mostra os resultados dos modelos de regressão para cada tipo de incidente investigado. Agora, a variável dependente é dada pelo número de incidentes Bot (IB_t), número de incidentes Hacking (IH_t) e número de incidentes Spam (IS_t). Em cada um dos modelos, foi aplicado primeiramente o algoritmo LARS em todas as doze métricas para selecionar as variáveis que entrarão no modelo de regressão.

Os resultados presentes na Tabela 4.5 indicam que as categorias de incidentes de segurança possuem diferentes métricas de segurança relevantes, confirmando a resposta positiva para a pergunta 3. De fato, as métricas relevantes para os incidentes Bot (T_t (G1), TAt_t (G2) e $AlAt_t$ (G2)) são diferentes das métricas relevantes para os incidentes Hacking (At_t

(G2) e AlT_t (G1)) e também diferentes das métricas relevantes para os incidentes Spam (T_t (G2)). Além das diferenças, certas similaridades entre os incidentes puderam ser notadas. Nenhuma das seguintes métricas foram sequer selecionadas pelo LARS nos três tipos de incidentes investigados: Al_t (G2), At_t (G1), S_t (G2) e AtT_t (G1). Ao analisar a Tabela 4.4, é possível notar que essas quatro métricas também não foram selecionadas pelo LARS no modelo IV onde todos os incidentes foram analisados. Além disso, nos casos em que tais métricas foram inseridas nos modelos, nenhuma delas foi considerada relevante. Assim, foi encontrada uma forte evidência empírica de que tais métricas não estão relacionadas aos incidentes reportados, indicando um primeiro critério utilizado para a seleção de métricas de segurança: quais não devem ser usadas.

A análise de cada uma dessas métricas ao longo dos quatro anos de estudo mostra que:

- O número de atacantes externos, assim como a relação entre esses atacantes e seus respectivos alvos não influencia a ocorrência de incidentes de segurança na instituição investigada;

- Os alertas gerados pelos atacantes dentro da organização, assim como a diversidade desses ataques, também não influencia a ocorrência de incidentes de segurança na instituição investigada;

Dentre as seis métricas relevantes encontradas na Tabela 4.5, quatro delas são do grupo G2 e somente duas são do grupo G1. Resultado similar foi encontrado nos modelos de regressão presentes na Tabela 4.4, em que as quatro métricas relevantes são do grupo G2, mostrando que foram encontradas evidências empíricas de que as métricas referentes as tentativas de ataque de dentro para fora da organização estão mais relacionadas aos incidentes do que as métricas referentes as tentativas de ataque de fora para dentro da organização, confirmando a resposta positiva para a pergunta 2.

Esse resultado representa o oposto da análise descritiva feita nos dados IPS, em que mais de 92,5% dos dados são do grupo G1. Isso mostra que o tamanho do conjunto de dados pode não ser diretamente proporcional ao volume de informação útil disponível. É possível que o próprio perfil da universidade seja um dos fatores responsáveis por esse comportamento. Em ambientes acadêmicos, geralmente os nós da rede não são completamente controlados pelo departamento de TIC (como em uma organização privada), o

que garante uma certa liberdade para os usuários da rede. Essa liberdade, pode ocasionar diversos problemas de segurança originados pelos computadores de dentro da organização. Da mesma forma, as universidades podem ser consideradas alvos valiosos para os atacantes devido a quantidade e diversidade de alvos disponíveis. Assim, o alto número de ataques externos direcionados à organização e a criação de diversas regras para bloqueá-los, somado às políticas de uso mais relaxadas dentro do ambiente acadêmico poderia explicar parte desse comportamento.

É importante mencionar que a descoberta de novos incidentes pode, eventualmente, alterar vários dos comportamentos encontrados. Por esse motivo, a relevância das métricas deve ser investigada periodicamente, a fim de minimizar os impactos de problemas em futuras análises.

4.1.4 Discussões e implicações práticas

Os resultados apresentados evidenciam que: as métricas de segurança obtidas a partir de dados do IPS são relacionadas aos incidentes de segurança, métricas relacionadas a posição do atacante perante a rede da organização são associadas aos incidentes de segurança e também que as métricas significativas variam de acordo com o tipo de incidente. Três importantes implicações práticas desses resultados são: a identificação de possíveis indicadores de incidentes, o desenvolvimento de métodos para melhorar a prevenção de incidentes e a análise da eficiência do IPS com relação aos diversos tipos de incidentes.

Assim como em outras áreas da ciência, indicadores de segurança representam informações que sinalizam o comportamento de determinados processos de segurança. As variáveis relevantes em um modelo de regressão possuem um comportamento similar a esse. O valor do coeficiente para a métrica número de alvos por atacante (TAt_t) é de 0,427. Isso mostra que TAt_t está associado a um aumento de $0,427$ incidentes por semana e, de acordo com a Tabela 4.5, as seguintes métricas são possíveis candidatas a indicadores de incidentes: número de alvos (T_t (G1)), número de alvos por atacante (TAt_t) e número de alertas por alvo ($AlAt_t$) para incidentes Bot, número de atacantes (At_t (G2)) e número de alertas por alvo (AlT_t) para incidentes Hacking e número de alvos (T_t (G2)) para incidentes Spam.

De posse dos resultados obtidos com os modelos de regressão, é possível filtrar, entre

um grande conjunto de métricas, quais delas são estatisticamente relevantes para a investigação. O comportamento dos incidentes e consequentemente das métricas também pode mudar, devido a natureza da segurança da informação. Como saber, então, se tais métricas identificadas como relevantes podem ser usadas como indicadores de incidentes?

Parte dessa resposta reside em estudar cada uma dessas métricas em diferentes períodos de tempo. Um possível critério de avaliação seria a ocorrência dessa métrica relevante nesses diferentes períodos de tempo. Se uma determinada métrica foi considerada relevante, mas nos outros períodos estudados esse mesmo comportamento não foi encontrado, o resultado da regressão pode ter revelado somente uma relação entre as sequências de dados, e que a causalidade entre elas não existe. A junção dessas duas análises (resultado do modelo de regressão e estudo da relevância de acordo com períodos de tempo) aumentaria a confiança sobre a eficiência da métrica e a possibilidade dela ser usada como um indicador.

Para investigar mais profundamente essa questão, nove janelas de tempo foram escolhidas para investigar o comportamento das métricas relevantes ao longo do tempo: 2007, 2008, 2009, 2010, 2007/2008, 2008/2009, 2009/2010, 2007 /2008/2009 e 2008/2009/2010. Um modelo híbrido OLS/LARS foi criado para cada período de tempo. Considerando os três tipos de incidentes possíveis e as dez janelas definidas, um total de 27 modelos de regressão foram criados. O objetivo dessa análise consiste em encontrar métricas relevantes com a maior ocorrência ao longo dos períodos e métricas não relevantes em diferentes períodos de tempo. A Tabela 4.6 mostra os resultados obtidos. As métricas com (*) representam as variáveis identificadas como relevantes de acordo com a Tabela 4.5.

Os resultados apresentados na Tabela 4.6, demonstram que dentre as seis métricas relevantes identificadas anteriormente (Tabela 4.5) somente uma delas, o número de alertas por atacante (AlA_t) não foi considerada relevante nos nove períodos investigados. Nos outros casos, as métricas aparecem como relevantes em no mínimo 2 dos 9 períodos. Em especial, a frequência das métricas T_t (G2), T_t (G1), At_t (G2), AlT_t (G1) e TAt_t (G2) é maior quando comparada com as outras métricas do mesmo grupo de incidentes. Esse resultado aumenta a confiança de que essas cinco métricas podem ser usadas como indicadores de incidentes.

Esse tipo de análise também revelou resultados interessantes como: Bot é o grupo

Tabela 4.6: Métricas relevantes ao longo do tempo

Métricas	Frequência (Total)	Frequência (Bot)	Frequência (Hacking)	Frequência (Spam)
T_t (G2)	8	3	1	4 (*)
T_t (G1)	6	3 (*)	2	1
At_t (G2)	5	0	3 (*)	2
Al_t (G1)	5	2	2	1
AlT_t (G1)	4	2	2 (*)	0
TAt_t (G2)	3	3 (*)	0	0
At_t (G1)	3	1	1	1
AtT_t (G1)	1	1	0	0
S_t (G1)	1	1	0	0
S_t (G2)	1	1	0	0
$AlAt_t$ (G2)	0	0 (*)	0	0
Al_t (G2)	0	0	0	0

que possui o maior número de métricas relevantes, 9 de um total de 12 métricas foram consideradas relevantes ao menos uma vez e as únicas métricas estatisticamente irrelevantes entre os nove períodos estudados foram o número de alertas (Al_t (G2)) e o número de alertas por atacante (AlA_t). Além disso, o número de alvos (T_t (G2)), seguido pelo número de alvos (T_t (G1)) são as métricas com a maior frequência nos períodos investigados. Isso mostra que os alvos dos ataques, tanto quanto os computadores dentro da organização como os computadores fora da organização, aparecem como uma importante métrica para avaliar os incidentes de segurança.

O estudo das métricas ao longo do tempo pode ser usado para identificar o modo com que as métricas relevantes se relacionam com os incidentes. Ao analisar a Figura 4.3, é possível notar que entre 2007 e 2009 ao menos uma métrica foi considerada significativa para os incidentes Bot. Entretanto, nenhuma métrica foi dada como relevante nos seguintes períodos: 2010, 2009/2010 e 2008/2009/2010, o que sugere uma situação atípica associada ao ano de 2010. A Figura 4.4 apresenta a distribuição dos tipos de incidente Bot por ano.

Na Figura 4.4, é possível notar que não houve nenhum incidente do tipo *irc bot* em 2010, da mesma forma que não houve nenhum incidente do tipo *bot controller* em 2008 e 2009. Além disso, a ocorrência de incidentes do tipo *virus generic bot* diminuiu drasticamente a partir de 2008 e os incidentes do tipo *bot controller* se concentram, em sua grande maioria, em um único dia. Esse novo comportamento (diminuição de *virus generic bot*, ausência de *irc bot* e um pico de incidentes do tipo *bot controller*) pode ter modificado o impacto das

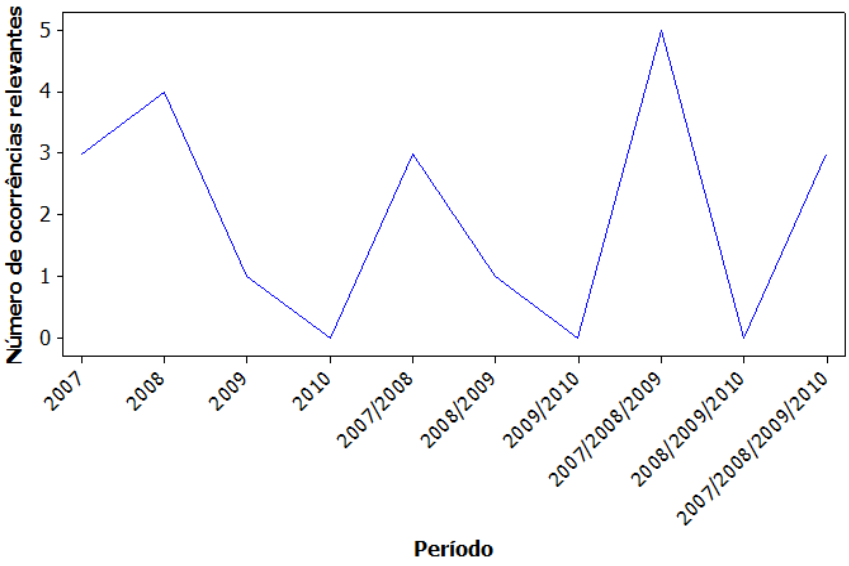


Figura 4.3: Evolução de métricas relevantes - Bot

métricas nesse tipo de incidente. Nesse caso, outras métricas poderiam ser testadas a fim de encontrar um novo conjunto que seja relevante para essa distribuição de incidentes.

Conforme apresentado no capítulo 2, um indicador de segurança representa uma métrica correlacionada a uma determinada propriedade de segurança. Com base nas análises desenvolvidas é possível criar critérios para a seleção de indicadores de incidentes a partir do estudo das métricas relevantes ao longo do tempo. O critério apresentado possui como característica comparar o conjunto de métricas relevantes encontrado na análise de regressão inicial com as métricas relevantes encontradas na análise de regressão em cada um dos períodos definidos. Conforme discutido anteriormente, a união de tais análises aumenta a confiança sobre a eficiência da métrica e a possibilidade dela ser usada como um indicador.

Seja s_t o conjunto de dados referente ao intervalo de tempo em que as variáveis dependentes e independentes foram coletadas com $t = 1, \ldots, n$ períodos e n = número de intervalos de tempo adotado (ano, mês, semanas, por exemplo). Y_t representa a variável dependente ao longo do período t, X_{s_t} denota o conjunto de variáveis independentes avaliadas ao longo do período t e Xr_{s_t} o conjunto de variáveis independentes relevantes ao conjunto Y_t. Cada um dos períodos investigados é representado por um subconjunto de s_t, denotado por s_{t1}, s_{t2}, ..., s_{tk}, com $k = 1, \ldots, m$ e m = número de períodos definidos

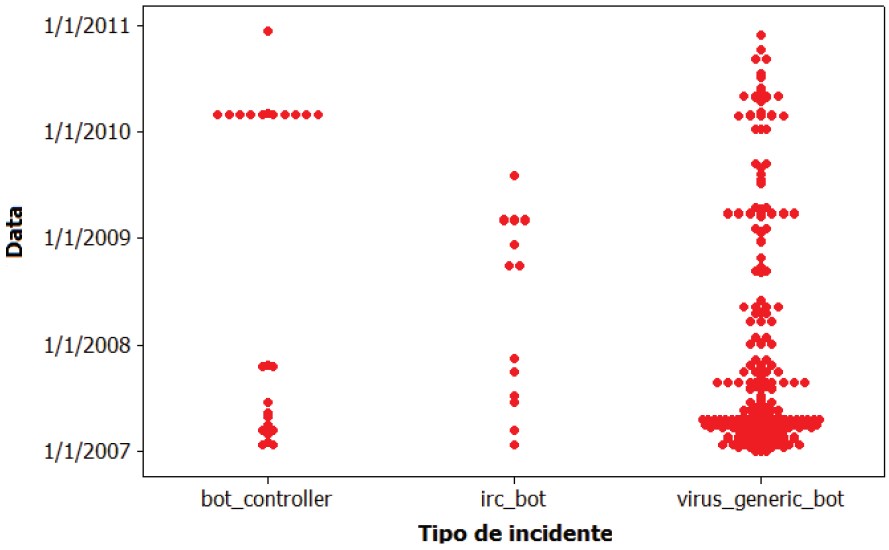


Figura 4.4: Distribuição de incidentes Bot

para análise e $k < n$. O número de intervalos escolhidos também deve respeitar o tamanho mínimo da amostra para a aplicação de regressão ou qualquer outro tipo de método para análise multivariada. Existem diversos trabalhos que discutem os tamanhos mínimos de amostra para análises multivariadas. Para uma regressão linear múltipla com o intuito de fornecer somente a explicação das variáveis, um número mínimo de 50 amostras é exigido Green (1991).

O critério proposto consiste em:

1. Aplicar o modelo de regressão nos conjuntos X_t e Y_t com o objetivo de encontrar o conjunto de variáveis independentes relevantes Xr_{s_t} referente ao intervalo completo de tempo;

2. Definir os m intervalos de tempo para investigação;

3. Aplicar os modelos de regressão nos conjuntos X_{t1} e Y_{t1}, X_{t2} e Y_{t2}, ..., X_{tk} e Y_{tk}, com o objetivo de encontrar os conjuntos de variáveis independentes relevantes $Xr_{s_{t1}}$, $Xr_{s_{t2}}$, ..., $Xr_{s_{tk}}$, com $k = 1, \ldots, m$;

4. Comparar as variáveis independentes relevantes presentes no conjunto Xr_{s_t}, com as variáveis independentes relevantes presentes em cada um dos conjuntos $Xr_{s_{t1}}$, $Xr_{s_{t2}}$,

..., $Xr_{s_{tk}}$;

5. O resultado da intersecção entre os conjuntos Xr_{s_t} e $Xr_{s_{t1}}$, Xr_{s_t} e $Xr_{s_{t2}}$, ..., Xr_{s_t} e $Xr_{s_{tk}}$ fornece um novo grupo de métricas. As métricas presentes nesse grupo serão denominadas indicadores;

De acordo com os critérios descritos acima e os nove períodos analisados, as seguintes métricas coletadas no ambiente da University of Maryland podem ser consideradas indicadores de incidentes:

- Bot - número de alvos (T_t (G1)) e número de alvos por atacante (TAt_t (G2));
- Hacking - número de atacantes (At_t (G2)) e número de alertas por alvo (AlT_t (G1));
- Spam - número de alvos (T_t (G2)).

a partir da definição de um conjunto de indicadores de incidentes, novas regras para a prevenção de incidentes podem ser desenvolvidas. Como os resultados da regressão mostraram que existe uma associação entre o aumento do número de alvos externos atacados por computadores da University of Maryland (T_t (G2)) e o aumento do número de incidentes Spam. Essa informação pode ser usada para alertar a equipe de TIC sobre a possibilidade de um aumento no número de incidentes Spam, auxiliando as tomadas de decisão.

A seguir, será mostrado como as métricas relevantes (ou os indicadores selecionados) podem ser usados para alertar a equipe de TIC sobre possíveis eventos. A ideia consiste em comparar o comportamento das métricas quando o número de incidentes de segurança aumenta. O método conhecido como Teste de Laplace permite a identificação de tendência em um conjunto de dados baseado em um valor $u(t)$ por um período $[0, t]$ e é definido da seguinte forma (Kanoun et al., 1991):

$$u(t) = \frac{\frac{\sum_{i=1}^{t}((i-1)n_i)}{N(t)} - \frac{t-1}{2}}{\sqrt{\frac{t^2-1}{12(N(t))}}} \tag{4.2}$$

onde t representa o número de dias (ou outra unidade de tempo), n_i é a variável analisada no tempo i (o número de incidentes Bot ou número de alvos, por exemplo) e $N(t)$ é o

número cumulativo referente a variável que está sendo analisada (o número cumulativo de incidentes Bot ou número cumulativo de alvos, por exemplo).

A interpretação prática do Teste de Laplace pode ser feita em dois níveis (Chrun, 2011):

- Globalmente: quando o valores do coeficiente de Laplace são maiores do que 2 ou -2. Se os valores são positivos (negativos), existe um aumento global (diminuição) na variação analisada. Valores entre -2 e $+2$ indicam estabilidade;

- Localmente: valores que aumentam (diminuem) indicam um aumento (diminuição) local da variável analisada.

Dessa forma, a abordagem proposta consiste em examinar os valores de tendência dos incidentes de segurança em um determinado período de tempo e comparar com os valores de tendência das métricas relevantes no mesmo período. Se a tendência observada em uma variável (incidente) segue a tendência observada na outra variável (métrica), então é possível propor maneiras para alertar a equipe de TIC sobre possíveis eventos de segurança.

Primeiramente, serão analisados os valores do Teste de Laplace para os incidentes Bot, Hacking e Spam em todo o período de investigação. As Figuras 4.5, 4.6 e 4.7 apresentam esses valores. Será selecionado em cada gráfico um período para investigação. O critério adotado é a escolha de períodos onde exista uma tendência de aumento global nos valores. Dessa forma, os seguintes períodos foram selecionados: i) Bot, entre 10/04/2007 e 12/05/2007 (dias 100 a 132), ii) Hacking, entre 05/10/2010 e 13/11/2010 (dias 1374 a 1413) e iii) Spam, entre 01/11/2009 e 12/12/2009 (dias 1036 a 1072).

O próximo passo consiste em selecionar as métricas relevantes para cada tipo de incidente e criar o gráfico com os valores do coeficiente $u(t)$ do Teste de Laplace para cada período. As métricas relevantes escolhidas, em nosso caso, serão os indicadores de incidentes: número de alvos (T_t (G1)) e número de alvos por atacante (TAt_t (G2)) para o incidente Bot, número de atacantes (At_t (G1)) para o incidente Hacking e número de alvos (T_t (G2)) para o incidente Spam. As Figuras 4.8, 4.9 e 4.10 mostram os valores do coeficiente $u(t)$ para cada tipo de incidente.

A Figura 4.8 mostra uma tendência de aumento no número de incidentes Bot no dia 14. É possível notar também uma tendência de aumento no número de alvos (T_t (G1))

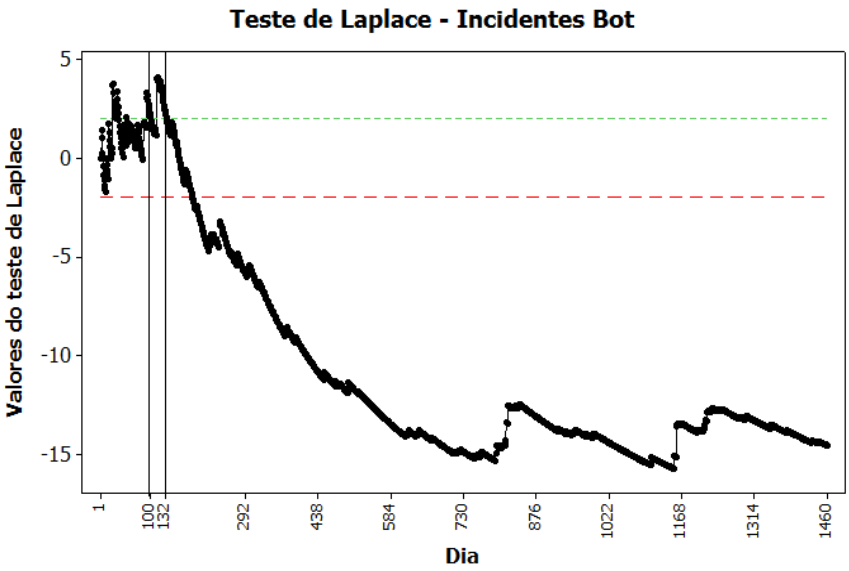


Figura 4.5: Teste de Laplace - Incidentes Bot

alguns dias antes do dia 14 e que começa a diminuir bem próximo do dia 14. Além disso, é possível notar um aumento no número de alvos por atacante (TAt_t (G2)) logo após o dia 14. Essa combinação de resultados indica que:

1. Houve uma alteração (aumento) no número de alvos antes do número de incidentes Bot se movimentar (aumentar);

2. Houve uma alteração (aumento) no número de alvos por atacante depois do número de incidentes se movimentar (aumentar);

Comparando com a terminologia usada nos indicadores econômicos, o primeiro caso é conhecido como um indicador antecedente ou futuro (*leading indicator*). Já o segundo caso é conhecido como indicador atrasado ou passado (*lagging indicator*). Indicadores futuros e passados refletem condições que existem antes ou depois de uma alteração na segurança (Jansen, 2010).

Uma análise similar pode ser feita para os outros incidentes (Hacking e Spam). A Figura 4.9 apresenta dois períodos de tempo onde o número de incidentes Hacking apresenta tendências de crescimento: próximo aos dias 6 e 42. Note que para ambos os períodos, o número de atacantes (G2) também mostra uma tendência de crescimento um pouco antes

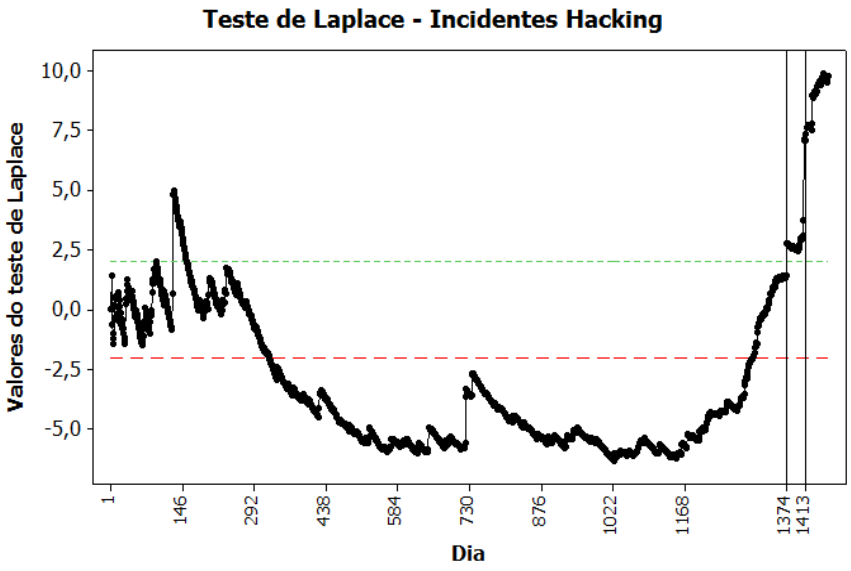


Figura 4.6: Teste de Laplace - Incidentes Hacking

do aumento do número de incidentes. Esse resultado sugere que o número de atacantes (G2) se comporta como um indicador antecedente para os incidentes do tipo Hacking. Já a Figura 4.10, referente aos incidentes do tipo Spam, ilustra uma tendência de crescimento dos incidentes a partir do dia 14 e alguns dias depois (entre os dias 21 e 25) o número de alvos (G2) também apresenta uma tendência de crescimento. Nesse caso o número de alvos (G2) pode ser interpretado como um indicador atrasado para os incidentes Spam.

Um analista de segurança poderia usar esses resultados da seguinte forma:

- Disparar alertas quando o número de alvos (G1) aumentar, identificando um possível aumento no número de incidentes Bot;
- Disparar alertas quando o número de atacantes (G2) aumentar, identificando um possível aumento no número de incidentes Hacking;
- Identificar possíveis eventos de segurança que já ocorreram (ou ainda estão ocorrendo), quando o número de alvos por atacante aumentar, mas nenhuma tendência de crescimento de incidentes Bot foi previamente detectada;
- Identificar possíveis eventos de segurança que já ocorreram (ou ainda estão ocorrendo), quando o número de alvos (G2) aumentar, mas nenhuma tendência de cres-

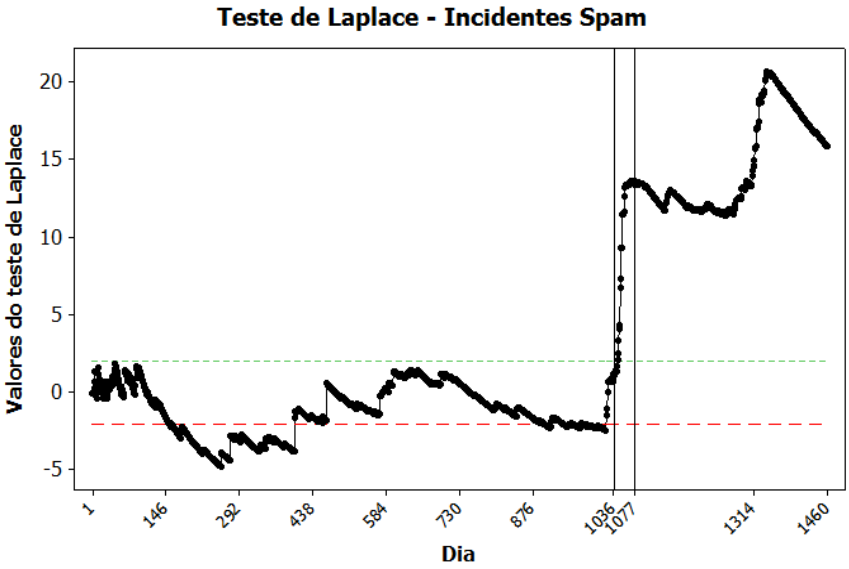


Figura 4.7: Teste de Laplace - Incidentes Spam

cimento de incidentes Spam foi previamente detectada.

A última implicação prática discutida nessa seção é relacionada a análise da eficiência do IPS com relação aos diversos tipos de incidentes. Existem alguns fatores usados para avaliar a eficiência de sistemas de detecção/prevenção de intrusão, como: as regras de detecção definidas pelos administradores, as políticas de atualização de assinaturas, a taxa de falso positivos/negativos e o contexto em que o dispositivo está localizado. A identificação de métricas relevantes para determinados tipos de incidentes fornece um outro modo para avaliação da eficiência de um IPS.

Conforme mencionado anteriormente, uma rápida análise na Tabela 4.5 sugere que o IPS da University of Maryland possui uma identificação maior com os incidentes Bot (três métricas relevantes) do que com os incidentes Hacking (duas métricas relevantes) ou com os incidentes Spam (somente uma métrica relevante). Para verificar esse resultado, foi realizado um estudo similar ao mostrado anteriormente, com nove períodos de tempo: 2007, 2008, 2009, 2010, 2007/2008, 2008/2009, 2009/2010, 2007/2008/2009 e 2008/2009/2010. A partir desse estudo, é possível estimar o nível de associação entre um determinado tipo de incidente e o dispositivo IPS pela presença e quantidade de métricas relevantes em um determinado período de tempo.

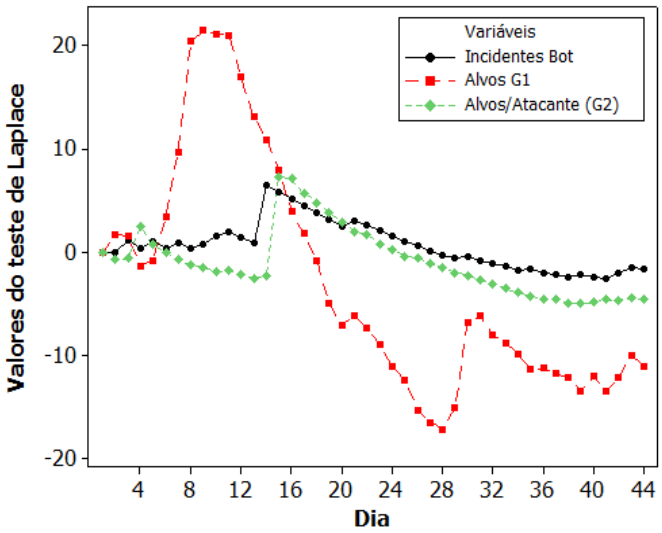


Figura 4.8: Valores do teste de Laplace entre 10/04/2007 e 12/05/2007.

Seja t o número de períodos analisados, a_t o número total de métricas relevantes no período t e b_i a presença (0 ou 1) de ao menos uma métrica relevante no período t. O coeficiente C_j de associação entre um determinado tipo de incidente j e um conjunto de métricas relevantes é calculado da seguinte forma:

$$C_j = \frac{p_j}{t} \sum_{i=1}^{t} a_i^{(j)} \tag{4.3}$$

onde $p_j = \frac{1}{t} \sum_{i=1}^{t} b_i^{(j)}$, com $0 \leq p_j \leq 1$. A notação $a_i^{(j)}$ representa o cálculo de a_i para cada tipo de incidente j.

A ideia do coeficiente é representar não só a quantidade de métricas relevantes em um determinado período, mas também levar em consideração os períodos em que nenhuma métrica foi considerada relevante. A Tabela 4.7 mostra os resultados dessa análise, que também inclui o período completo 2007/2008/2009/2010.

De acordo com a tabela, os coeficientes de associação para cada tipo de incidente são:

$C_{Bot} = 0,7 * 2 = 1,4$

$C_{Hacking} = 0,6 * 1,3 = 0,78$

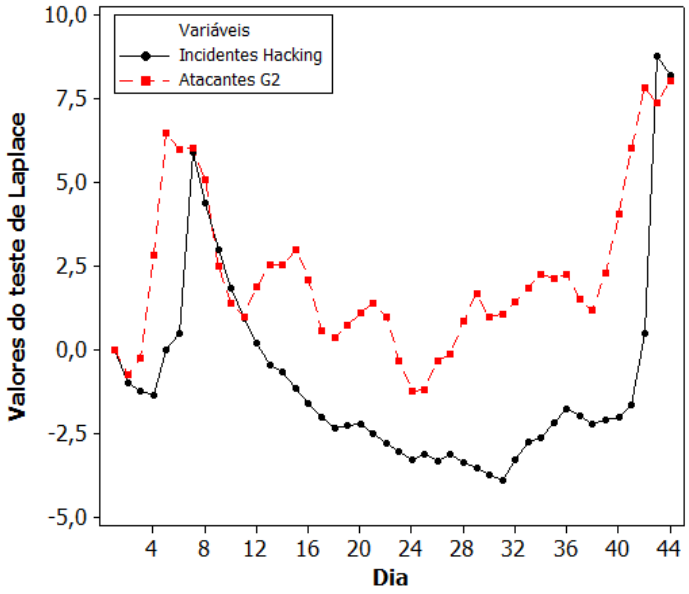


Figura 4.9: Valores do teste de Laplace entre 05/10/2010 e 13/11/2010.

$C_{Spam} = 0,8 * 1 = 0,8$

É possível notar que, entre os tipos de incidentes estudados, Bot foi o que obteve o maior grau de associação. Além disso, entre todos os períodos analisados, em quatro deles (2007, 2008, 2007/2008/2009 e 2007/2008/2009/2010) os incidentes Bot têm mais métricas relevantes do que Hacking e Spam. Em somente um período (2009/2010) foram encontradas mais métricas relevantes do tipo Hacking, analogamente para o Spam

Tabela 4.7: Evolução das métricas relevantes por tipo de incidente

Período	Bot	Hacking	Spam	Total
2007	3	0	1	4
2008	4	0	2	6
2009	1	0	1	2
2010	0	1	1	2
2007-2008	3	3	0	6
2008-2009	1	0	1	2
2009-2010	0	1	2	3
2007-2008-2009	5	4	1	10
2008-2009-2010	0	2	0	2
2007-2008-2009-2010	3	2	1	6
Total	20	13	10	43

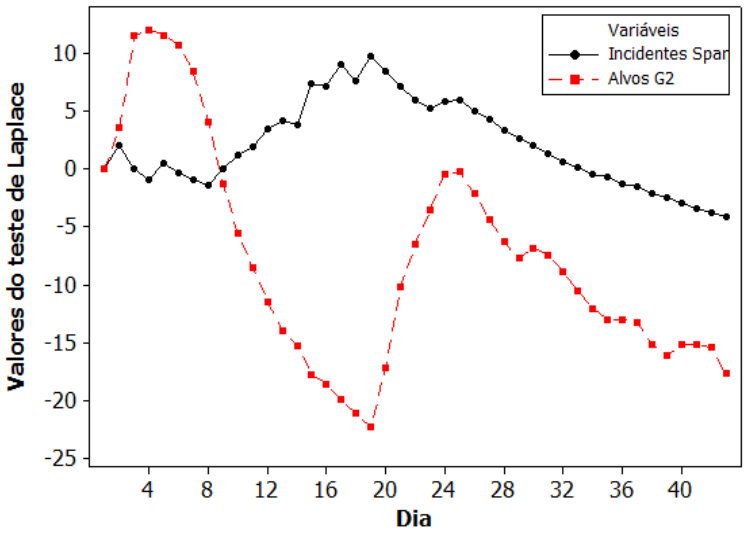


Figura 4.10: Valores do teste de Laplace entre 01/11/2009 e 12/12/2009.

(2008/2009/2010). Tais resultados confirmam o que foi discutido anteriormente sobre o dispositivo IPS investigado possuir uma identificação maior com os incidentes Bot. É importante notar que esse resultado está diretamente ligado ao conjunto de métricas que foi definido para o estudo. A investigação de novas métricas extraídas do sistema de prevenção de intrusão pode mudar essa perspectiva.

Ainda com relação a Tabela 4.7, ao analisar somente os períodos que contém o ano de 2010, os resultados serão sensivelmente diferentes. Em 2010, não foram encontradas métricas relevantes para os incidentes Bot. O mesmo aconteceu nos períodos 2009/2010 e 2008/2009/2010. Somente na análise dos quatro anos (2007/2008/2009/2010) que as métricas relevantes para os incidentes Bot voltaram a aparecer. Isto evidencia que, apesar do resultado geral mostrar que o IPS investigado possui uma identificação maior com os incidentes Bot, o cenário se modificou em 2010. Estudos adicionais nos anos de 2011 e 2012 podem confirmar essa hipótese. Este novo comportamento pode ter sido causado pela descoberta de novos incidentes de segurança ou também devido a alteração de regras no IPS. A Figura 4.11 apresenta o número cumulativo de cada um dos incidentes de segurança por semana. Conforme discutido, é possível notar uma mudança de comportamento

(aumento) no número de incidentes Hacking e Spam no final do ano de 2010, quando comparado ao comportamento do início do ano.

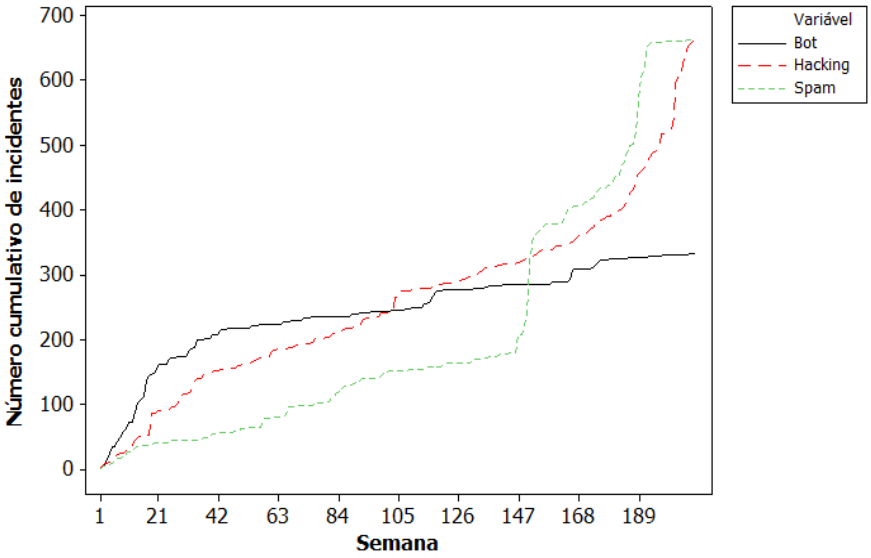


Figura 4.11: Número cumulativo de incidentes de segurança por semana

É possível usar esse tipo de informação como um método alternativo para avaliar a eficiência de sistemas de prevenção / detecção de intrusão. Considere que uma organização concluiu que seu dispositivo IPS, ao longo dos últimos anos, possui uma identificação maior com um determinado tipo de incidente. Se esse comportamento muda, existe também um indicativo de mudança no próprio dispositivo ou nos ataques. Ausência ou atraso nas atualizações de assinaturas e alterações nas configurações são alguns exemplos, assim como o surgimento de novos tipos de ataques ou diminuição de determinados tipos de ataque.

4.1.5 Resumo dos resultados

Os principais resultados encontrados na presente seção podem ser sumarizados da seguinte forma:

- Desenvolvimento de técnica para avaliação da relevância de métricas de segurança usando modelos de regressão híbridos;

- Identificação de indicadores de incidentes a partir da análise temporal de métricas significativas;
- Aplicação do teste de Laplace para detectar movimentos futuros e atrasados na frequência de incidentes de segurança;
- Criação de um método para avaliar a eficiência de sistemas de prevenção de intrusão com base na quantificação da relação entre os tipos de incidentes e as métricas que refletem as características dos ataques bloqueados pelo IPS.

Com relação aos resultados específicos para o ambiente estudado (University of Maryland):

- Foi encontrada evidência empírica de que métricas de segurança extraídas dos dados de IPS são relacionadas aos incidentes de segurança;
- A posição dos ataques bloqueados influencia os incidentes de segurança: métricas referentes as tentativas de ataques dos computadores de dentro da organização para alvos fora da organização (G2) possuem uma relação melhor com os incidentes reportados;
- A relevância das métricas varia de acordo com o tipo de incidente: número de alvos (G1), número de alvos por atacante (G2) e número de alertas por atacante (G2) para os incidentes Bot, número de atacantes (G2) e número de alertas por alvo (G1) para os incidentes Hacking e número de alvos (G2) para os incidentes Spam;
- O tipo de incidente Bot foi o que obteve o maior grau de associação com o dispositivo IPS investigado (de acordo com as 12 métricas definidas).

4.2 Outros fatores que influenciam a ocorrência de incidentes de segurança

Na seção anterior foi apresentado como investigar a relação entre uma métrica e um determinado alvo ou processo de segurança (incidentes de segurança) e também diversos

desdobramentos obtidos com essa análise. Foram usadas métricas obtidas com o auxílio dos dados de um sistema de prevenção de intrusão. Porém, outros fatores podem influenciar a ocorrência de incidentes de segurança. O principal objetivo desse segundo estudo é propor uma análise complementar sobre outros tipos de fatores que podem influenciar a ocorrência de incidentes de segurança.

O conjunto de dados usado neste estudo foi fornecido pelo CAIS/RNP e cada um dos incidentes reportados possui os seguintes atributos: i) número de identificação, ii) data, iii) identificação da instituição que reportou o incidente, iv) categoria do incidente, v) tipo do incidente e iv) estado de origem da instituição que reportou o incidente. A partir da avaliação de tais dados, e inspirado por estudos anteriores sobre comprometimento de contas de usuários em universidades (Zhang et al., 2012a) e (Zhang et al., 2012b), os seguintes fatores são estudados:

- Fatores temporais - verificar se a ocorrência dos incidentes varia de acordo com certos períodos, como em diferentes épocas do ano;
- Associação entre incidentes - analisar a relação entre os diferentes tipos de incidentes;

Os detalhes sobre os dados de incidentes de segurança fornecidos pelo CAIS/RNP, a metodologia utilizada para o estudo de cada um dos fatores e os resultados serão mostrados a seguir.

4.2.1 Dados - CAIS/RNP

Primeira rede de acesso à Internet no Brasil, a Rede Nacional de Ensino e Pesquisa (RNP) integra mais de 800 instituições de ensino e pesquisa no país, beneficiando mais de 3,5 milhões de usuários. A RNP foi criada em 1989 pelo Ministério da Ciência e Tecnologia com o objetivo de construir uma infraestrutura de rede para a comunidade acadêmica. A rede começou a ser construída em 1991. Em 1994, já atingia todas as regiões do país. Entre 2000 e 2001, a rede foi totalmente atualizada para oferecer suporte a aplicações avançadas. Desde então, o backbone RNP, como é chamado, possui pontos de presença em todos os estados brasileiros. Em 2005, a tecnologia do backbone foi novamente atualizada com links ópticos operando a múltiplos gigabits por segundo.

Além de melhorar a infraestrutura de redes em níveis nacional, metropolitano e local (redes de campus), atender as demandas de comunidades específicas (telemedicina, biodiversidade, astronomia etc.) e promover a capacitação de recursos humanos em tecnologias da informação e comunicação, a RNP também atua na detecção, resolução e prevenção de incidentes de segurança através do CAIS. Criado em 1997, o CAIS também divulga informações, alertas de segurança e participa de organismos internacionais na área. As atividades do CAIS incluem:

- Atendimento a incidentes de segurança;
- Coordenação com grupos de segurança já existentes;
- Fomento à criação de novos grupos de segurança no país;
- Disseminação de informações na área de segurança em redes;
- Divulgação de recomendações e alertas;
- Testes e recomendação de ferramentas de segurança;
- Recomendação de políticas para a RNP;
- Recomendação de políticas para os provedores;
- Recomendação de políticas para o backbone da RNP.

Os dados disponibilizados pelo CAIS consistem em incidentes de segurança referentes a RNP de forma direta ou indireta. A forma direta diz respeito quando uma instituição filiada a rede está envolvida no incidente, seja como origem ou destino do ataque. Já a forma indireta acontece quando o CAIS descobre e notifica incidentes relacionados a outras instituições não filiadas a RNP (como bancos ou outros grupos de segurança). Por exemplo, se o CAIS encontra uma página fraudulenta de um banco hospedada em uma máquina em outro país, o CAIS notifica o banco sobre isso. Indiretamente, é de interesse da RNP que tal problema seja resolvido.

O CAIS disponibiliza em sua página na Internet somente as estatísticas de incidentes reportados por ano, sem nenhum tipo de agrupamento. Após reuniões com diretores e

Tabela 4.8: Resumo dos incidentes (2011/2012) - CAIS/RNP

Número de incidentes	Número de instituições	Número de categorias	Número de tipos
452.766	422	8	15

responsáveis, os seguintes dados entre 01/01/2011 e 31/12/2012 foram cedidos: i) número de identificação do incidente, ii) data que o incidente foi reportado, iii) identificação da instituição que reportou o incidente, iv) categoria do incidente, v) tipo do incidente e iv) estado de origem da instituição que reportou o incidente.

Devido a restrições de privacidade, dados sobre a origem e destino dos ataques não foram cedidos. Além disso, os registros referentes a identificação da instituição que reportou o incidente foram sanitizados também por questões de privacidade. A Tabela 4.8 sumariza os dados. Dentre os incidentes investigados, 319.327 foram reportados em 2011 e 133.439 em 2012.

O conjunto de dados possui 422 instituições filiadas ao RNP e identificadas por um indicador único. Quatro tipos de incidentes foram encontrados: incidentes vinculados a instituições com identificação de estado, incidentes vinculados a instituições mas sem identificação de estado, incidentes que não estão vinculados a instituições mas com identificação de estado e incidentes que não estão vinculados a instituições e não possuem identificação de estado. Os casos em que os incidentes não são vinculados a instituições representam incidentes recebidos e tratados pelo CAIS, mas sem ligação ao RNP. Exemplos dessa situação incluem um usuário comum escrevendo ao CAIS para colaborar com o catálogo de fraudes e bancos solicitando filtros contra sites hospedando páginas falsas.

Conforme as regras do CAIS, cada instituição está vinculada a somente um estado. Ao longo da análise foram encontradas algumas inconsistências na base de dados, com uma instituição vinculada a mais de um estado. Tais inconsistências foram informadas ao CAIS e consequentemente solucionadas antes do encerramento das investigações.

A taxonomia de incidentes do CAIS inclui 9 categorias e 24 tipos:

1. Conteúdo abusivo - Spam, Assédio/Discriminação;

2. Código malicioso - Bot, Worm, Vírus, Trojan, Spyware, Scripts;

3. Prospecção por informações - Varredura, Escuta não autorizada, Engenharia social;
4. Tentativa de intrusão - Tentativa de exploração de vulnerabilidades, Tentativa de login;
5. Intrusão - Comprometimento de conta de usuário, Comprometimento de aplicação;
6. Indisponibilidade de serviço ou informação - Negação de Serviço e Sabotagem;
7. Segurança da informação - Acesso não autorizado à informação e Modificação não autorizada da informação;
8. Fraude - Violação de direitos autorais, Fingir ou falsificar identidade ou instituição e Uso de recursos de forma não autorizada;
9. Outros - Incidentes não representados anteriormente.

A Tabela 4.9, mostra os incidentes reportados por tipo. Os dados revelam uma polarização dos incidentes. Mais de 80% de todos os incidentes reportados entre 2011 e 2012 são do tipo Bot. Grande parte desse número (281.965) foi reportado em 2011, conforme apresenta a Figura 4.12. Mesmo considerando somente o número de incidentes Bot reportado no ano de 2012 (86.943), a diferença ainda é grande quando comparado ao número de Spam, segundo colocado na lista. Isso mostra que esse tipo de ataque ainda é muito comum no Brasil, mesmo com estudos sugerindo que atacantes estão trocando a criação de redes de Bot por ataques online que exploram vulnerabilidades de segurança (Maslennikov e Namestnikov, 2012).

Outro dado interessante é relacionado aos incidentes por estado. A Tabela 4.10, apresenta o número de incidentes reportados por estado, o número de instituições por estado e também a taxa de incidentes por instituição.

É possível notar que mais de 32% dos incidentes reportados são oriundos dos estados do Rio de Janeiro e Santa Catarina. Com 28 instituições (27 filiadas e 1 representando os incidentes sem instituição definida, mas com origem no estado) e nenhum Grupo de Segurança e Resposta a Incidentes (CSIRT) oficialmente cadastrado (CERT.br, 2013), o resultado em Santa Catarina se destaca. Outro resultado que chama atenção é o do estado da Bahia. Apesar de possuir um CSIRT e contar com 18 instituições (17 filiadas

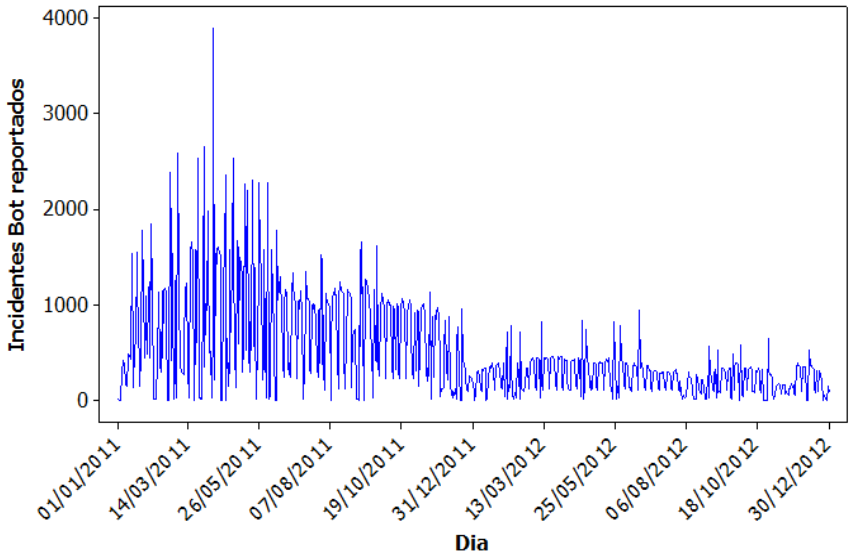


Figura 4.12: Incidentes Bot - 2011/2012 (CAIS/RNP)

e 1 representando os incidentes sem instituição definida, mas com origem no estado), somente 549 incidentes foram reportados nos dois anos de estudos. Foi um número muito próximo ao encontrado no estado do Roraima, com somente 6 instituições. A presença de profissionais de segurança pode ter um efeito benéfico na organização, reduzindo o número de incidentes reportados ao longo prazo (Chrun, 2011). Porém, o resultado também pode indicar uma baixa atividade de ataques em tal região. Dados adicionais seriam necessários a fim de diagnosticar qual da duas situações acima o estado da Bahia se encaixa. Nessa mesma linha, outro resultado que chama a atenção é a alta taxa de incidentes por número de instituições que o estado da Paraíba obteve.

A análise de estatísticas simples, como as exibidas anteriormente, motiva a investigação de fatores que influenciam a ocorrência de incidentes de segurança. A seguir, a metodologia proposta é apresentada.

4.2.2 Metodologia

O fator temporal é o primeiro a ser analisado. A detecção de padrões em segurança da informação auxilia o desenvolvimento de modelos de predição mais eficientes e também revela tendências que podem ser usadas para auxiliar a tomada de decisões. Estudos

Tabela 4.9: Resumo dos incidentes por tipo (2011/2012) - CAIS/RNP

Tipo de incidente	Número de incidentes	Porcentagem
Bot	369.331	81,5727%
Spam	19.667	4,3438%
Fingir ou Falsificar Identidade	12.327	2,7226%
Comprometimento de Aplicação	10.335	2,2827%
Tentativa de Login	8.292	1,8314%
Violação de Direitos Autorais	8.116	1,7925%
Outros	6.894	1,5227%
Incidentes não Representados	6.773	1,4959%
Tentativa de Exploração de Vulnerabilidades	5.547	1,2251%
Uso de Recursos de Forma não Autorizada	4.652	1,0275%
Varredura	474	0,1047%
Worm	185	0,0409%
Negação de Serviço	121	0,0267%
Vírus	30	0,0066%
Comprometimento de Conta de Usuário	19	0,0042%

anteriores (Chrun, 2011), demonstram que existe uma tendência de crescimento no número de incidentes de segurança logo nos primeiro dias referentes ao início do semestre letivo. Além disso, outro estudo (Condon e Cukier, 2012) realizado na University of Maryland, mostra que o semestre de outono (Agosto - Dezembro), possui, proporcionalmente mais incidentes do que os outros dois semestres do calendário norte-americano (Janeiro - Maio e Junho - Julho). Com base em tais trabalhos, a forma com que os incidentes de segurança variam ao longo do tempo será investigada.

Um conjunto de observações x_t, cada uma gravada em tempo específico t é chamado de série temporal (Brockwell e Davis, 2002). O conjunto de dados de incidentes de segurança reportados por dia, é um exemplo de uma série temporal. Em especial, esse tipo de série é definida como série temporal discreta, quando as observações são feitas em intervalos de tempo fixos.

Uma série temporal possui, em geral, quatro tipos de comportamentos:

- Tendência - Uma tendência existe quando existe um aumento ou diminuição em um longo período nos dados, não necessariamente linear;

Tabela 4.10: Resumo dos incidentes por estado (2011/2012) - CAIS/RNP

Estado	Número de incidentes	Porcentagem	Número de instituições	Taxa (Incidentes/Número de instituições)
pop-ac	1824	0,402%	2	912,00
pop-al	11346	2,505%	7	1620,86
pop-am	1849	0,4084%	12	154,08
pop-ap	1529	0,3377%	4	382,25
pop-ba	549	0,1213%	18	30,50
pop-ce	10556	2,331%	16	659,75
pop-df	31428	6,941%	27	1164,00
pop-es	4251	0,9389%	12	354,25
pop-go	9306	2,0554%	13	715,85
pop-ma	5440	1,2015%	6	906,67
pop-mg	26384	5,8273%	32	824,50
pop-ms	3508	0,7748%	7	501,14
pop-mt	5155	1,1386%	14	368,21
pop-pa	6479	1,431%	11	589,00
pop-pb	29957	6,6165%	11	2723,36
pop-pe	32525	7,1837%	23	1414,13
pop-pi	3667	0,8099%	8	458,38
pop-pr	32403	7,1567%	22	1472,86
pop-rj	89372	19,7392%	53	1686,26
pop-rn	9423	2,0812%	8	1177,88
pop-ro	1389	0,3068%	4	347,25
pop-rr	561	0,1239%	6	93,50
pop-rs	11198	2,4733%	43	260,42
pop-sc	57574	12,7161%	28	2056,21
pop-se	2345	0,5179%	6	390,83
pop-sp	16678	3,6836%	48	347,46
pop-to	4248	0,9382%	7	606,86
sem-pop	41819	9,2364%	20	2090,95

- Sazonal - Esse tipo de padrão existe quando uma série é influenciada por períodos como mês, trimestre, semestre, ano e dia da semana. A sazonalidade sempre ocorre em um período fixado e conhecido;
- Cíclico - Um padrão cíclico ocorre quando os dados exibem crescimento e decrescimento em um período não fixo;
- Aleatório - Quando os dados não exibem nenhum dos comportamentos citados anteriormente.

Será analisado o comportamento do número de incidentes de segurança de acordo com dois intervalos de tempo: dia e mês. Duas métricas serão analisadas, o número de incidentes de segurança reportados por dia e o número de incidentes de segurança reportados por mês. A Figura 4.13 mostra o número de incidentes reportado por dia. A simples visualização do gráfico não é o suficiente para concluir se existe alguma tendência ou componente cíclico. Para isso, será usada a função de autocorrelação e também o índice de sazonalidade.

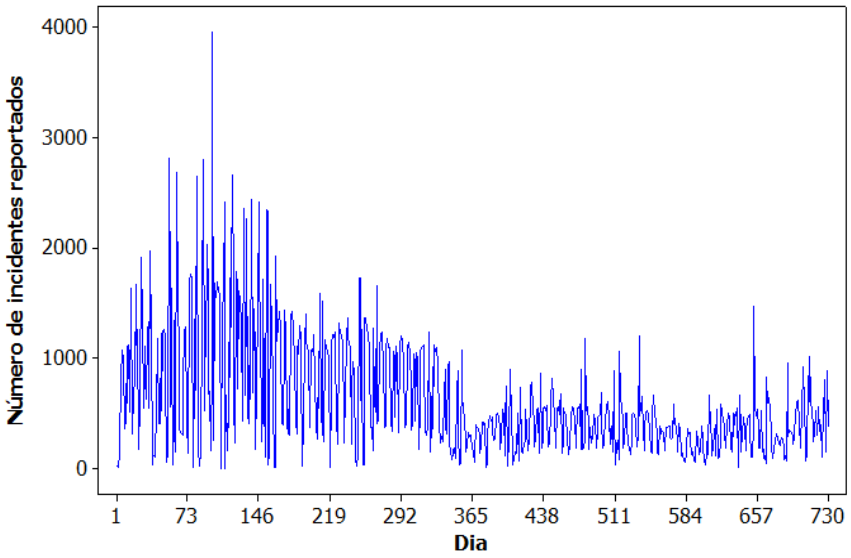


Figura 4.13: Incidentes - 2011/2012 (CAIS/RNP)

A autocorrelação é uma medida de dependência entre observações da mesma série, separadas por um determinado intervalo de observação (*lag*) (Wei, 1994). A análise da

autocorrelação fornece informações sobre a relação entre uma variável X medida no tempo t, com ela mesma medida em um tempo posterior $t + k$, onde k representa o intervalo de observação. Seja $z_b, z_{b+1}, \ldots, z_n$ os valores de uma série temporal, o coeficiente de autocorrelação r_k em um determinado intervalo de observação k é dado por:

$$r_k = \frac{\sum_{t=b}^{n-k} (z_t - \widehat{z})(z_{t+k} - \widehat{z})}{\sum_{t=b}^{b} (z_t - \widehat{z})^2} \tag{4.4}$$

onde $\widehat{z} = \frac{\sum_{t=b}^{n} z_t}{(n-b+1)}$ representa a média das observações. Valores do coeficiente de autocorrelação próximos de zero indicam ausência de persistência ou sazonalidade em tal intervalo de observação, enquanto que valores próximos de 1 mostram uma relação significativa associada a tal intervalo de observação. A análise da autocorrelação de uma série de dados frequentemente inclui a criação de um gráfico, chamado correlograma entre os valores do coeficiente de correlação e os intervalos de observação.

O valor de r_k, aliado a análise do correlograma são usados para estabelecer critérios sobre uma série temporal. Três possíveis situações podem ocorrer (Brockwell e Davis, 2002), (Croarkin e Tobias, 2003):

1. A série temporal é considerada aleatória ou estacionária se a maioria dos coeficientes de autocorrelação (geralmente, 95% dos valores para $p < 0.05$) estão entre os intervalos de confiança e nenhum padrão foi detectado no correlograma;

2. A série temporal é considerada não estacionária "moderada", quando os valores dos coeficientes de correlação diminuem lentamente conforme k aumenta, caracterizando um comportamento de tendência;

3. A série temporal é considerada não estacionária "forte", quando os valores dos coeficientes de correlação diminuem lentamente conforme k aumenta, mas de acordo com uma periodicidade, caracterizando um padrão sazonal;

A principal diferença entre as situações 2) e 3) é que uma série temporal não estacionária "moderada" não exibe um comportamento periódico. Nesses tipos de dados, é comum encontrar componentes isolados relacionados a uma tendência de crescimento (ou diminuição) ou ainda alguns tipos de padrões relacionados a sazonalidade.

Para obter uma estimativa razoável da função de autocorrelação, são necessárias no mínimo $N = 50$ observações e as autocorrelações devem ser calculadas para $k = 0, 1, \ldots, k$, com k não maior do que $N/4$. Para amostras com mais de 240 observações, uma estimativa de k é dada por $\sqrt{n} + 45$ (Black, 2011).

Primeiramente, serão calculados os coeficientes de correlação das $N = 730$ observações que contemplam os incidentes de segurança reportados por dia. Nesse caso, o número de intervalos usado é de $k = 72$. A Figura 4.14 apresenta o correlograma paras os intervalos de observação definidos.

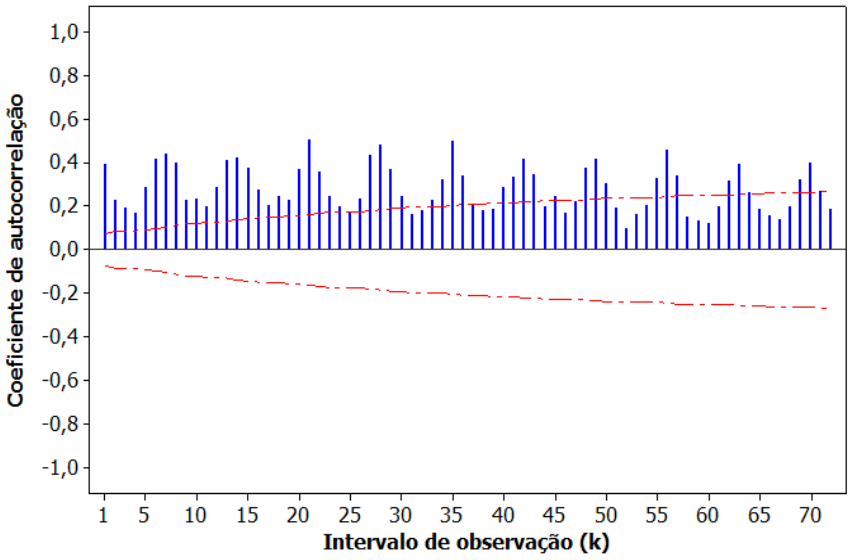


Figura 4.14: Correlograma - incidentes reportados entre 2011 e 2012

As linhas em vermelho presentes no correlograma representam um intervalo de confiança de 95% para os valores do coeficiente de autocorrelação. Os intervalos de confiança são usados para mostrar quando os coeficientes de autocorrelação podem ser significantemente diferentes de zero. Consequentemente, intervalos de observação com valores fora desses limites, possuem correlação significativa para o estudo.

É possível notar na Figura 4.14 que existe um padrão que se repete a cada 7 intervalos de observação, o que indica uma periodicidade nos dados a cada semana. Essa relação sugere um comportamento cíclico no modo em que os incidentes de segurança são reportados. Isto faz sentido, pois geralmente as equipes trabalham entre segunda e sexta-feira em

Tabela 4.11: Incidentes reportados por dia da semana

Dia da semana	Número total de incidentes reportados	Índice Z
Domingo	31791	-1,59607
Segunda	38529	-1,26905
Terça	73756	0,44061
Quarta	81021	0,79320
Quinta	81904	0,83605
Sexta	73742	0,43993
Sábado	71999	0,35534

horário comercial (09:00 - 18:00). Além disso, o fator humano envolvido pode desenvolver a presença de certos hábitos no processo de notificação de incidentes. O agrupamento dos incidentes de segurança por dia da semana pode ser usado para encontrar os intervalos de repetição. A Tabela 4.11 apresenta os incidentes agrupados e normalizados por dia da semana (usando o índice padrão z que mede o quão longe uma observação está da média, onde $z = \frac{x-\mu}{\sigma}$ com μ = média da população e σ = o desvio padrão da população).

Quarta e quinta-feira são os dias com as maiores ocorrências de incidentes de segurança, assim como domingo e segunda-feira são os dias com a menor ocorrência. A Figura 4.15 ilustra esse padrão com a representação da série temporal referente ao número de incidentes reportados somente no domingo e quinta-feira. Isso mostra que as notificações de ataque diminuem entre o domingo e segunda-feira, mas atingem um pico entre a quarta e quinta-feira. A partir dos resultados do correlograma e da análise dos incidentes normalizados por dia da semana foi possível extrair um padrão sobre o comportamento dos ataques e notificações de incidentes do CAIS/RNP.

Esse resultado indica que a periodicidade dos dados é um fator que deve ser levado em consideração na análise dos incidentes reportados pelo CAIS/RNP, especialmente no desenvolvimento de modelos de previsão de incidentes e análises exploratórias como a desenvolvida na seção anterior usando os dados da University of Maryland. A presença da periodicidade nos dados exige que outros modelos de regressão sejam utilizados, como os modelos conhecidos como auto-regressivos, ao invés da regressão linear. O correlograma do número de incidentes reportados pela University of Maryland entre 2007 e 2011 (Figura 4.16) ilustra a diferença do comportamento entre os dados do CAIS/RNP e da University of Maryland.

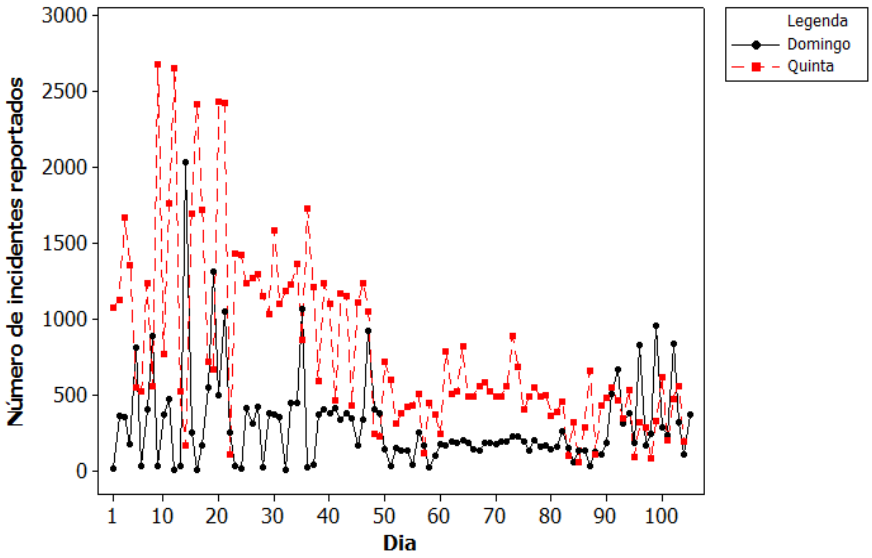


Figura 4.15: Incidentes reportados somente no domingo e quinta-feira

O padrão encontrado nos incidentes do CAIS/RNP diz respeito aos dados agregados de todas as instituições presentes no conjunto de dados. Uma questão importante consiste em identificar se o comportamento de cada instituição segue o mesmo padrão encontrado. Na próxima seção esse tópico será investigado com mais detalhes.

A análise mensal também pode ser útil para caracterizar o processo de notificação de incidentes realizado no CAIS. O gráfico da série temporal dos incidentes de segurança por mês é apresentado na Figura 4.17. É possível notar uma tendência de decrescimento logo após o mês de março de 2011. Além disso, nenhum outro comportamento sazonal ou cíclico nos meses é aparente. Para melhorar a compreensão entre os meses, outra análise deve ser feita. A Figura 4.18 apresenta a métrica número cumulativo de incidentes de segurança por mês em cada um dos anos. Apesar da diferença entre os números de incidentes reportados entre os anos, é possível notar uma similaridade entre os primeiros meses do ano seguido por um aumento no número de incidentes.

Nesse caso, como o número mínimo de amostras para usar a função de autocorrelação não é o suficiente $N = 24 < 50$, será usado um outro método para encontrar periodicidade em um conjunto de dados, conhecido como índice de sazonalidade (*seasonal index*) (Arsham, 2003). O índice representa a amplitude da influência sazonal para um determi-

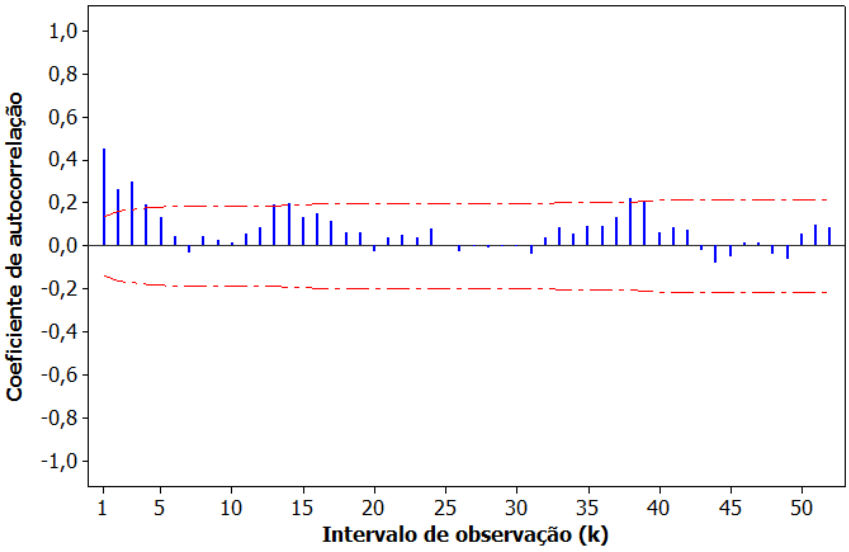


Figura 4.16: Correlograma - incidentes reportados entre 2007 e 2012 (University of Maryland)

nado período. O cálculo envolve a comparação entre o valor esperado para aquele período e a média entre todos os valores esperados. Um índice de sazonalidade mensal é calculado da seguinte forma:

$$S_i = \frac{d_i}{D} \tag{4.5}$$

onde S_i é o índice para o i-ésimo mês, d_i é a média aritmética do i-ésimo mês e D é a média aritmética entre cada um dos d_i. O índice mostra o quanto a média de um determinado período tente a ser maior ou menos do que a média global D. Por exemplo, um valor de S_i igual a $1,25$, indica que o valor esperado para aquele mês é 25% maior do que 1/12 da média global. Já um valor de S_i igual a 1, indica que o valor esperado para aquele mês representa 1/12 da média global.

A Figura 4.19 apresenta os valores do índice de sazonalidade para os doze meses entre os anos de 2011 e 2012. Os valores indicam que os valores esperados para os meses de Janeiro, Fevereiro, Julho, Agosto, Setembro, Novembro e Dezembro são menores do que a média global. Isto significa que o número de incidentes esperados para os meses de Março, Abril, Maio e Junho (referentes ao primeiro semestre acadêmico no Brasil) são

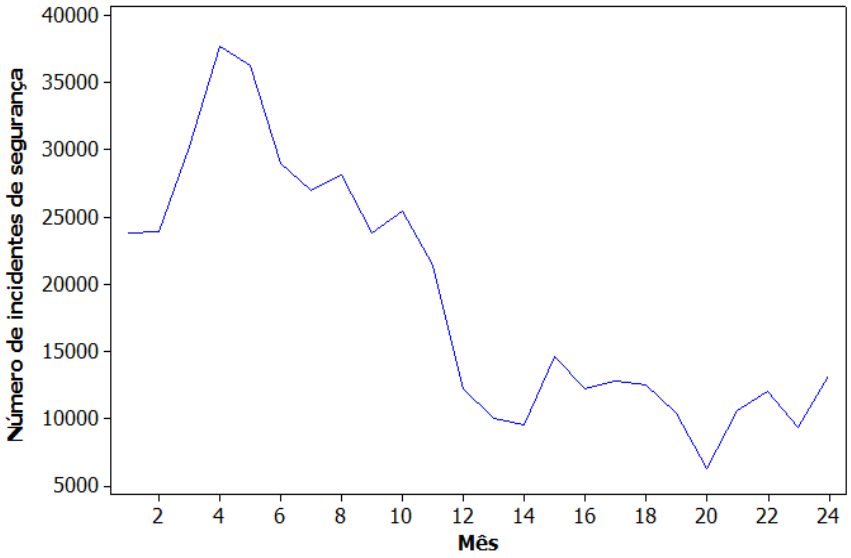


Figura 4.17: Número de incidentes de segurança por mês (CAIS/RNP)

maiores do que a média global. Esse resultado é semelhante ao encontrado por (Condon e Cukier, 2012) no semestre de outono da universidade analisada. Além disso, os meses de Janeiro e Fevereiro e Agosto e Setembro possuem valores semelhantes, revelando um comportamento similar entre esses meses.

Como os dados são referentes a instituições acadêmicas, esse resultado sugere uma tendência de aumento do número de incidentes após o início do primeiro período letivo (após os meses de Janeiro e Fevereiro). Conforme mostrado em (Chrun, 2011), o retorno dos estudantes as instituições e o aumento da população no campus pode ser um fator que impacta o número de incidentes de segurança. Para avaliar esse comportamento, é preciso estudar os anos de 2011 e 2012 separadamente. A Figura 4.20 mostra os valores do teste de Laplace para cada um dos anos.

Os valores de Laplace no gráfico indicam uma tendência de crescimento no número de incidentes após o mês de fevereiro. Em 2011 essa tendência seguiu até o mês de maio, enquanto em 2012, no mesmo período, foi detectada uma estabilidade. Nada pode ser afirmado com relação a ambos os períodos no segundo semestre devido a grande diferença de comportamento.

Portanto, é possível concluir que nenhum comportamento sazonal foi encontrado na

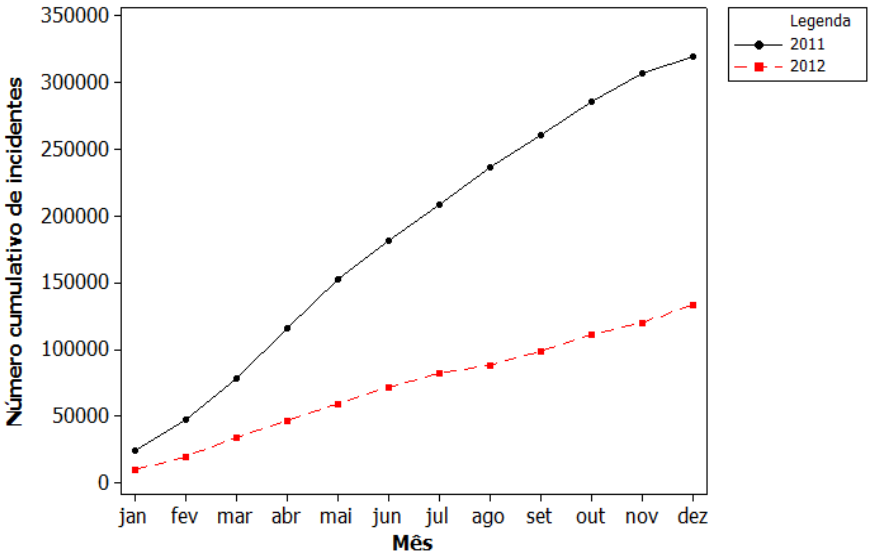


Figura 4.18: Número cumulativo de incidentes de segurança por mês (CAIS/RNP)

análise da métrica número de incidentes de segurança reportados por mês. Os resultados sugerem um crescimento do número de incidentes reportados após os meses de Janeiro e Fevereiro, porém, para a validação dessa hipótese outros dados são necessários.

Outra métrica relevante é o grau de associação entre os diferentes tipos de incidentes. Diversos estudos foram desenvolvidos para a criação de taxonomias para incidentes de segurança (Howard, 1997), (Vasiu e Vasiu, 2004), (Howard e Longstaff, 1998). O agrupamento de incidentes em categorias semelhantes auxilia o desenvolvimento de técnicas de prevenção que podem, eventualmente, ser aproveitadas por ataques de um mesmo tipo. Códigos maliciosos como bots, worms e vírus são um exemplo desse tipo de estratégia. Porém, o caminho usado por um atacante até o destino final do ataque, pode envolver uma série de ataques intermediários. O comprometimento da conta de um usuário pode ser usado para enviar Spam a outros usuários, assim como instalar softwares maliciosos em computadores. Alguns trabalhos tentam analisar a sequência e o comportamento de alguns tipos de ataques (Cooke et al., 2005), (Bento e Bento, 2004), porém, a ausência de dados empíricos dificulta outras investigações sobre o assunto.

A análise do relacionamento entre diferentes tipos de incidente é um passo inicial para entender como os incidentes de segurança são propagados na organização. O primeiro

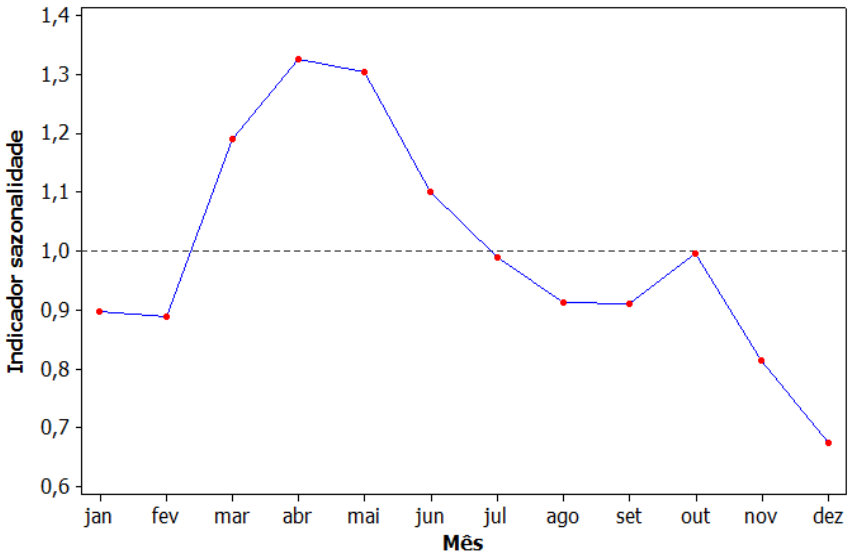


Figura 4.19: Índice mensal de sazonalidade - 2011/2012

passo para isso consiste em compreender o grau de associação entre os tipos de incidentes. Duas situações podem ocorrer entre dois tipos de incidentes A e B:

1. Um aumento (ou diminuição) do número de incidentes do tipo A está relacionado a um aumento (ou diminuição) do número de incidentes do tipo B no mesmo intervalo de observação t;

2. Um aumento (ou diminuição) do número de incidentes do tipo A está relacionado a um aumento (ou diminuição) do número de incidentes do tipo B após um determinado intervalo de tempo k.

Em ambos os casos, a associação pode ser estimada pelo cálculo de um coeficiente de correlação. No primeiro caso, o coeficiente de correlação de Pearson pode ser usado. Já no segundo caso, um possível método é o cálculo do coeficiente de correlação cruzada (*cross-correlation*). É importante notar que o valor do coeficiente de correlação fornece somente uma indicação da forma com que as séries estão relacionadas e também a força dessa relação. Uma provável causalidade envolvida entre essas duas séries deve ser investigada de maneira cuidadosa e usando uma sustentação teórica adequada.

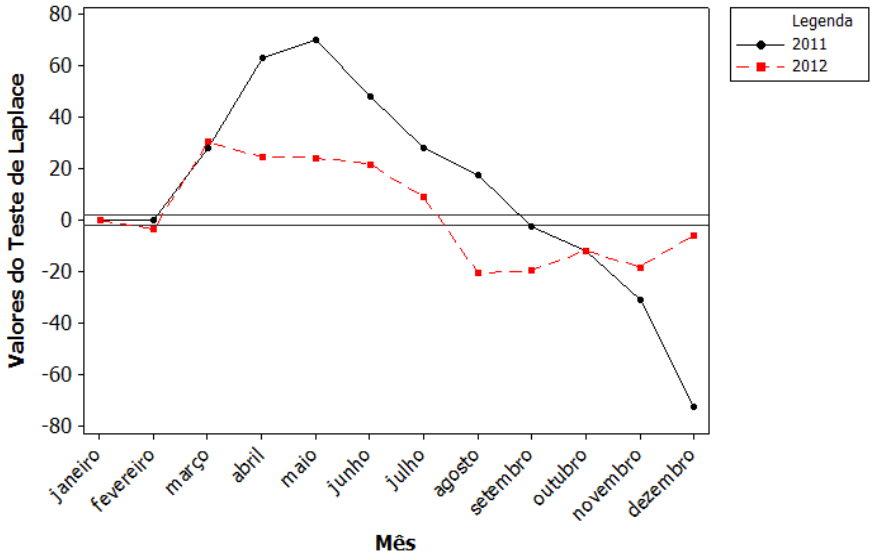


Figura 4.20: Teste de Laplace para o número de incidentes por mês

Suponha a existência de um relacionamento entre duas séries referentes a dois tipos de incidentes A e B. Um analista de segurança, pode usar esse fato para estudar a existência de causalidade entre os tipos de incidentes e em caso positivo, estabelecer a criação de políticas de prevenção e mitigação de incidentes. Se o comprometimento de conta de usuário possuir uma relação de causalidade com o número de softwares maliciosos, a organização pode usar essa informação para criar políticas de segurança para a proteção da conta de usuário, e assim afetar a quantidade de softwares maliciosos disseminados na organização.

Quando a causalidade não pode ser estabelecida, a relação entre os incidentes pode ser causada por outros fatores ou ainda ser apenas um comportamento aleatório entre as duas séries de dados. Se a varredura de serviços disponíveis possui uma relação com a tentativa de login usando "força bruta", esse pode ser um indício de que os serviços de login remoto como SSH estão funcionando em portas padrão e, consequentemente, aumentando as tentativas de login.

O coeficiente de correlação de Pearson, que reflete a intensidade de uma relação linear entre dois conjuntos de dados, é usado para estabelecer a primeira situação. Frequentemente denotado por r, o coeficiente é um índice adimensional com valores entre -1 e 1. O

sinal indica a direção positiva ou negativa do relacionamento, e o valor sugere a força da relação entre as variáveis. Uma correlação perfeita (-1 ou 1), indica que o valor de uma variável pode ser determinado exatamente ao se saber o valor da outra. No lado oposto, uma correlação de valor zero indica que não há relação linear entre as variáveis. Outras informações sobre o coeficiente podem ser encontradas em (Rodgers e Nicewander, 1988).

Já o coeficiente de correlação cruzada possui as mesmas características da correlação de Pearson, mas mede a correlação entre as séries em diferentes períodos de tempo. O coeficiente de correlação cruzada para um determinado período de tempo k é dado por (Wei, 1994):

$$s_{xy}(k) = \frac{\sum_{i=1}^{n-h} (x_{i+h} - \mu_x)(y_i - \mu_y)}{n^{-1} \sum_{i=1}^{n} (x_i - \mu_x)^2 \sum_{i=1}^{n} (y_i - \mu_y)^2} \tag{4.6}$$

onde x_i e y_i são duas séries de dados, μ_x e μ_y representam as médias de cada série e n é o número de observações de cada série.

A interpretação do valor dos coeficientes de correlação (Pearson e cruzada) usada é a seguinte (Guilford et al., 1965):

- Valores menores do que $0,2$ - Correlação inexistente;
- Valores entre $0,2$ e $0,4$ - Correlação baixa;
- Valores entre $0,4$ e $0,7$ - Correlação moderada;
- Valores entre $0,7$ e $0,9$ - Correlação alta;
- Valores maiores do que $0,9$ - Correlação muito alta.

Além disso, os valores p serão usados para testar a hipótese nula H_0 de que não existe relação entre as duas variáveis. Valores p menores do que $0,05$ indicam um resultado significativo, e a hipótese nula de que não existe relacionamento entre as duas variáveis pode ser rejeitada, aceitando a hipótese alternativa.

Exemplos sobre como calcular e interpretar o grau de associação entre incidentes de segurança serão apresentados na próxima seção.

4.2.3 Exemplos

Na seção anterior, foi mostrado como avaliar os efeitos de três métricas: número de incidentes de segurança reportados por dia, número de incidentes de segurança por mês e o grau de associação entre diferentes tipos de incidentes. Foi utilizado o número absoluto de incidentes para ilustrar a aplicação de tais métricas. Nesta seção, serão fornecidos alguns exemplos com base no número de incidentes reportados por instituição. A intenção é investigar o comportamento das métricas em instituições com diversas características.

Devido as limitações impostas pela base de dados do CAIS, instituições com as seguintes características serão analisadas:

1. Instituições com um número semelhante de incidentes reportados e do mesmo estado;
2. Instituições com um número semelhante de incidentes reportados, mas de estados diferentes;
3. Instituições com um número diferente de incidentes reportados, mas do mesmo estado;
4. Instituições com um número diferente de incidentes reportados e de estados diferentes;

Essa configuração permite a análise do comportamento das métricas em diferentes circunstâncias, situações onde elas podem ser empregadas e também as limitações. Duas instituições para cada caso foram selecionadas.

Para encontrar duas instituições com um número semelhantes de incidentes, o seguinte método foi usado. O primeiro passo consiste em encontrar as instituições com os maiores números de incidentes reportados. A seguir, calcular a menor distância d entre os pontos P_a e P_b que correspondem ao número de incidentes reportados nas instituições A e B. As duas instituições com o maior número de incidentes e com a menor distância entre eles são, então, selecionadas.

O método para encontrar as instituições com número diferente de incidentes, consiste em encontrar duas instituições X e Y com número de incidentes reportados a e b tal que $a > b$ e a distância d_{ab} entre a e b respeite a seguinte condição $d_{ab} \geq \mu + 2\sigma$, onde μ é

Tabela 4.12: Instituições investigadas

Critério	Instituição 1	Número de incidentes(1)	Instituição 2	Número de incidentes (2)	Estado
1	A_1	23.315	A_2	21.039	RJ
2	B_1	15.587	B_2	15.575	PB e RJ
3	C_1	32.023	C_2	9.309	SC
4	D_1	29.403	D_2	19.067	DF e PR

o valor da média da amostra e σ representa o desvio padrão da amostra. As instituições com o maior número $a + b$ de incidentes são selecionadas. A desigualdade acima é usada com frequência para detectar observações atípicas (*outliers*) em conjunto de dados (Chrun et al., 2008a). A Tabela 4.12 mostra as instituições selecionadas para cada um dos critérios previamente definidos e os respectivos números de incidentes e estados.

A média do número de incidentes por instituição é de $\mu = 962,10$ e o desvio padrão dessa amostra é $\sigma = 3479,59$. Os incidentes das instituições selecionadas correspondem a $165.318/452.766 = 36,51\%$ do número total de incidentes presentes no conjunto de dados.

A Tabela 4.13 apresenta os resultados da análise do número de incidentes por dia. Para cada instituição, foram calculados os coeficientes de autocorrelação do número de incidentes reportados por dia e também os respectivos correlogramas. Nos casos em que uma tendência foi detectada, o teste de Laplace é utilizado para verificar o início e a duração de cada tendência.

A semelhança dos resultados entre as instituições A_1, A_2, B_1, C_1 e D_1 e B_2, C_2 e D_2 sugere que as organizações compartilham algumas características comuns relacionadas ao processo de reportar incidentes e também ao modo com que os ataques são direcionados a organização. Também é possível notar que apesar das diferentes características entre as instituições, em nenhuma delas o número de incidentes reportados por dia apresentou um comportamento completamente aleatório. Isso sugere que parte dos incidentes reportados pelo CAIS/RNP estão associados a um componente estacionário, seja a exibição de uma tendência ou sazonalidade. Esse resultado corrobora algumas conclusões encontradas em (Condon et al., 2008) e (Condon e Cukier, 2012), de que os incidentes de segurança reportados em uma organização podem, em determinados casos, ser modelados usando séries temporais não estacionárias, devido a fatores como o calendário acadêmico, o número de

Tabela 4.13: Resultados - número de incidentes por dia

Instituição	Tendência	Sazonalidade	Aleatória
A_1	-	A cada 7 dias	-
A_2	-	A cada 7 dias	-
B_1	-	A cada 7 dias	-
B_2	Diminuição a partir do dia 270	-	-
C_1	-	A cada 7 dias	-
C_2	Diminuição, à partir do dia 270	-	-
D_1	-	A cada 7 dias	-
D_2	Diminuição a partir do dia 347	-	-

máquinas ativas no campus e os períodos que envolvem o lançamento de atualizações de segurança. Porém, os autores afirmam que outros fatores, como características da população e tipos específicos de incidentes de segurança, também devem ser estudados a fim de obter modelos de previsão mais eficientes.

A Tabela 4.14 apresenta os resultados da análise do número de incidentes por mês. Para cada instituição, foi calculado o índice de sazonalidade mensal para o número total de incidentes reportados. A análise dos resultados revela que todas as instituições analisadas possuem uma expectativa de incidentes esperada para o mês de Dezembro menor do que a média global, pois os valores dos índices para esse mês em todas as instituições é menor do que 1. Analogamente, em todas as instituições, os meses de Março, Abril e Maio possuem índices maiores que 1, ou seja, existe uma tendência de aumento no número de incidentes reportados nesses meses. A Figura 4.21 ilustra a diferença entre os meses de Março, Abril, Maio e Dezembro. Esse tipo de resultado pode ser usado para a tomada de decisões práticas como aumentar a monitoração nos meses de Março, Abril e Maio e investigar se a diminuição dos incidentes reportados em Dezembro é relacionada a diminuição da população no campus ou outros fatores como a ausência de funcionários do grupo de respostas a incidentes de segurança.

A Tabela 4.15 apresenta o grau de associação entre os tipos de incidentes. Os incidentes Bot, Spam e Uso de recursos de forma indevida, foram escolhidos devido a incidência de cada um deles no conjunto de dados. O símbolo "-" indica que a correlação não pode ser

Tabela 4.14: Resultados - número de incidentes por mês

Instituição	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
A_1	1,11	0,88	1,11	1,38	1,43	0,85	0,88	1,04	1,03	1,06	0,79	0,43
A_2	1,01	0,95	1,19	1,38	1,42	0,93	0,89	0,87	0,95	1,02	0,84	0,55
B_1	0,70	0,89	1,26	1,36	1,33	1,07	1,10	1,03	0,95	0,96	0,77	0,59
B_2	0,99	0,89	1,11	1,20	1,33	0,91	1,05	0,90	0,86	0,99	1,07	0,70
C_1	0,75	0,78	1,26	1,59	1,56	1,36	1,17	1,23	0,78	0,57	0,56	0,39
C_2	0,28	1,35	1,78	2,09	1,76	0,88	1,39	1,39	0,54	0,31	0,18	0,06
D_1	1,24	0,91	1,06	1,22	1,28	1,07	0,97	0,87	0,97	1,03	0,88	0,50
D_2	0,44	0,72	1,27	1,63	1,75	1,47	1,19	0,90	0,71	0,80	0,81	0,32

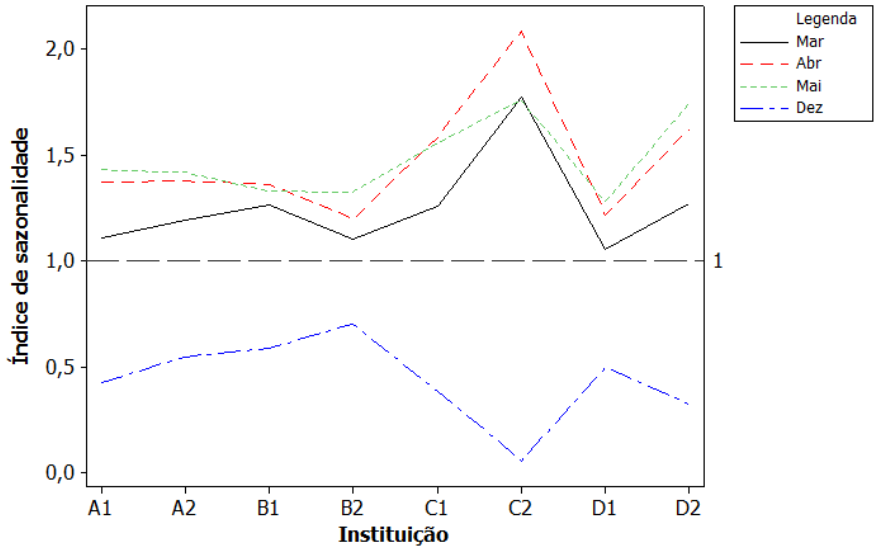


Figura 4.21: Índice de sazonalidade - Março, Abril, Maio e Dezembro

calculada pois um dos incidentes não foi reportado pela instituição. Já "*" denota um valor $p < 0,05$ para tal coeficiente.

Os resultados mostram que dentre as oito instituições, quatro delas A_1, A_2, B_2 e D_1 apresentaram um grau de associação de no mínimo $0,2$, caracterizando uma correlação baixa. Em todos os casos, a correlação aconteceu entre os incidentes Bot e Spam. Comportamento similar foi observado quando no cálculo dos coeficientes de correlação cruzada em cada uma das instituições. Correlações baixas, entre $0,2$ e $0,3$, foram encontradas somente entre os incidentes Bot e Spam nas instituições A_1, A_2, B_2 e D_1. Esse tipo de investigação pode auxiliar a compreender o modo com que os incidentes Bot são usados em cada organização.

Tabela 4.15: Resultados - grau de associação entre os tipos de incidentes

Instituição	Bot x Spam	Bot x Uso	Spam x Uso
A_1	0,226*	0,016	0,005
A_2	0,38*	-0,033	-0,013
B_1	0,127*	-	-
B_2	0,391*	-0,023	0,019
C_1	-0,024	-	-
C_2	-	-	-
D_1	0,369*	0,106*	-0,025
D_2	0,01	0,054	-0,004

Tabela 4.16: Grau de associação entre os incidentes Bot por instituição

	A_1	A_2	B_1	B_2	C_1	C_2	D_1
A_2	0,935*						
B_1	0,899*	0,9*					
B_2	0,788*	0,787*	0,732*				
C_1	0,808*	0,792*	0,863*	0,697*			
C_2	0,814*	0,786*	0,848*	0,673*	0,9*		
D_1	0,906*	0,914*	0,927*	0,714*	0,845*	0,795*	
D_2	0,752*	0,750*	0,833*	0,645*	0,7*	0,647*	0,767*

Computadores infectados com Bots frequentemente formam uma rede entre si, controlada por criminosos. Essas redes são chamadas de Botnets, e usadas com diversos propósitos, a maioria deles ligado a atividades maliciosas. Alguns usos incluem: ataques de Negação de Serviço, envio de Spam e Phishing, distribuição ilegal de conteúdo, roubo de informação pessoal entre outros (Karasaridis et al., 2007). Em nosso caso, os resultados mostram que dentre as oito instituições investigadas, em quatro delas o uso das Botnets pode ser ligado com a disseminação de Spam.

Uma possível aplicação desse resultado é o agrupamento de instituições com comportamentos semelhantes relacionados ao uso de Bot e assim identificar possíveis Botnets entre as organizações. Conforme discutido em (Cooke et al., 2005), tais redes podem ser altamente distribuídas, com nós em diversas redes e localizadas em várias cidades (ou até países) e a cooperação entre organizações é um passo importante para o desmantelamento das Botnets. Levando em consideração esse tópico, será verificado o grau de associação entre cada tipo de incidente nas instituições selecionadas. Esse estudo pode revelar similaridades entre os diferentes tipos de incidentes em cada uma das instituições.

As Tabelas 4.16 e 4.17 mostram os coeficientes de correlação para os incidentes Bot

Tabela 4.17: Grau de associação entre os incidentes Spam por instituição

	A_1	A_2	B_1	B_2	C_1	D_1
A_2	0,213*					
B_1	0,022	0,102*				
B_2	0,22*	0,447*	0,098*			
C_1	0,003	-0,013	0,057	0,015		
D_1	0,185*	0,328*	0,005	0,211*	-0,039	
D_2	0,056	0,026	0,031	0,099*	-0,003	0,018

e Spam, respectivamente. De acordo com a Tabela 4.16, a correlação entre os incidentes Bot em todas as oito instituições é significativa e na maioria dos casos alta. Isso indica uma semelhança no comportamento dos incidentes Bot reportados nas instituições, apesar de cada organização possuir equipes de segurança e políticas de tratamento e prevenção próprias. No caso dos incidentes Spam (Tabela 4.17), foi encontrado um comportamento completamente diferente nas instituições. Quais as possíveis explicações para que um tipo de incidente tenha comportamento similar em oito instituições diferentes?

Primeiramente, no caso dos incidentes Bot, é preciso levar em consideração a existência de vários tipos de softwares maliciosos que atuam como bots, como por exemplo, *conficker*, *downadup*, *sality*, *zeus*, entre outros. Essa distinção não foi feita ao longo da nossa análise. De acordo com (Bailey et al., 2009), cada tipo de Bot possui um meio de propagação, comunicação e ataque. Uma análise mais detalhada do problema exige o estudo da correlação entre os diferentes tipos de Bot.

Mesmo considerando o caso onde todos os incidentes do tipo Bot estão agrupados, é possível notar que tais ataques compartilham características semelhantes ao longo dos dois anos de estudo. A Figura 4.22 mostra o número de incidentes acumulados para cada uma das oito instituições. É possível notar que todas as instituições apresentaram aumento no número de incidentes Bot em 2011 e diminuição, ou estabilidade em 2012. Esse pode ser considerado um dos fatores que ocasionou a alta correlação entre as instituições. O próximo passo seria a investigação das razões que culminaram com esse mesmo comportamento nas instituições. A possibilidade de ataques coordenados direcionados às instituições, ou a presença de botnets comuns a essas instituições são dois exemplos de hipóteses que poderiam ser pesquisadas.

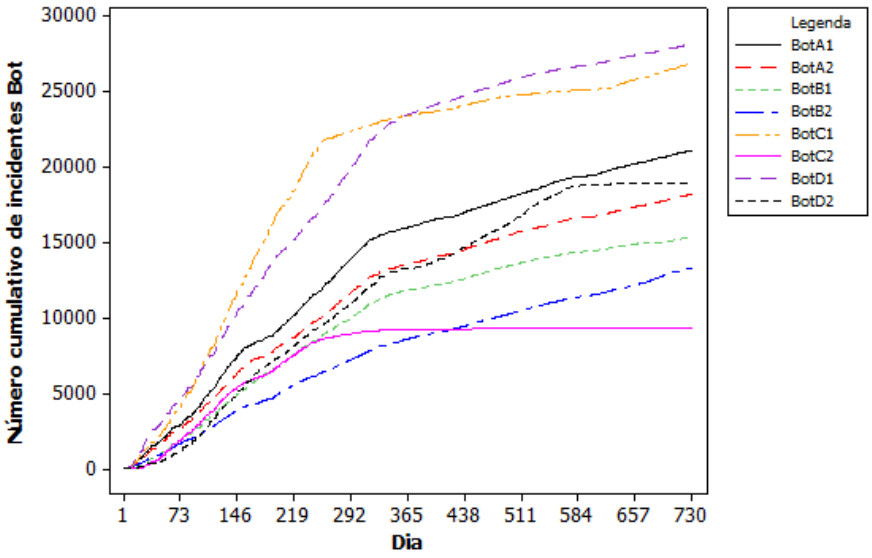


Figura 4.22: Número cumulativo de incidentes Bot por instituição

4.2.4 Resumo dos resultados

Os principais resultados encontrados na presente seção podem ser sumarizados da seguinte forma:

- A análise dos dados agregados referentes aos incidentes reportados por dia entre 2011 e 2012 exibiu um comportamento periódico, indicando a importância do componente não-estacionário nos incidentes de segurança reportados. A mesma análise, mas em diferentes instituições, confirmou esses resultados;

- A análise dos incidentes reportados por mês entre 2011 e 2012 indica uma tendência de aumento dos incidentes após os meses de Janeiro e Fevereiro. A mesma análise, mas em diferentes instituições, confirmou esses resultados e também mostrou que a expectativa de incidentes para o mês de Dezembro é menor do que a média global. Os resultados sugerem uma relação entre o calendário acadêmico e os incidentes de segurança;

- O grau de associação (Pearson e correlação cruzada) entre os tipos de incidente Bot, Spam e Uso de recursos de forma não autorizada não foi estatisticamente relevante

para o estudo, com exceção do coeficiente de Pearson para os incidentes Bot e Spam na metade das instituições analisadas (4 de 8);

- O comportamento dos incidentes Bot foi semelhante em todas as instituições analisadas, diferentemente dos incidentes do tipo Spam;

- Além do fator humano e das falhas presentes em softwares e hardwares, as características do ambiente também influenciam o maneira com que os ataques são executados.

4.3 Limitações

Algumas limitações devem ser mencionadas acerca dos dois conjuntos de dados analisados. Em ambos os conjuntos, foi disponibilizada somente a data em que o incidente foi registrado, ou seja, não é possível distinguir quando o incidente realmente ocorreu. Na maioria dos casos um incidente é notado somente após a execução de um conjunto de ações, assim, é difícil estimar com precisão a data real de ocorrência do incidente.

4.3.1 University of Maryland

Devido ao método utilizado pela universidade para validar os incidentes, é possível afirmar que todos os incidentes usados no trabalho são reais e que não existem falsos positivos entre os incidentes reportados. Porém, é impossível especificar o número de ataques não detectados e as intrusões que não se tornaram incidentes de segurança. O conjunto de dados é restrito aos incidentes detectados e reportados pela universidade.

Outra limitação é relacionada aos dados do IPS. O IPS investigado não foi avaliado e a quantidade de falsos positivos e falsos negativos que o mesmo produz não é conhecida. Um ataque bloqueado pelo IPS não necessariamente resultaria em um ataque com sucesso, ou ainda pode não ter sido uma real tentativa de ataque. Conforme mostrado em (Chrun et al., 2008a) e (Chrun et al., 2008b), as configurações presentes no IPS da University of Maryland são otimizadas para bloquear potenciais ataques em estágio inicial, mesmo que isso signifique bloquear tráfego válido.

4.3.2 CAIS/RNP

O CAIS é o grupo de segurança responsável pela RNP, e qualquer incidente envolvendo as instituições que se beneficiam dos serviços dessa rede pode ser notificado ao CAIS, que encaminhará corretamente o incidente. O processo de tratamento de incidentes do CAIS inicia-se de dois modos: i) recebimento de notificação sobre algum incidente de segurança ou ii) monitoração do incidente de segurança.

No primeiro caso, o CAIS somente grava o incidente notificado em sua base de dados. A validação do incidente cabe a instituição responsável pela notificação. Já no segundo caso, o CAIS detecta e valida o incidente, antes de gravar na base de dados e notificar a instituição responsável. Dessa forma, como os métodos empregados para a validação dos incidentes em cada uma das 422 instituições são desconhecidos, é impossível afirmar que todos os incidentes são reais. Além disso, não é possível determinar se um certo incidente presente na base de dados foi notificado pelo CAIS ou por uma das instituições filiadas.

4.4 Modelo para a identificação de métricas de segurança relevantes

As análises propostas mostraram caminhos possíveis acerca do uso e validação de métricas de segurança. O emprego de dados reais impõe novos desafios, porém abre espaço para diversas discussões sobre as aplicações das métricas. Além dos resultados obtidos, foi possível extrair com o auxílio de ambos estudos algumas atividades para auxiliar o processo de validação e comparação de métricas de segurança para outros casos.

1. Identificação do problema - A formulação do problema é o passo inicial. O objetivo do trabalho consiste em avaliar a qualidade/relevância das métricas de acordo com processos (ou parâmetros). Exemplo: avaliar a relevância entre métricas e incidentes de segurança;

2. Caracterização do processo - O processo ou parâmetro usado para avaliar a relevância da métrica deve ser definido de forma a permitir comparações. Exemplo: usar o número de incidentes de segurança reportados por semana;

3. Caracterização e definição das métricas - Após a identificação do problema e a caracterização do processo, os critérios de escolha das métricas devem ser estabelecidos, assim como os métodos empregados para o cálculo das mesmas. Exemplo: tentativas de ataques direcionadas à organização a partir de computadores fora do perímetro da rede;

4. Escolha e adequação dos dados - Consiste na decisão dos dados que irão alimentar as métricas e em alguns casos o processo de comparação. Exemplo: a base de dados de incidentes de segurança da University of Maryland será utilizada para prover o número de incidentes de segurança por semana e a base de dados de IPS será usada para fornecer os dados das métricas;

5. Definição da metodologia usada para avaliar a relação entre a métrica e o processo - Estabelece o método usado para avaliar as métricas, assim como possíveis limitações. Exemplo: aplicação de modelos de regressão linear;

6. Elaboração de critérios para análise da relevância das métricas - Os critérios de avaliação, geralmente, possuem relação direta com a metodologia definida. Exemplo: teste de hipótese nula, usando $p < 0.05$;

7. Investigação do impacto das métricas para a segurança da organização - Correspondem as situações práticas em que as métricas analisadas são usadas para auxiliar a compreensão de problemas e tomada de decisão. Exemplo: construção de indicadores de incidentes e avaliação da eficiência do sistema de prevenção de intrusão.

8. Possível aplicação de medidas corretivas (ou criação de políticas) baseada no resultado das métricas - Inclui a criação de regras para prevenção de ataques, alocamento de recursos, atualização de equipamentos, entre outros.

A Figura 4.23 ilustra a visão geral do fluxo entre cada uma das atividades propostas. O primeiro critério de decisão trata da relação entre os dados escolhidos e as métricas. Em determinados casos, os dados não são suficientes para a construção das métricas propostas. Nesse caso, novos dados podem ser incorporados ao processo, até que a base de dados contemple os casos escolhidos. Em alguns casos, uma simplificação, ou alteração

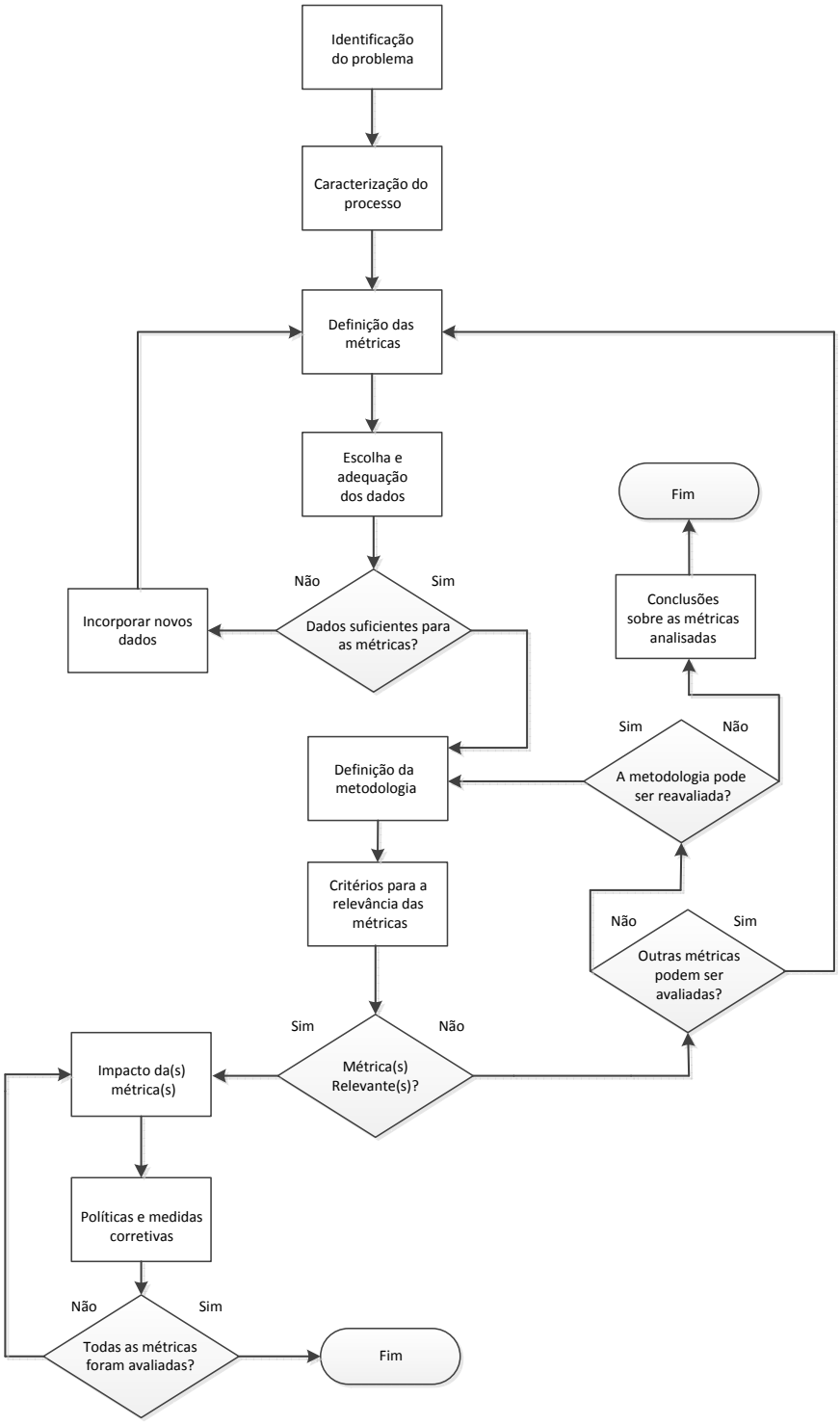


Figura 4.23: Visão geral do processo de identificação de métricas relevantes

nas métricas iniciais também pode ser feita. Um exemplo ocorreu ao formular o seguinte problema envolvendo a base do CAIS: “Avaliação do impacto de características organizacionais da instituição na ocorrência de incidentes”. A ideia seria avaliar fatores como o tamanho, tipo da instituição e reputação. Porém, os dados referentes às instituições foram sanitizados e a única característica disponível foi o estado de origem.

Outro critério de decisão é a análise das métricas relevantes. Se com os métodos empregados não foi possível obter informação sobre a relevância das métricas, outras métricas podem ser testadas, assim como outras metodologias (que inclui a adequação da metodologia as características dos dados ou a adoção de uma nova técnica, por exemplo). Em caso negativo, é importante traçar conclusões acerca da importância desse resultado para a segurança da informação.

O modelo proposto permite o desenvolvimento de novos estudos com base um alicerce já conhecido contribuindo principalmente para a construção de experimentos similares. Suponha que a University of Maryland (ou outra instituição) queira avaliar a relação entre as vulnerabilidades de segurança encontradas nos servidores do campus e determinados tipos de incidentes, com o intuito de melhorar a política de atualizações de segurança da universidade. A similaridade desse estudo hipotético com a pesquisa desenvolvida neste trabalho (análise de fatores que influenciam a segurança) norteia a construção do novo estudo, pois, o ciclo principal já foi devidamente mapeado. A repetição de experimentos usando diferentes fontes de dados é um outro exemplo de pesquisa que pode se beneficiar do mapeamento das atividades de validação e comparação de métricas de segurança. A ausência de investigações desse tipo foi citada por Verendel (2009) como uma das razões da estagnação da área de quantificação de segurança.

Capítulo 5

Questionário para a Avaliação do Uso de Métricas

Pesquisas de avaliação, também conhecidas como *surveys*, são usadas para coletar informações através de questionários enviados a um determinado número de pessoas. A pesquisa proposta neste trabalho é um passo inicial para compreender como as diferentes métricas propostas na literatura são aplicadas no cotidiano das empresas e qual é a visão desses profissionais sobre os problemas que exigem os maiores cuidados. Em particular, a intenção do questionário é obter opiniões de especialistas sobre os seguintes itens: 1) quais métricas são usadas para avaliação da segurança, 2) qual o grau de importância das métricas e 3) qual é o nível de complexidade das métricas.

Este capítulo mostra a metodologia usada para o desenvolvimento do questionário, assim como detalhes sobre a aplicação da pesquisa para o público. Os resultados obtidos, assim como as discussões sobre o impacto da pesquisa para comunidade científica também são apresentados.

5.1 Metodologia

Durante a criação do questionário, as seguintes discussões foram propostas:

1. Qual meio de divulgação deve ser usado?

2. Quantas questões devem ser incluídas?

3. Que tipos de questões devem ser usadas: dissertativa, múltipla escolha, escala de avaliação?

4. Além das opiniões, características demográficas e biográficas também farão parte da pesquisa?

Como o público alvo da pesquisa é a comunidade de TIC/Segurança, foi utilizado um questionário anônimo e online. Este tipo de abordagem já foi usada em várias pesquisas sobre segurança e os resultados foram considerados satisfatórios (Kajava e Savola, 2005), (Chrun, 2011), (Sademies, 2004), (Baker e Wallace, 2007) e (Bayuk, 2011). Outra opção seria selecionar um grupo de participantes e conduzir entrevistas. Essa hipótese foi descartada devido a dificuldade em organizar e conduzir entrevistas com profissionais da área de segurança da informação. Além disso, as entrevistas geralmente exigem um tempo maior de todos os envolvidos no processo.

Outro problema que envolve a elaboração de questionários é o número de perguntas. Questionários com muitas perguntas ou perguntas complexas podem desestimular os participantes. Profissionais de TIC e segurança possuem, na maioria das vezes, muitas tarefas para se preocupar e um questionário longo e complexo poderia não atraí-los de maneira satisfatória. Assim, optou-se pela adoção de um formato simples e que estimulasse respostas rápidas, em que o participante demore por volta de 15 - 20 minutos para responder toda a pesquisa. Porém, como o objetivo da pesquisa é coletar informações sobre métricas usadas para avaliação da segurança, a criação de uma lista de métricas para avaliação foi inevitável.

Baseado no questionário proposto por (Bayuk, 2011), optou-se por fornecer uma lista de métricas para ser selecionada e também avaliada pelo participante (múltipla escolha e escala de avaliação). Também foi inserida, no final do questionário, uma questão subjetiva para o participante fornecer possíveis métricas não presentes na lista original. Cinco grupos foram criados a fim de facilitar a seleção das métricas presentes no questionário. Cada um dos grupos está relacionado ao objetivo comum em todas as organizações: evitar ataques e proteger a informação. Os grupos são:

- Ameaças: trata dos diferentes tipos de ataques que a organização enfrenta;

- Vulnerabilidades de segurança: explorar as vulnerabilidades em sistemas é um dos métodos de ataque usados com muita frequência. Além disso, conforme mencionado no capítulo 2, as vulnerabilidades de segurança representam um importante ponto de acesso para potenciais ameças. Como nem sempre uma vulnerabilidade significa um ataque concreto, uma classificação individual para esse grupo foi criada.

- Como a organização lida com os ataques: a maneira com que os ataques são tratados e prevenidos;

- Alvos dos ataques: representa os possíveis alvos direcionados pelos atacantes;

- Detecção de ataques: trata dos métodos de detecção usados para encontrar ataques;

Os grupos foram baseados na classificação proposta por Geer e Pareek (2012), em que foram mapeadas seis importantes características usadas para avaliar o nível de segurança da informação em uma organização. O trabalho, porém, não investiga como essas características são medidas, ou ainda a complexidade que envolve cada uma delas.

Após discussões com profissionais da área e da análise de diversos trabalhos (The Center for Internet Security, 2010), (Chew et al., 2008), (Jaquith, 2007), (Herrmann, 2007), (Torres et al., 2006) e (Boyer e McQueen, 2008), 30 métricas foram incluídas no questionário. Outras métricas poderiam fazer parte dessa lista, porém, foram escolhidas métricas já existentes na literatura e que estritamente relacionadas aos grupos definidos. Além disso, a presença de muitas métricas na pesquisa poderia aumentar o tempo de preenchimento do questionário e consequentemente diminuir o interesse dos participantes. A Tabela 5.1 apresenta as métricas e os respectivos grupos.

Além da avaliação das métricas, foram incluídas algumas questões para ajudar a caracterizar a demografia dos participantes. Esse tipo de questão é importante nessa categoria de pesquisa pois auxilia a interpretação dos resultados. Por exemplo, a experiência do participante em segurança da informação pode ser um fator que influencia a escolha de certas métricas. Dessa forma, foram definidas um total de dez questões, de acordo com a disposição apresentada na Tabela 5.2. O Apêndice C apresenta o questionário completo.

A pesquisa foi criada com o auxílio do *SurveyMonkey*, uma ferramenta online que oferece uma infraestrutura completa para a criação e publicação de questionários. Porém,

Tabela 5.1: Métricas avaliadas na pesquisa

Métrica	Grupo
Número de ataques relacionados à Botnets	Ameaças
Número de ataques relacionados à Malwares	Ameaças
Número de ataques relacionados à Negação de Serviço	Ameaças
Número de ataques relacionados à Phishing	Ameaças
Número de ataques relacionados à Engenharia Social	Ameaças
Número de ataques relacionados a Spam	Ameaças
Número de ataques relacionados à exploração de vulnerabilidades de segurança	Ameaças
Número de ataques relacionados à estrutura física da organização	Ameaças
Número de vulnerabilidades de segurança encontradas em servidores Web	Vulnerabilidades de segurança
Número de vulnerabilidades de segurança encontradas em equipamentos de rede	Vulnerabilidades de segurança
Número de vulnerabilidades de segurança encontradas em dispositivos móveis	Vulnerabilidades de segurança
Número de vulnerabilidades de segurança encontradas em dispositivos na Nuvem	Vulnerabilidades de segurança
Número de vulnerabilidades de segurança encontradas em estações de trabalho	Vulnerabilidades de segurança
Tempo médio para encontrar um incidente	Como a organização lida com os ataques
Tempo médio entre incidentes	Como a organização lida com os ataques
Tempo médio para se recuperar de um incidente	Como a organização lida com os ataques
Custo médio por incidente	Como a organização lida com os ataques
Número de atualizações de segurança aplicadas por período	Como a organização lida com os ataques
Número de atualizações de segurança não aplicadas por período	Como a organização lida com os ataques
Número de ataques direcionados a servidores Web	Alvos dos ataques
Número de ataques direcionados a equipamentos de rede	Alvos dos ataques
Número de ataques direcionados a dispositivos móveis	Alvos dos ataques
Número de ataques direcionados a dispositivos na Nuvem	Alvos dos ataques
Número de ataques direcionados a estações de trabalho	Alvos dos ataques
Porcentagem de tentativas de intrusão bloqueadas	Detecção de ataques
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	Detecção de ataques
Porcentagem de funcionários de TIC com dedicação exclusiva à segurança da informação	Detecção de ataques
Número de incidentes de segurança internos reportados/detectados	Detecção de ataques
Número de incidentes de segurança externos reportados/detectados	Detecção de ataques
Número de incidentes críticos reportados/detectados	Detecção de ataques

Tabela 5.2: Questões presentes na pesquisa

Ordem	Questão	Tipo
1	Selecione a área de atuação da organização em que trabalha	Múltipla escolha
2	Selecione a atividade desempenhada na organização	Múltipla escolha
3	Selecione uma das opções que melhor caracteriza o tamanho da organização em que você trabalha	Múltipla escolha
4	Selecione uma das opções com relação ao número de computadores presentes na organização em que você trabalha	Múltipla escolha
5	Digite o número de anos com relação à sua experiência na área de segurança da informação	Dissertativa (Caixa de texto numérica)
6	Digite o número de anos em que está trabalhando na organização	Dissertativa (Caixa de texto numérica)
7	Quais das métricas abaixo você atualmente utiliza para auxiliar a compreender o nível de segurança da informação de sua organização?	Múltipla escolha (várias respostas)
8	Em uma escala de 1 a 5 (com 5 para mais importante), analise as métricas de acordo com a sua importância em avaliar o nível de segurança da informação da organização	Escala de avaliação
9	Em uma escala de 1 a 5 (com 5 para mais complexo), avalie as métricas de acordo com a complexidade de sua utilização	Escala de avaliação
10	Cite outras métricas que podem ser utilizados para avaliar o nível de segurança da informação de uma organização	Dissertativa (Caixa de texto)

antes de disponibilizar a pesquisa para o público, foram feitos alguns testes na versão inicial do questionário, com a ajuda de dois profissionais da área de TIC/Segurança. Após alguns ajustes (erros ortográficos e de digitação e sugestões nas perguntas demográficas), a pesquisa foi publicada no seguinte endereço: *http://www.surveymonkey.com/s/LT2XR2M*, durante 1 mês (entre 23/01/2013 à 23/02/2013).

Com o intuito de atingir um número representativo de respostas da comunidade de segurança, a pesquisa foi compartilhada nas seguintes listas de e-mail: administradores de rede da Unicamp, funcionários do CAIS/RNP, Sociedade Brasileira de Computação (SBC), Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CESeg), analistas do CERT.br e grupos de segurança e resposta a incidentes brasileiros.

É importante observar que, em uma pesquisa do tipo censo, o objetivo não é enumerar uma população inteira a partir de uma amostra, mas sim, fornecer um estudo inicial sobre o uso, importância e complexidade de diferentes métricas de segurança em ambientes reais.

5.2 Resultados

Conforme discutido em Kotulic e Clark (2004), pesquisas que envolvem investigações sobre segurança da informação costumam ter baixas taxas de resposta. As principais razões citadas pelos participantes inclui: a política da empresa não permite a participação em pesquisas, informações sobre a segurança da organização não podem ser compartilhadas e o cronograma da equipe não permite a alocação de novas tarefas, como responder pesquisas.

As taxas de resposta de algumas pesquisas sobre segurança presentes na Tabela 5.3, ilustram esse cenário. Um total de 47 respostas foram obtidas ao longo do período em que a presente pesquisa foi disponibilizada. Porém, devido ao método escolhido para disseminar o questionário, não é possível estimar com precisão uma taxa de resposta.

As Figuras 5.1, 5.2, 5.3 e 5.4, apresentam os resultados das primeiras quatro perguntas, usadas para analisar o perfil dos participantes. Os resultados completos de cada uma das dez perguntas, encontram-se no Apêndice D.

De acordo com as respostas, a maioria dos participantes (mais de 65%) trabalham em empresas de TIC ou do ramo da educação (universidades e centros de pesquisa) e grande parte ocupam posições estritamente ligadas a resolução de problemas em segurança da

Tabela 5.3: Taxas de respostas de pesquisas sobre segurança

Número de participantes	População	Taxa de resposta	Referência
15	600	0,025	Chrun (2011)
23	250	0,092	Machado et al. (2009)
23	1474	0,015	Kotulic e Clark (2004)
40	170	0,235	Torres et al. (2009)

informação (mais de 68% são gerentes de TIC ou analistas de TIC, suporte ou segurança).

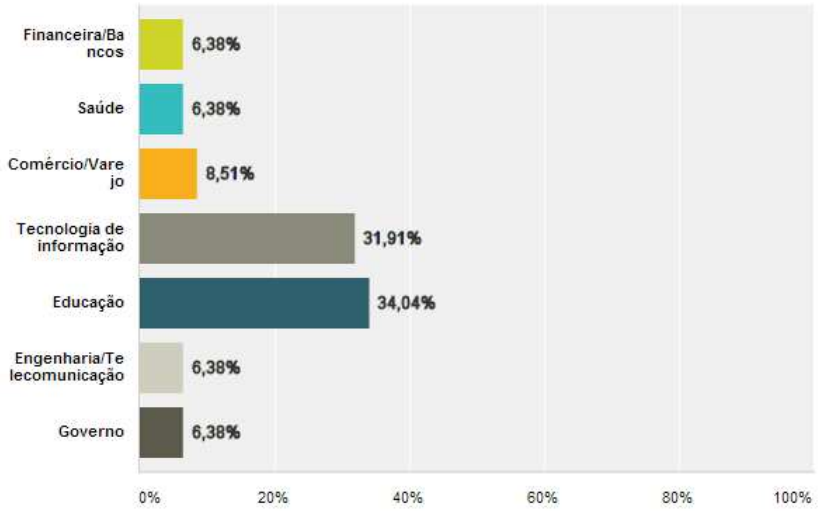


Figura 5.1: Respostas - Questão 1

As respostas das perguntas 5 e 6, indicam que os participantes possuem, em média, 7 anos de experiência em segurança da informação, e 6,5 anos trabalhando na mesma organização. A Tabela 5.4 apresenta um resumo sobre o conteúdo das respostas em cada uma dessas questões. Importante notar que alguns participantes não responderam a essas perguntas. Dentre os 47, três não responderam a questão 5 e dois não responderam a questão 6.

Apesar das respostas sobre experiência em segurança variarem entre 0 e 24 anos, as Figuras 5.5 e 5.6, mostram que praticamente metade dos participantes que responderam a essa pergunta ($23/44 = 52\%$) possuem entre 2 a 10 anos de experiência e onze participantes afirmaram ter mais de 10 anos de experiência em segurança da informação.

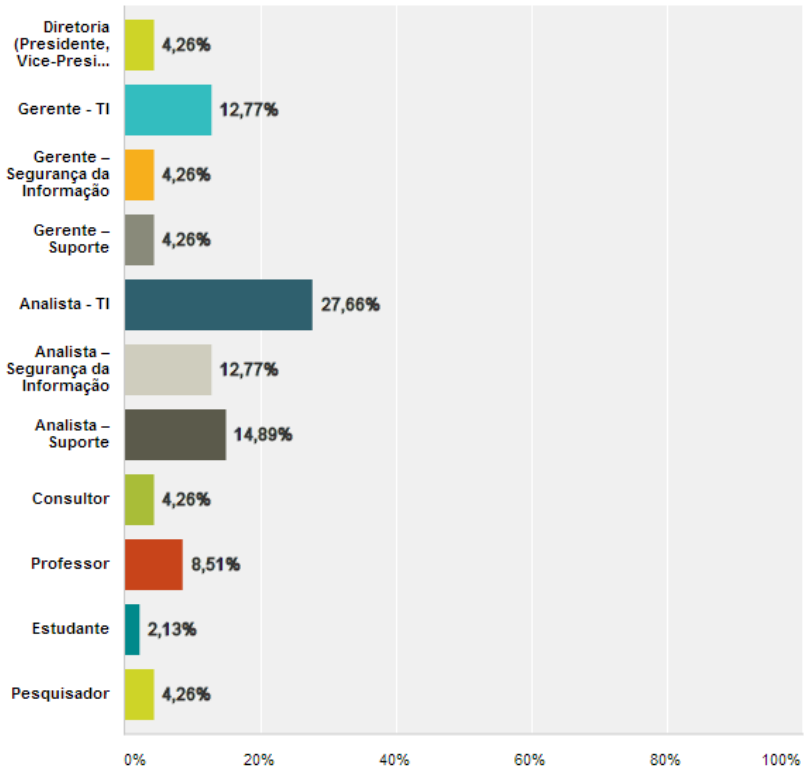


Figura 5.2: Respostas - Questão 2

As Tabelas 5.5 e 5.6 apresentam os principais resultados das métricas usadas na organização, da importância das métricas e da complexidade. O principal objetivo das tabelas é apresentar os cinco primeiros e os cinco últimos resultados em cada uma das três questões (Q7, Q8 e Q9). O campo Resultado (Q7) mostra o número de participantes que escolheram tal métrica e a respectiva porcentagem. Os campos Resultado (Q8) e Resultado (Q9) representam as avaliações médias (relativa a escala de avaliação entre 1 a 5) obtidas para a importância e complexidade das métricas.

A Tabela 5.5 demonstra que duas das métricas que estão entre as mais utilizadas,

Tabela 5.4: Estatística descritiva das respostas - Questões 5 e 6

Questão	Média	Desvio padrão	Mínimo	Q1	Mediana	Q3	Máximo
5)	7,091	6,313	0,000	2,000	6,500	10,750	24,000
6)	6,467	5,715	1,000	2,000	5,000	9,500	26,000

Tabela 5.5: Questões 7, 8 e 9 - Cinco primeiros resultados

Métricas utilizadas (Q7)	Métricas importantes (Q8)	Complexidade das métricas (Q9)	Resultado (Q7)	Resultado (Q8)	Resultado (Q9)
Número de ataques relacionados a Spam	Número de vulnerabilidades de segurança em servidores	Número de ataques a recursos que estão na Nuvem	23 (48,94%)	3,87	3,55
Número de ataques relacionados a Negação de Serviço	Número de ataques direcionados a servidores	Custo médio por incidente	21 (44,68%)	3,83	3,43
Número de incidentes de segurança internos	Número de incidentes críticos	Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	21 (44,68%)	3,79	3,38
Número de vulnerabilidades de segurança em servidores	Número de incidentes de segurança internos	Tempo médio para encontrar um incidente	20 (42,55%)	3,79	3,36
Número de incidentes de segurança externos	Número de ataques relacionados a exploração de vulnerabilidades de segurança	Tempo médio para se recuperar de um incidente	19 (40,43%)	3,74	3,34

Tabela 5.6: Questões 7, 8 e 9 - Cinco últimos resultados

Métricas utilizadas (Q7)	Métricas importantes (Q8)	Complexidade das métricas (Q9)	Resultado (Q7)	Resultado (Q8)	Resultado (Q9)
Número de vulnerabilidades de segurança em recursos que estão na Nuvem	Número de ataques direcionados a dispositivos móveis	Porcentagem de funcionários de TIC com dedicação exclusiva à segurança da informação	4 (8,51%)	2,83	2,38
Custo médio por incidente	Número de atualizações de segurança não aplicadas por período	Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	5 (10,64%)	2,85	2,49
Número de correções (patches) não aplicadas por período	Número de ataques a recursos que estão na Nuvem	Número de ataques relacionados a Spam	5 (10,64%)	2,85	2,77
Número de ataques direcionados a dispositivos móveis	Número de atualizações de segurança aplicadas por período	Porcentagem de tentativas de intrusão bloqueadas	5 (10,64%)	2,87	2,83
Número de ataques a recursos que estão na Nuvem	Número de vulnerabilidades de segurança em recursos que estão na Nuvem	Número de ataques relacionados a Phishing	5 (10,64%)	2,89	2,87

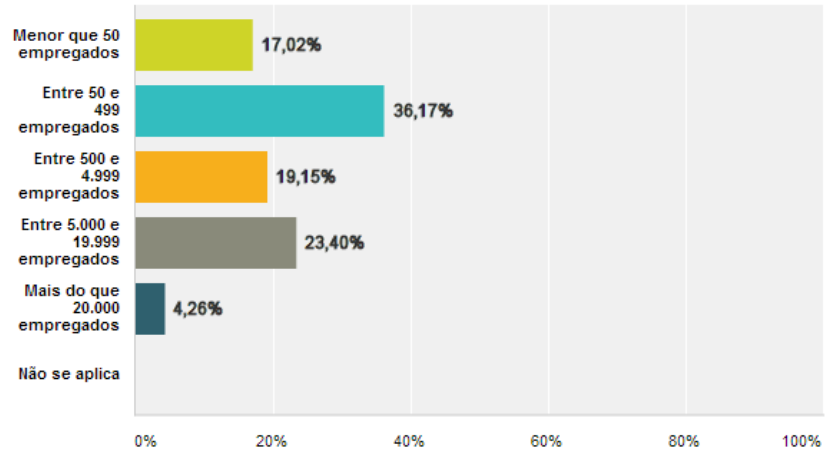


Figura 5.3: Respostas - Questão 3

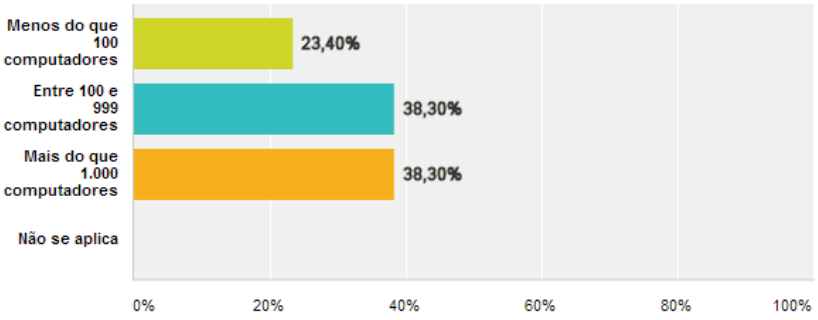


Figura 5.4: Respostas - Questão 4

também figuraram como as mais importantes: número de incidentes de segurança internos e o número de vulnerabilidades de segurança em servidores. O número de incidentes de segurança internos, em especial, chama a atenção. Esse tipo de ataque pode causar muitos problemas à organização e além disso é, geralmente, mais difícil de detectar do que os ataques externos. Porém, estudos como (Richardson, 2011) e (Verizon, 2012), apontam uma queda no número dos ataques internos. Algumas das razões apontadas incluem o aumento de ataques externos que podem ser lançados em grande número de alvos, como os crimes digitais e os ataques movidos por ideais e questões políticas (*hacktivism*), além do aumento dos controles contra os ataques internos. A pesquisa mostra que apesar da tendência de diminuição, os ataques internos ainda preocupam os profissionais de segurança.

Outro resultado encontrado na Tabela 5.5, indica que nenhuma das cinco métricas consideradas como as mais complexas, apareceram entre as mais importantes ou mais utiliza-

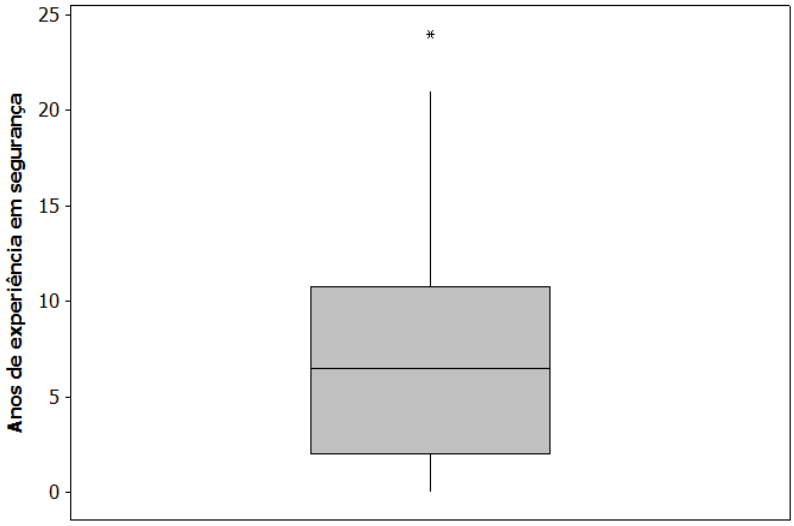


Figura 5.5: Experiência dos participantes em segurança da informação - Box plot

das. Isso sugere que as métricas complexas não são necessariamente as mais importantes, e também que a utilização da métrica pode estar relacionada com a sua complexidade. O custo médio de um incidente, por exemplo, mede o custo dos incidentes reportados e pode ser considerado difícil de estimar, pois exige diversos tipos de informação que em muitos casos a organização não possui, como o tempo e o dinheiro gasto para se recuperar de um incidente (The Center for Internet Security, 2010). De fato, tal métrica foi considerada como a segunda mais complexa entre todas as investigadas, contudo, não figurou entre as mais importantes.

A Tabela 5.6 mostra que três das métricas que estão entre as menos utilizadas também figuraram como as de menor importância para os participantes: número de ataques a dispositivos móveis, número de ataques a recursos que estão na nuvem e número de vulnerabilidades de segurança em recursos da nuvem. Isso indica uma preocupação menor com a segurança dos dispositivos móveis e os recursos alocados na nuvem. Esses dois tipos de recursos são razoavelmente novos do ponto de vista tecnológico, ou seja, a frequência de ataques em tais recursos pode ainda não ser a suficiente para chamar a atenção dos profissionais de segurança. Ou ainda, os recursos de segurança existentes não dão o suporte necessário para tais áreas, dificultando a detecção e tratamento desses ataques. A segurança da computação em nuvem é um tópico de pesquisa atual e com diversos pro-

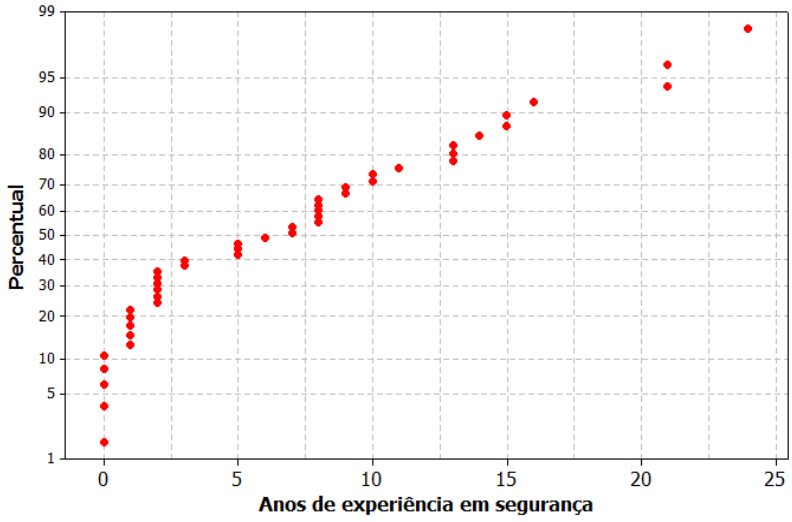


Figura 5.6: Experiência dos participantes em segurança da informação - Frequências

blemas em aberto (Kaufman, 2009), (Jensen et al., 2009), assim como como o aumento da tendência de funcionários levarem os próprios dispositivos móveis (*smartphones*, *tablets* e *laptops*) para os domínios da empresa. Esse paradigma é conhecido como BYOD (*Bring Your Own Device*) e pesquisas recentes revelam as dificuldades enfrentadas pelos profissionais de segurança com essa nova situação (Thomson, 2012).

Por fim, com relação a última questão do questionário, somente cinco participantes responderam tal pergunta. O baixo número de respostas pode ter ocorrido devido a dois fatores: a última pergunta do questionário e exigência dos participantes a uma resposta escrita. Cada uma das respostas é citada a seguir:

1. Percentual de funcionários treinados sobre segurança da informação;

2. Nível de conhecimento dos usuários sobre segurança da informação;

3. Número de senhas de usuários “quebradas” utilizando ferramentas automatizadas;

4. Existência de políticas de segurança efetivas, equipes de segurança dedicadas e com poder de ação;

5. Estrutura organizacional precária.

As duas primeiras métricas tratam do elemento humano dentro da organização. Políticas de uso, conjuntos de boas práticas, treinamentos e seminários sobre segurança da informação são alguns exemplos de fontes de dados para tais métricas. Outra métrica relevante citada pelos participantes foi o número de senhas de usuários reveladas utilizando ferramentas automatizadas. Também conhecidos como força-bruta, esses métodos representam um dos vetores de início de ataque (Verizon, 2012), (Richardson, 2011) e também pode revelar o uso de senhas pouco seguras.

5.3 Análise e discussão

As seguintes análises foram propostas com o intuito de melhorar a compreensão dos resultados obtidos:

- Estudo dos resultados a partir da classificação proposta das métricas;
- Investigar a relação entre o tipo de empresa e a utilização, importância e complexidade das métricas;
- Investigar a relação entre a experiência em segurança e a utilização, importância e complexidade das métricas;

5.3.1 Resultados agrupados

Será analisado se as respostas variam de acordo com a classificação das métricas em um dos 5 grupos definidos anteriormente: ameaças, vulnerabilidades de segurança, como a organização lida com os ataques, alvos dos ataques e detecção dos ataques. Para isso, será utilizada uma técnica conhecida como análise de variância ou ANOVA.

De forma simplificada, a análise de variância refere-se a procedimentos estatísticos para a análise de respostas quantitativas de unidades experimentais (Devore, 2012). Um problema ANOVA unidirecional ou de fator único, envolve a análise dos dados obtidos de amostras de mais de duas distribuições ou populações. A característica que diferencia as distribuições entre si é chamado de fator em estudo, e as populações diferentes são chamadas níveis do fator.

A ANOVA de fator único concentra-se na comparação de mais de duas médias populacionais ou de tratamento. Seja:

I = o número de populações que estão sendo comparadas,
μ_1 = a média populacional 1
$\vdots$
μ_I = a média populacional I.

Então, as hipóteses de interesse são:

$H_0 : \mu_1 = \mu_2 = \ldots = \mu_I$
H_a : pelo menos dois μ_i são diferentes.

Para testar essas hipóteses, é necessário ter uma amostra aleatória de cada população e analisar o respectivo valor p. Se H_0 for verdadeira, não há evidência de diferença significativa entre as populações. Caso contrário, se H_a for verdadeira, existem evidências de diferença significativa entre pelo menos duas médias da população estudada.

A Tabela 5.7 apresenta os resultados da ANOVA para cada um dos grupos de métricas e também para cada questão (7, 8 e 9). São apresentados os valores da média (μ) e do desvio padrão (σ), além do grau de significância usado para testar a hipótese nula H_0.

De acordo com os valores p, é possível aceitar a hipótese nula para a questão que trata das métricas utilizadas (Q7). Isso mostra que não existe diferença significativa entre os cinco grupos com relação as métricas escolhidas pelos participantes. O mesmo aconteceu com a questão sobre a importância das métricas (Q8). A hipótese H_0 verdadeira para as duas questões (Q7 e Q8) sugere uma semelhança entre esses dois conjuntos. A seguir, a relação entre as métricas escolhidas pelos participantes e a importância dada a elas será analisada.

Essa possível relação ressalta o caso em que, se a métrica é utilizada para um determinado objetivo, então ela é importante. O conceito de importância pode ser considerado subjetivo, mas deve envolver, necessariamente a validação da métrica para a comprovação de tal fato. Em nosso caso, o coeficiente de correlação de Pearson entre as 47 respostas de

Tabela 5.7: Tabela ANOVA - Influência dos grupos

Tipo da métrica	Métricas utilizadas (Q7)	Importância da métricas (Q8)	Complexidade das métricas (Q9)
Alvos de ataques	$\mu = 9,6$ $\sigma = 5,5$	$\mu = 3,246$ $\sigma = 0,4176$	$\mu = 3,28$ $\sigma = 0,216$
Ameaças	$\mu = 15,625$ $\sigma = 5,069$	$\mu = 3,3287$ $\sigma = 0,2578$	$\mu = 3,0725$ $\sigma = 0,211$
Como a organização lida com os ataques	$\mu = 8,167$ $\sigma = 3,061$	$\mu = 3,1833$ $\sigma = 0,3077$	$\mu = 3,195$ $\sigma = 0,2244$
Detecção de ataques	$\mu = 14,333$ $\sigma = 5,046$	$\mu = 3,435$ $\sigma = 0,323$	$\mu = 2,8433$ $\sigma = 0,344$
Vulnerabilidades de segurança	$\mu = 11,6$ $\sigma = 5,941$	$\mu = 3,318$ $\sigma = 0,3893$	$\mu = 3,206$ $\sigma = 0,0918$
Valor p	0,062	0,749	0,035

cada uma das questões 7 e 8 (vide Apêndice D) foi de $0,707$, com um valor $p < 0,01$, o que representa uma correlação alta de acordo com a interpretação de Guilford citada no capítulo 4. Portanto, as respostas obtidas indicam que métricas mais utilizadas tendem a ser consideradas também mais importantes.

A compreensão dos métodos usados para considerar uma métrica importante poderia trazer novas informações acerca dos critérios empregados para a seleção de métricas de segurança. Jaquith (2007) cita que nem sempre os objetivos de segurança da organização são usados como critérios para o uso de determinadas métricas. A disponibilidade de dados é um dos diversos fatores que podem motivar a escolha de métricas, mesmo que tais métricas não sejam relevantes para a organização.

Com relação a outra questão, complexidade das métricas (Q9), como o valor $p < 0,05$, a hipótese nula de que a complexidade média entre os cinco grupos de métrica é a mesma é rejeitada e a hipótese alternativa H_a, em que pelo menos duas médias são diferentes, é aceita. De acordo com o método de Tukey (Devore, 2012), usado para avaliar quais populações diferem entre si, foram encontrados dois grupos distintos de médias: i) grupo A formado por Alvos dos ataques, Vulnerabilidades de segurança, Como a organização lida com os ataques e Ameaças e ii) grupo B formado por Vulnerabilidades de segurança, Como a organização lida com os ataques, Ameaças e Detecção de ataques.

O teste de Tukey afirma que populações no mesmo grupo não são significativamente

diferentes. Nesse caso, é possível notar que somente as métricas dos grupos Alvos de Ataque e Detecção de ataques diferem entre si, e, de acordo com os resultados das médias, as métricas do grupo detecção de ataque foram classificadas como mais simples do que as métricas relacionadas aos alvos de ataque.

Os resultados das métricas: número de ataques a recursos que estão na nuvem (3,55), número de ataques direcionados a equipamentos de rede como switches (3,38), roteadores e access points e número de ataques direcionados a dispositivos móveis (3,32) para o grupo Alvos de Ataque e porcentagem de tentativas de intrusão bloqueadas (2,83), porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários (2,49) e porcentagem de funcionários de TIC com dedicação exclusiva à segurança da informação para o grupo Detecção de ataques (2,38) são exemplos da diferença entre os grupos.

A análise dos grupos apontou uma diferença relevante somente na avaliação da complexidade das métricas. Esse resultado, indica uma certa homogeneidade (com relação aos grupos) nas respostas das questões sobre utilização das métricas e importância das métricas. O consenso encontrado na análise global dos resultados pode não ser necessariamente verdade se as amostras específicas da população forem analisadas. A seguir serão investigadas as diferenças entre tipos de empresa e a experiência em segurança da informação.

5.3.2 Relação entre o tipo de empresa e as métricas

Conforme discutido no capítulo 2, os objetivos de segurança podem variar de acordo com o tipo da organização. Consequentemente, a visão sobre as métricas de segurança também podem variar segundo esse princípio. Nesta seção, essa hipótese será investigada, em especial as diferenças entre os dois tipos de empresa com o maior número de ocorrências na pesquisa: TIC (15) e Educação (16).

Primeiramente, será encontrado o coeficiente de correlação entre as respostas dadas pelos dois grupos. Se as respostas não apresentarem qualquer tipo de correlação, as diferenças entre os dois grupos definidos de profissionais se tornam mais aparentes. Caso contrário, os conjuntos podem apresentar semelhanças entre si, e outras análises devem

Tabela 5.8: Tipos de empresa - Correlação entre as perguntas

	Questão 7	Questão 8	Questão 9
Correlação	0,63	0,528	0,302
Valor p	0,000	0,003	0,105

Tabela 5.9: Tabela ANOVA - Influência do tipo de empresa

Tipo da métrica	Métricas utilizadas (Q7)	Importância da métricas (Q8)	Complexidade das métricas (Q9)
Educação	$\mu = 4,733$ $\sigma = 2,49$	$\mu = 3,2653$ $\sigma = 0,4327$	$\mu = 3,2473$ $\sigma = 0,3114$
TIC	$\mu = 3,467$ $\sigma = 1,795$	$\mu = 3,3323$ $\sigma = 0,3577$	$\mu = 3,038$ $\sigma = 0,3644$
Valor p	0,028	0,516	0,02

ser feitas a fim de determinar possíveis divergências.

A Tabela 5.8 exibe os coeficientes de correlação para cada uma das perguntas. É possível notar um grau de correlação moderado entre as métricas utilizadas e as métricas importantes. Não foi encontrada correlação significativa para a complexidade das métricas entre os dois setores. Isso aponta a existência de semelhanças entre as métricas utilizadas e consideradas importantes para os dois tipos de organização e diferenças entre a complexidade das métricas. A seguir algumas dessas similaridades e divergências entre os tipos de empresa serão apresentadas.

A Tabela 5.9 apresenta os resultados da análise de variância entre esses dois tipos. Os valores p para cada uma das questões, mostram diferenças significativas entre os dois tipos de empresa com relação as métricas utilizadas (Q7) e a complexidade das métricas (Q9). Os participantes vinculados a empresas do setor de Educação responderam que usam, em média, 4,73 métricas contra 3,467 do setor de TIC. Além disso, as avaliações da complexidade das métricas pelos participantes do setor de TIC foi, em média, mais baixa do que os participantes de Educação. O próximo passo consiste em compreender as diferenças em Q7 e Q9. A Tabela 5.10 apresenta os resultados da ANOVA para os grupos de métricas em cada questão. μ_1 representa a média das respostas para os participantes

Tabela 5.10: Tabela ANOVA - Influência do tipo da empresa

Tipo da métrica	Métricas utilizadas (Q7)	Importância das métricas (Q8)	Complexidade das métricas (Q9)
Alvos de ataques	$\mu_1 = 3,6$ $\mu_2 = 3,8$ $p = 0,898$	$\mu_1 = 3,28$ $\mu_2 = 3,2$ $p = 0,797$	$\mu_1 = 3,106$ $\mu_2 = 3,44$ $p = 0,081$
Ameaças	$\mu_1 = 4,5$ $\mu_2 = 6,375$ $p = 0,096$	$\mu_1 = 3,3337$ $\mu_2 = 3,345$ $p = 0,955$	$\mu_1 = 2,9763$ $\mu_2 = 3,1488$ $p = 0,207$
Como a organização lida com os ataques	$\mu_1 = 1,667$ $\mu_2 = 2,833$ $p = 0,185$	$\mu_1 = 3,2917$ $\mu_2 = 3,0117$ $p = 0,214$	$\mu_1 = 3,3783$ $\mu_2 = 3,2317$ $p = 0,359$
Detecção de ataques	$\mu_1 = 4,333$ $\mu_2 = 5,667$ $p = 0,256$	$\mu_1 = 3,3783$ $\mu_2 = 3,585$ $p = 0,350$	$\mu_1 = 2,5333$ $\mu_2 = 3,18$ $p = 0,015$
Vulnerabilidades de segurança	$\mu_1 = 4,2$ $\mu_2 = 2,8$ $p = 0,195$	$\mu_1 = 3,124$ $\mu_2 = 3,376$ $p = 0,357$	$\mu_1 = 3,312$ $\mu_2 = 3,266$ $p = 0,583$

do setor de TIC, μ_2 representa a média das respostas para os participantes do setor de Educação e p indica o respectivo valor p entre as médias encontradas.

Os resultados da ANOVA mostram que para a questão 9 uma diferença relevante foi encontrada entre as métricas do grupo Detecção de ataques. Com relação a questão 7, apesar da Tabela 5.9 apontar uma diferença relevante entre as área de TIC e Educação, não foi possível notar a distinção a partir da comparação entre os grupos de métricas definidos (todos os valores $p > 0,05$). Outro modo encontrado para identificar diferenças entre as respostas dadas pelos participantes de cada uma das áreas é a comparação das respostas ordenadas. O resultado pode ser encontrado nas Tabelas 5.11 e 5.12.

A Tabela 5.11 mostra que cinco métricas estão entre as mais utilizadas em ambos os setores: número de ataques relacionados a negação de serviço, número de incidentes de segurança (externos/internos) reportados, número de ataques relacionados a Spam e número de ataques direcionados a servidores.

Ao contrário da área de Educação, é possível notar a preocupação do setor de TIC com a proteção da infraestrutura física da organização. Esse é possivelmente um reflexo do maior controle imposto pelas organizações privadas (TIC), em comparação com o setor de Educação, em especial as instituições de nível superior.

Tabela 5.11: Questão 7 - Diferenças entre TIC e Educação

Métricas utilizadas - TIC	Métricas utilizadas - Educação
Número de ataques relacionados a estrutura física da organização (7)	Número de ataques relacionados a Spam (11)
Número de incidentes de segurança internos reportados (7)	Número de ataques relacionados a Negação de Serviço (8)
Número de ataques direcionados a servidores (6)	Porcentagem de funcionários de TIC com dedicação exclusiva à segurança da informação (8)
Número de ataques relacionados a Negação de Serviço (6)	Número de ataques relacionados a Malwares (8)
Número de incidentes de segurança externos reportados (6)	Número de ataques direcionados a servidores (7)
Número de ataques relacionados a Engenharia Social (5)	Número de incidentes de segurança externos reportados (7)
Número de ataques relacionados a exploração de vulnerabilidades de segurança (5)	Número de ataques direcionados a estações de trabalho (7)
Número de ataques relacionados a Spam (5)	Número de incidentes de segurança internos reportados (7)
	Número de vulnerabilidades de segurança em servidores (7)

Tabela 5.12: Questão 9 - Diferenças entre TIC e Educação

Métricas (Detecção de ataques)	TIC	Educação
Número de incidentes de segurança internos reportados	2,27	3,63
Número de incidentes de segurança externos reportados	2,6	3,63
Porcentagem de funcionários de TIC com dedicação exclusiva à segurança da informação	2,47	2,56
Porcentagem de tentativas de intrusão bloqueadas	2,53	3
Número de incidentes críticos (severos) reportados	2,8	3,63
Porcentagem de funcionários de segurança com relação ao número total de empregados	3	2,63

Já na Educação, destaca-se a preocupação com os ataques Malware e Spam. Considerando que o questionário foi enviado para diversos profissionais que trabalham em universidades, o uso de métricas para avaliar os ataques associados a Spam e Malware é coerente com o ambiente acadêmico. A ocorrência desses tipos de incidentes em redes acadêmicas é demonstrada no capítulo 4. Contudo, devido a alta incidência de incidentes do tipo Bot nos últimos anos, um desempenho melhor da métrica que avalia esse tipo de incidente era esperado.

A principal diferença entre os dois setores, com relação ao uso de métricas na prática, é dado pelas seguintes métricas: número de ataques relacionados a Spam (citado cinco vezes nas empresas de TIC e onze em Educação) e porcentagem de funcionários de TIC com dedicação exclusiva a segurança da informação (citado quatro vezes nas empresas de TIC e oito em Educação). Esses resultados revelam uma preocupação maior do setor de Educação com relação ao controle de Spam, quando comparado as empresas de TIC. Já a diferença encontrada para a métrica "Porcentagem de funcionários de TIC com dedicação exclusiva a segurança da informação", pode indicar interpretações distintas acerca da importância de um quadro de funcionários com dedicação exclusiva a segurança. Um exemplo é a visão de que empregados dedicados somente a segurança custam mais caro para a empresa.

Com relação a complexidade, a Tabela 5.12 revela as diferenças entre as métricas do grupo Detecção de ataques. O grande contraste entre os grupos foi encontrado nas métricas que envolvem o número de incidentes de segurança reportados (externos, internos e críticos). Embora os participantes do setor de Educação considerem a detecção de segurança um processo complexo, o mesmo não foi encontrado na área da TIC.

As várias semelhanças encontradas na questão 7 entre os participantes da área de TIC e Educação podem ser usadas para iniciar as discussões sobre o uso de métricas de segurança em diferentes organizações. A existência de um possível conjunto comum de métricas utilizado na prática e compartilhado entre diferentes empresas pode ser o primeiro passo para fortalecer a disseminação das métricas na comunidade científica. Além disso, outras investigações podem ser realizadas com o objetivo de compreender os fatores que influenciam a escolha de métricas de segurança.

Tabela 5.13: Experiência do participante - Correlação entre as perguntas

	Questão 7	Questão 8	Questão 9
Correlação	0,687	0,627	0,7
Valor p	0,000	0,000	0,000

5.3.3 Relação entre a experiência em segurança e as métricas

Além da diferença entre os tipos de empresa, a experiência do profissional pode ser um fator relevante nas decisões tomadas sobre as métricas de segurança. É razoável supor que profissionais com mais experiência em segurança da informação tenham percepções diferentes sobre as questões que envolvem as métricas de segurança do que os profissionais com uma experiência menor. A forma mais simples de analisar essa situação é a criação de dois grupos distintos de participantes com relação a experiência em segurança. Consequentemente, dois grupos do presente conjunto de dados serão investigados: i) participantes com até dois anos de experiência em segurança da informação e ii) participantes com mais de dez anos de experiência em segurança da informação. O número de pessoas para cada um dos casos foi de 16 e 13, respectivamente.

Primeiramente, será verificada a correlação entre as respostas dadas pelos dois grupos. Se as respostas não apresentarem qualquer tipo de correlação, as diferenças entre os dois grupos de profissionais se tornam mais aparentes. Caso contrário, os conjuntos podem apresentar semelhanças entre si, e outras análises devem ser feitas a fim de determinar possíveis divergências.

A Tabela 5.13 exibe os coeficientes de correlação para cada uma das perguntas. É possível notar uma correlação moderada entre as métricas escolhidas pelos participantes (Q7) e também entre as métricas consideradas importantes (Q8), além de uma correlação alta entre a complexidade das métricas. Isso significa que existe uma relação entre as três respostas dadas pelos participantes menos experientes e mais experientes. A seguir, cada uma das questões será analisada, na tentativa de estabelecer as diferenças e similaridades entre os conjuntos.

A Tabela 5.14 apresenta os resultados das diferenças das médias em cada uma das questões. Conforme os valores p observados na tabela, não foi possível distinguir diferenças

Tabela 5.14: Tabela ANOVA - Influência da experiência em segurança da informação

	Métricas utilizadas (Q7)	Importância das métricas (Q8)	Complexidade das métricas (Q9)
Até dois anos	$\mu = 3,367$ $\sigma = 2,008$	$\mu = 3,2037$ $\sigma = 0,3730$	$\mu = 3,0237$ $\sigma = 0,2443$
Mais do que 10 anos	$\mu = 4,133$ $\sigma = 1,737$	$\mu = 3,5703$ $\sigma = 0,3303$	$\mu = 3,3537$ $\sigma = 0,3223$
Valor p	0,119	0,000	0,000

somente nas repostas da questão 7. Contudo, foram encontradas diferenças significativas para a importância das métricas e também para a complexidade. O próximo passo consiste em identificar tais diferenças.

A Tabela 5.15 apresenta a análise das diferenças entre a experiência do participante e cada um dos grupos de métricas. O agrupamento das métricas facilita a visualização dos resultados. μ_1 representa a média das respostas para os participantes com até dois anos de experiência em segurança, μ_2 representa a média das respostas para os participantes com mais de dez anos de experiência em segurança e p indica o respectivo valor p entre as médias encontradas.

Os resultados da ANOVA indicam que a hipótese nula não deve ser rejeitada para nenhum dos grupos de métrica na questão 7. Isso mostra que as respostas para essa questão, dadas por profissionais com menos de dois anos de experiência ou com mais de dez anos, não são diferentes em relação aos grupos. Já a hipótese nula foi rejeitada em um caso para a questão 8 (Vulnerabilidades) e em dois casos para a questão 9 (Alvos e Como a organização lida com os ataques).

A análise individual das métricas mostra que a principal diferença entre as duas classes de respondentes analisadas, com relação ao uso na prática, é relacionada ao estudo e tratamento de incidentes: tempo médio para encontrar um incidente (citado uma vez por participantes com menos de dois anos de experiência e cinco vezes pelos participantes com mais de dez anos), número de incidentes críticos (severos) reportados/detectados (citado duas vezes por participantes com menos de dois anos de experiência e cinco vezes pelos participantes com mais de dez anos).

Em resumo, esse resultado demonstra que o contraste nas respostas dadas pelos profis-

Tabela 5.15: Tabela ANOVA - Influência da experiência em segurança da informação por tipo de métrica

Tipo da métrica	Métricas utilizadas (Q7)	Importância das métricas (Q8)	Complexidade das métricas (Q9)
Alvos de ataques	$\mu_1 = 2,8$ $\mu_2 = 3,6$ $p = 0,424$	$\mu_1 = 3,19$ $\mu_2 = 3,6$ $p = 0,079$	$\mu_1 = 3,138$ $\mu_2 = 3,632$ $p = 0,012$
Ameaças	$\mu_1 = 4,25$ $\mu_2 = 4,875$ $p = 0,529$	$\mu_1 = 3,2588$ $\mu_2 = 3,4925$ $p = 0,223$	$\mu_1 = 2,968$ $\mu_2 = 3,24$ $p = 0,080$
Como a organização lida com os ataques	$\mu_1 = 1,833$ $\mu_2 = 2,667$ $p = 0,44$	$\mu_1 = 2,9183$ $\mu_2 = 3,36$ $p = 0,085$	$\mu_1 = 3,043$ $\mu_2 = 3,3967$ $p = 0,002$
Detecção de ataques	$\mu_1 = 4,333$ $\mu_2 = 4,5$ $p = 0,864$	$\mu_1 = 3,4067$ $\mu_2 = 3,7433$ $p = 0,069$	$\mu_1 = 2,8033$ $\mu_2 = 3,1017$ $p = 0,131$
Vulnerabilidades de segurança	$\mu_1 = 4,8$ $\mu_2 = 3,2$ $p = 0,195$	$\mu_1 = 3,708$ $\mu_2 = 3,228$ $p = 0,034$	$\mu_1 = 3,508$ $\mu_2 = 3,238$ $p = 0,060$

sionais com menos de dois anos de experiência e com mais de dez anos de experiência em segurança da informação reside em dois fatores: a importância e a avaliação da complexidade dadas às métricas. Não foram encontrados resultados estatisticamente relevantes acerca do uso de métricas diferentes para esses dois tipos de profissionais. Assim, apesar da diferença encontrada na avaliação da importância e da complexidade, ambos os grupos usam um conjunto de métricas semelhantes entre si, analogamente aos resultados obtidos para as organizações do setor de TIC e Educação.

Os resultados encontrados sugerem que a experiência em segurança é um fator usado para distinguir as métricas importantes e identificar a complexidade das métricas, porém, as métricas efetivamente utilizadas na organização, não necessariamente variam de acordo com a experiência. Isso pode ser explicado devido a questões de orçamento, tempo disponível para implantação das métricas e as inúmeras decisões gerenciais envolvidas no processo.

5.4 Resumo dos resultados

Os principais resultados encontrados na presente seção podem ser sumarizados do seguinte modo:

- Métricas mais utilizadas (Q7): número de ataques relacionados a Spam, número de ataques relacionados a Negação de serviço, número de incidentes de segurança internos, número de vulnerabilidades de segurança em servidores e número de incidentes de segurança externos;
- Número de incidentes de segurança internos e número de vulnerabilidades de segurança em servidores estão entre as mais usadas (Q7) e mais importantes (Q8);
- Número de ataques a dispositivos móveis, número de ataques a recursos que estão na nuvem e número de vulnerabilidades de segurança em recursos da nuvem estão entre as menos utilizadas (Q7) e as de menor importância (Q8);
- Houve correlação alta entre as métricas mais utilizadas (Q7) e as consideradas mais importantes (Q8);
- A análise de cada um dos grupos de métricas definidos mostrou diferenças estatisticamente significantes somente entre as respostas da pergunta Q9 (complexidade das métricas). O mesmo não ocorreu para as perguntas Q7 e Q8;
- A área da empresa (TIC e Educação) e a experiência em segurança da informação (até dois anos e mais de dez anos de experiência) também apresentaram as maiores diferenças com relação a percepção da complexidade das métricas. Somente diferenças sutis foram encontradas nas métricas utilizadas (Q7) e consideradas mais importantes (Q8);

Capítulo 6

Conclusões e Trabalhos Futuros

O uso de métodos quantitativos para medir a segurança de sistemas apresenta diversos desafios. O objetivo deste trabalho foi investigar e discutir os benefícios e a relevância da abordagem quantitativa aplicada em segurança da informação. Para tanto, as pesquisas foram direcionadas às seguintes abordagens:

- Identificação das razões que envolvem a ausência de validação nos métodos empregados para a quantificação da segurança;
- Investigação de fatores que influenciam a segurança de uma organização usando dados coletados em ambientes reais;
- Criação e aplicação de um questionário para investigar o uso de métricas na prática.

O primeiro passo da pesquisa envolveu o levantamento de métodos empregados para medir a segurança de sistemas. Os três *surveys* publicados sobre o tema ((Villarrubia et al., 2004), (Verendel, 2009) e (Rudolph e Schwarz, 2012)) indicam que um dos desafios da área é lidar com a ausência de validação dos diversos métodos propostos usando dados empíricos. Boa parte da literatura sobre quantificação de segurança não apresenta evidências sobre os benefícios e restrições de tais métodos. Como os trabalhos analisados não forneceram repostas sobre as razões desse problema, foi desenvolvida uma pesquisa para tentar entender as possíveis origens dessa limitação.

A análise crítica dos 57 artigos permitiu a criação de uma nova taxonomia para a categorização e comparação de modelos de quantificação de segurança baseado em três

critérios: o alvo da medida, ou seja, o sistema ou processo de interesse, a metodologia de obtenção da medida e os dados utilizados. Os resultados encontrados indicam que grande parte dos modelos para quantificar segurança investigados buscam medir alvos genéricos e complexos, como por exemplo medir a segurança da rede ou a segurança da organização. Uma característica encontrada em tais modelos foi a ausência de validação. Além disso, dentre os modelos estudados, o uso de dados reais e tentativas de validações aparecem com maior frequência nos trabalhos que propõem a quantificação de alvos específicos.

As inúmeras tentativas de quantificar a segurança de toda uma rede ou organização possuem virtudes que podem ser aproveitadas, contudo, tais abordagens ainda não foram extensivamente validadas pela comunidade científica. A pesquisa apresentada mostrou evidências de que a quantificação de segurança é melhor aproveitada quando são tratados problemas menores e específicos. São esses os modelos que devem ser validados e comparados entre si usando diferentes tipos de dados.

Uma analogia interessante pode ser feita com a área econômica. As mudanças na economia são detectadas com o auxílio de diversos indicadores Kaminsky et al. (1998), Saisana e Tarantola (2002). Cada indicador é responsável por interpretar determinadas situações e modelos que investigam o relacionamento entre os indicadores são necessários para compreender interpretar os acontecimentos como recessões ou expansões. Os resultados encontrados nesta tese mostram que as pesquisas em quantificação de segurança devem seguir um caminho semelhante a esse.

Com esse intuito, foram propostos dois estudos para investigar possíveis fatores que influenciam um aspecto específico da segurança de uma organização: a frequência de incidentes de segurança reportados. O primeiro estudo consistiu em analisar a relação entre os dados do IPS e o número de incidentes de segurança a partir de dados fornecidos pela University of Maryland. Essa suposta relação foi sugerida em trabalhos anteriores, mas ainda não tinha sido investigada. Um dos benefícios do estabelecimento dessa relação é a grande quantidade de informação presente nos registros de IPS. Endereços IP dos atacantes e dos alvos do ataque, assinatura do ataque, volume de alertas e portas de origem e destino são alguns exemplos. Foram extraídas 12 métricas a partir desses atributos e um modelo de regressão linear híbrido foi criado com o objetivo de quantificar a relação entre as métricas e a frequência de incidente.

Os resultados mostraram que certas características dos ataques bloqueados influenciam o número de incidentes reportados, indicando que os dados de IPS podem ser usados para melhorar a compreensão dos incidentes de segurança em uma organização. Além disso, a análise realizada de acordo com o tipo de incidente (Hacking, Bot e Spam) revelou a existência de métricas relevantes diferentes para cada tipo de incidente estudado. Também foi mostrado que as métricas significativas encontradas com o auxílio da regressão linear devem ser investigadas a fim de determinar o nível de influência sobre o objeto de medida. Por meio da análise dos coeficientes do teste de Laplace, foi possível estudar o comportamento das métricas em períodos próximos a uma tendência de aumento no número de incidentes. Os resultados indicaram que é possível usar certas métricas (número de computadores atacados dentro da organização, por exemplo) como indicadores de mudança do comportamento de incidentes.

Outra aplicação relacionada a esse estudo foi a proposta de um método alternativo para avaliar a eficiência dos sistemas de prevenção de intrusão. Com base na quantificação da relação entre os tipos de incidentes e as diversas métricas obtidas por meio das características dos ataques bloqueados pelo IPS, foi possível propor um coeficiente de associação para estimar a relação entre um determinado tipo de incidente e o dispositivo IPS. No caso da University of Maryland, o dispositivo IPS obteve uma identificação maior com os incidentes Bot ao longo do período estudado (entre 2007 e 2010), mas levando em consideração somente períodos mais recentes, esse cenário está mudando. Esse resultado, porém, está estritamente ligado ao conjunto de métricas que foi definido para o estudo.

O segundo estudo apresentado neste trabalho envolve a análise de fatores temporais e a associação entre diferentes tipos de incidentes usando uma base de dados única, fornecida pelo CAIS/RNP, com mais de 450.000 incidentes e 422 instituições, em que foi possível comparar e validar os métodos propostos entre as inúmeras instituições presentes no conjunto de dados.

Primeiramente, foram desenvolvidos métodos para investigar a variação dos incidentes de acordo com o dia e o mês, baseado em conceitos de séries temporais. Esse estudo é particularmente interessante, pois o tempo pode ser utilizado como um indicador para outros fatores de risco relacionados as mudanças temporais como os períodos de férias em instituições de ensino superior que estão associados a uma diminuição na população

do campus. Os resultados com os dados agregados de todas as instituições sugerem um comportamento periódico no modo em que os incidentes de segurança são reportados nas organizações.

Foi possível mostrar que esse comportamento possui relação com horários e possíveis hábitos de trabalho, pois a maioria dos incidentes foi reportado em determinados dias da semana. Esse fato é um reflexo da interação manual que envolve o processo de notificação e o registro de incidentes. Uma tendência de aumento no número de incidentes logo após os meses de janeiro e fevereiro também foi encontrada, que pode ser explicada pelo aumento da população das instituições (a maioria das instituições são acadêmicas), devido ao término do período de férias. Padrões similares também foram encontrados na análise de dados de algumas instituições selecionadas. Isso mostra que, além do fator humano e das vulnerabilidades referentes ao aparatos tecnológicos adotados pelas organizações, as características do ambiente também influenciam na maneira com que os ataques são executados.

A última contribuição do trabalho foi a proposta de uma pesquisa de avaliação para compreender quais das diversas métricas propostas na literatura são usadas para avaliar o nível de segurança da informação das organizações. Para cumprir esse objetivo, três perguntas sobre um determinado conjunto de métricas foram inseridas no questionário: 1) quais são usadas na prática, 2) qual é a importância de cada um delas e 3) a complexidade das métricas.

A análise inicial da pesquisa revelou as seguintes métricas como as mais usadas: ataques relacionados a Spam, ataques de Negação de Serviço, incidentes de segurança internos, vulnerabilidades em servidores e incidentes de segurança externos. É possível notar a preocupação dos participantes com duas ameaças específicas (Spam e Negação de Serviço) assim como as vulnerabilidades de segurança encontradas em servidores. Além disso, os incidentes de segurança reportados (externos e internos) também foram classificados entre as cinco mais importantes para métricas para avaliar o nível de segurança. Esses resultados reafirmam a importância da investigação realizada no capítulo 4 sobre os incidentes de segurança. A partir desses resultados, também é possível propor ajustes na análise de fatores que influenciam os incidentes de segurança, como diferenciar os incidentes internos e externos, e considerar a severidade do incidente em questão.

Os resultados obtidos com a análise das respostas do questionário também foram importantes para discutir o problema da escolha de métricas de segurança. As métricas usadas na prática entre os respondentes de dois tipos diferentes de empresas e também de acordo com a experiência em segurança da informação entre os participantes foram comparadas.

A análise dos coeficientes de correlação, assim como os resultados da ANOVA, não apontaram diferenças significativas entre as respostas dos participantes dos dois grupos analisados. Somente diferenças pontuais em certas métricas foram encontradas. Além de sugerir a existência de um possível conjunto comum de métricas que possa compartilhado entre diferentes tipos de empresas, os resultados também abrem um novo caminho de pesquisa, com o objetivo de investigar os fatores que influenciam a adoção de métricas de segurança em uma organização. Outros fatores, além da experiência e da variação por tipo de empresa, devem ser analisados com o intuito de estabelecer critérios fundamentados por observações empíricas para a seleção de métricas de segurança. Pesquisas semelhantes também podem ser conduzidas para entender como as métricas são implementadas nas organizações e extrair recomendações para o uso delas na prática.

Em suma, as principais contribuições obtidas com as abordagens adotadas foram:

- Elaboração de uma classificação complementar para a categorização de modelos de quantificação de segurança fundamentada em preceitos básicos da teoria de quantificação de informação;

- Desenvolvimento de técnicas para a compreensão da relação entre métricas de segurança e o processo alvo da investigação;

- Verificação e validação das técnicas propostas usando dados coletados em ambientes reais;

- Discussão sobre os fatores que influenciam a frequência de incidentes de segurança e como os profissionais da área podem usar os resultados para a criação de políticas e ações preventivas;

- Investigação sobre a aplicação da abordagem quantitativa em segurança na prática, a partir de dados coletados por um questionário respondido por profissionais da

área de TIC. A pesquisa identificou métricas relevantes e mostrou a influência de características dos participantes na escolha de métricas;

- Levantamento de métodos e trabalhos que fizeram uso da abordagem quantitativa na análise de segurança;

As contribuições apresentadas nessa tese mostram exemplos reais para guiar novas pesquisas em quantificação de segurança. Como sugestão de trabalho futuro, pode-se analisar a influência de novas métricas extraídas do sistema de prevenção de intrusão na frequência de incidentes de segurança reportados. A severidade das assinaturas, o horário dos alertas, porta de destino e os endereços IP de origem dos ataques são alguns tipos de métricas que podem ser avaliadas. Além disso, é importante que esse estudo seja ampliado para outros conjuntos de dados. Uma opção interessante consistiria em trabalhar com instituições parceiras do RNP com características semelhantes às encontradas na University of Maryland e assim comparar a eficiência das métricas em outros ambientes.

Outras pesquisas envolvem a aplicação de modelos de regressão alternativos, de acordo com o comportamento dos dados investigados. Alguns exemplos incluem a regressão logística nos casos em que estudar a ocorrência do incidente é mais interessante do que a frequência, e o uso de modelos regressivos para certos tipos de incidentes que possuem componentes não estacionários. O uso de técnicas de aprendizado de máquinas como Redes Neurais Artificiais, Comparadores Naive Bayes e Support Vector Machines (SVM) também aparecem como uma alternativa interessante para a classificação dos dados de segurança. A aplicação de tais técnicas poderia ser utilizada para extrair informações sobre a probabilidade de ocorrência de um incidente usando informações como a data, tipo, instituição ou outras combinações de eventos.

Por fim, outra vertente de pesquisa originada pelo trabalho foi o desenvolvimento de ferramentas computacionais para automatizar o processo de identificação e análise de métricas de segurança. A grande quantidade de dados que devem ser processados para avaliar as métricas e fornecer informações precisas sobre a segurança da organização torna essa área cada vez mais importante. A criação do fluxo de atividades para auxiliar o processo de validação e comparação de métricas de segurança pode ser vista como um passo inicial em direção a esse caminho de investigação.

Bibliografia

Ahmed, M. S.; Al-Shaer, E.; e Khan, L. A Novel Quantitative Approach For Measuring Network Security. In *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*, p. 1957–1965, 2008.

Alkussayer, A. e Allen, W. Security risk analysis of software architecture based on AHP. In *The 7th International Conference on Networked Computing (INC), 2011*, p. 60–67, 2011.

Arora, A.; Krishnan, R.; e Nandkumar, A. Impact of vulnerability disclosure and patch availability-an empirical analysis. In *Third Workshop on the Economics of Information Security*, p. 1–20, 2004.

Arora, A.; Nandkumar, A.; e Telang, R. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, 8(5):350–362, November 2006.

Arsham, H. Time-Critical Decision Making for Business Administration. Technical report, University of Baltimore, USA, 2003.

Bailey, M.; Cooke, E.; Jahanian, F.; Xu, Y.; e Karir, M. A Survey of Botnet Technology and Defenses. In *2009 Cybersecurity Applications & Technology Conference for Homeland Security*, p. 299–304, 2009.

Baker, W. e Wallace, L. Is information security under control?: Investigating quality in information security management. *Security & Privacy, IEEE*, 5(1):36–44, 2007.

Balci, O. Verification, validation, and accreditation. In *Proceedings of the 30th conference on Winter simulation*, 1998.

Bayuk, J. L. *Measuring Systems Security: An Initial Security Theoretical Construct Framework*. PhD thesis, Stevens Institute of Technology, 2011.

Bengtsson, M. *Mathematical foundation needed for development of IT security metrics*. PhD thesis, Linkoping University, 2007.

Bento, A. e Bento, R. Empirical Test of a Hacking Model : An Exploratory Study. *Communications of the Association for Information Systems*, 14(1):678–690, 2004.

Bhatt, S.; Horne, W.; e Rao, P. On Computing Enterprise IT Risk Metrics. p. 271–280, 2011.

Bishop, M. *Computer Security: Art and Science*. Addison Wesley, 2002.

Black, K. *Business statistics: for contemporary decision making*. John Wiley & Sons, 2011.

Boyer, W. e McQueen, M. Ideal based cyber security technical metrics for control systems. In *Critical Information Infrastructures Security*, p. 246–260, 2008.

Brockwell, P. J. e Davis, R. A. *Introduction to time series and forecasting*. Springer Verlag, 2002.

Budescu, D. V. Dominance analysis: A new approach to the problem of relative importance of predictors in multiple regression. *Psychological Bulletin*, 114(3):542–551, 1993.

CERT.br, . Grupos de segurança brasileiros, 2013. URL `http://www.cert.br/csirts/brasil/`.

Chew, E.; Swanson, M.; Stine, K.; e Bartol, N. SP 800-55 Rev. 1. Performance Measurement Guide for Information Security. Technical Report July, National Institute of Standards and Technology (NIST), 2008.

Chrun, D. *Model-Based Support for Information Technology Security Decision Making*. PhD thesis, University of Maryland, 2011.

Chrun, D.; Cukier, M.; e Sneeringer, G. On the Use of Security Metrics Based on Intrusion Prevention System Event Data: An Empirical Analysis. In *2008 11th IEEE High Assurance Systems Engineering Symposium*, p. 49–58, December 2008a.

Chrun, D.; Cukier, M.; e Sneeringer, G. Finding corrupted computers using imperfect intrusion prevention system event data. In *Computer Safety, Reliability, and Security*, p. 221–234. Springer Berlin Heidelberg, 2008b.

Church, C. e Rogers, M. *Designing for Results: Integrating Monitoring and Evaluation in Conflict Transformation Programs*. Search for Common Ground, 2006.

Condon, E. e Cukier, M. Using Population Characteristics to Build Forecasting Models for Computer Security Incidents. *2012 IEEE 23rd International Symposium on Software Reliability Engineering*, p. 71–80, November 2012.

Condon, E.; Cukier, M.; e He, T. Applying Software Reliability Models on Security Incidents. In *The 18th IEEE International Symposium on Software Reliability (ISSRE '07)*, p. 159–168, November 2007.

Condon, E.; He, A.; e Cukier, M. Analysis of Computer Security Incident Data Using Time Series Models. In *2008 19th International Symposium on Software Reliability Engineering (ISSRE)*, p. 77–86. Ieee, November 2008.

Cooke, E.; Jahanian, F.; e Mcpherson, D. The Zombie Roundup : Understanding , Detecting , and Disrupting Botnets. In *Proceedings of the USENIX SRUTI Workshop*, p. 39–44, 2005.

Croarkin, C. e Tobias, P. *NIST/Sematech e-Handbook of Statistical Methods*. 2003. URL `http://www.itl.nist.gov/div898/handbook/`.

Cukier, M. e Panjwani, S. Prioritizing vulnerability remediation by determining attacker-targeted vulnerabilities. *IEEE Security and Privacy*, 7(1):42–48, 2009.

Cukier, M. e Panjwani, S. A Comparison between Internal and External Malicious Traffic. In *The 18th IEEE International Symposium on Software Reliability (ISSRE '07)*, p. 109–114, November 2007.

Dacier, Marc, Yves Deswarte, e Kaâniche, M. Quantitative Assessment of Operational Security : Models and Tools. Technical report, LAAS, 1996.

Daniel E. Geer Jr, e Pareek, M. ICS Update. *IEEE Security & Privacy Magazine*, (June): 93–95, 2012.

Department of Homeland Security, . Cyber Security Research and Development. Technical report, Department of Homeland Security, 2011.

Department of Homeland Security, . PREDICT, the Protected Repository for the Defense of Infrastructure Against Cyber Threats, 2013.

Devore, J. L. *Probability & Statistics for Engineering and the Sciences*. Duxbury Press, 2012.

Egan, G.; Haley, K.; Mckinney, D.; Millington, T.; Mulcahy, J.; Parsons, T.; Watson, A.; Nisbet, M.; Johnston, N.; e Hittel, S. Internet Security Threat Report. Technical Report April, Symantec, 2012.

Feng, C. e Jin-Shu, S. A Flexible Approach to Measuring Network Security Using Attack Graphs. In *2008 International Symposium on Electronic Commerce and Security*, p. 426–431. Ieee, 2008.

Frigault, M. e Wang, L. Measuring Network Security Using Bayesian Network-Based Attack Graphs. In *2008 32nd Annual IEEE International Computer Software and Applications Conference*, p. 698–703, 2008.

Geer, D.; Hoo, K.; e Jaquith, A. Information security: Why the future belongs to the quants. *Security & Privacy, IEEE*, 1(4):24–32, 2003.

Goel, S. e Chengalur-Smith, I. N. Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4):281–295, December 2010.

Green, S. B. How Many Subjects Does It Take To Do A Regression Analysis. *Multivariate Behavioral Research*, 26(3):499–510, July 1991. URL `http://www.tandfonline.com/doi/abs/10.1207/s15327906mbr2603_7`.

Guilford, J. P.; Fruchter, B.; e Others, . *Fundamental statistics in psychology and education*, volume 1. McGraw-Hill New York, 1965.

Halinski, R. S. e Feldt, L. S. The Selection of Variables in Multiple Regression. 7(3): 151–157, 1970.

Harrison, K. e White, G. An Empirical Study on the Effectiveness of Common Security Measures. In *2010 43rd Hawaii International Conference on System Sciences*, p. 1–7, 2010.

Hecker, M.; Goertsches, R. H.; Engelmann, R.; Thiesen, H.-J.; e Guthke, R. Integrative modeling of transcriptional regulation in response to antirheumatic therapy. *BMC bioinformatics*, 10:262, January 2009.

Herrmann, D. S. *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. Auerbach Publications, 2007.

Hinson, G. Seven myths about information security metrics. *Information System Security Association (ISSA)*, (July), 2006.

Holm, H.; Ekstedt, M.; e Andersson, D. Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks. *IEEE Transactions on Dependable and Secure Computing*, 9(6):825–837, November 2012.

Howard, J. D. *An Analysis Of Security Incidents On The Internet 1989 - 1995*. PhD thesis, Carnegie Mellon, 1997.

Howard, J. D. e Longstaff, T. A. A Common Language for Computer Security Incidents. Technical Report October, Sandia National Laboratories, 1998.

International Organization for Standardization, . ISO/IEC 27004. Technical report, International Organization for Standardization, 2009.

Jajodia, S.; Li, J.; e Singhal, A. Automatic security analysis using security metrics. In *2011 - MILCOM 2011 Military Communications Conference*, p. 1207–1212, November 2011.

Jansen, W. Directions in security metrics research. Technical report, National Institute of Standards and Technology (NIST), 2010.

Jaquith, A. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Professional, 2007.

Jensen, M.; Schwenk, J.; Gruschka, N.; e Iacono, L. L. On Technical Security Issues in Cloud Computing. *2009 IEEE International Conference on Cloud Computing*, p. 109–116, 2009.

Jonsson, E. e Pirzadeh, L. A Framework for Security Metrics Based on Operational System Attributes. In *2011 Third International Workshop on Security Measurements and Metrics*, p. 58–65, September 2011.

Kajava, J. e Savola, R. Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes. In *Proceedings of the European University Information Systems (EUNIS)*, 2005.

Kaminsky, G.; Lizondo, S.; e Reinhart, C. Leading indicators of currency crises. *Staff Papers -I nternational Monetary Fund*, 45(1):1–48, 1998.

Kanoun, K.; Rettelbusch, M.; Martini, D. B.; e Souza, J. M. D. A Method for Software Reliability Analysis and Prediction Application to the TROPICO-R Switching System. *IEEE Transactions on Software Engineering*, 17(4):334–344, 1991.

Karasaridis, A.; Rexroad, B.; e Hoeflin, D. Wide-scale botnet detection and characterization. In *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007.

Kaufman, L. Data security in the world of cloud computing. *Security & Privacy, IEEE*, p. 61–64, 2009.

Khan, J. a.; Van Aelst, S.; e Zamar, R. H. Robust Linear Model Selection Based on Least Angle Regression. *Journal of the American Statistical Association*, 102(480):1289–1299, December 2007.

Khan, M. A. e Hussain, M. Cyber security quantification model. In *Proceedings of the 3rd international conference on Security of information and networks - SIN '10*, p. 142, New York, New York, USA, 2010. ACM Press.

Kotenko, I. Attack graph based evaluation of network security. In *Communications and Multimedia Security*, p. 216–227, 2006.

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

Leversage, D. e James, E. Estimating a System's Mean Time-to-Compromise. *Security & Privacy, IEEE*, 2008.

Liu, C. *Two Tales of Variable Selection for High Dimensional Data : Screening and Model Building*. PhD thesis, The Ohio State University, 2012.

Machado, C.; Cabral, L.; Santos, J.; e Motta, G. Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. In *V Simpósio Brasileiro de Sistemas de Informação*, p. 97–108, 2009.

Maslennikov, D. e Namestnikov, Y. Kaspersky Security Bulletin 2012, 2012.

McCann, L. e Welsch, R. E. Robust variable selection using least angle regression and elemental set sampling. *Computational Statistics & Data Analysis*, 52(1):249–257, September 2007.

Mell, P.; Scarfone, K.; e Romanosky, S. A Complete Guide to the Common Vulnerability Scoring System. Technical report, National Institute of Standards and Technology (NIST), 2007.

Mendenhall, W. e Sincich, T. *A second course in business statistics: regression analysis*. Dellen Publishing Company, 1989.

Metz, C. AAA protocols: authentication, authorization, and accounting for the Internet. *Internet Computing, IEEE*, 3(6):75–79, 1999.

Miani, R. S. *Aplicação de métricas à análise de segurança em Redes Metropolitanas de Acesso Aberto*. Dissertação de mestrado, Universidade Estadual de Campinas (Unicamp), 2009.

Miani, R. S.; Zarpelão, B. B.; e Mendes, L. S. Application of Security Metrics in a Metropolitan Network : A Case Study. In *The 7th International Telecommunications Symposium (ITS 2010)*, Manaus, 2010.

Mitre, . Common Vulnerabilities and Exposures, 2013. URL `http://cve.mitre.org/`.

Montgomery, D.; Peck, E.; e Vining, G. *Introduction to linear regression analysis*. Wiley, 2012.

Nagahama, F. Y.; Farias, F.; Aguiar, E.; Gaspary, L.; Granville, L.; Cerqueira, E.; e Abelem, A. IPSFlow: Uma Proposta de Sistema de Prevenção de Intrusão Baseado no Framework OpenFlow. In *III Workshop de Pesquisa Experimental da Internet do Futuro*, p. 42–47, 2008.

Nakamura, E. T. e Geus, P. L. *Segurança de Redes em Ambientes Cooperativos*. Editora Novatec, 2007.

NIST, . National Vulnerability Database (NVD), 2013. URL `http://nvd.nist.gov/`.

Panjwani, S.; Tan, S.; Jarrin, K.; e Cukier, M. An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack. In *2005 International Conference on Dependable Systems and Networks (DSN'05)*, p. 602–611, 2005.

Patel, A.; Qassim, Q.; e Wills, C. A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, 18(4):277–290, 2010.

Paul E. Black, K. S. e Souppaya, M. Cyber security metrics and measures. *Handbook of Science and Technology for Homeland Security*, 5:1–9, 2008.

Payne, S. A guide to security metrics. Technical report, 2006.

Pfleeger, S. L. e Cunningham, R. K. Why measuring security is hard. *Security & Privacy, IEEE*, 8(4):46–54, 2010.

Pfleeger, S. L. Useful Cybersecurity Metrics. *IT Professional*, 11(June):38–45, 2009.

PriceWaterHouseCoopers, . Global State of Information Security Survey. Technical report, 2011.

Richardson, R. CSI Computer Crime & Security Survey. Technical report, Computer Security Institute (CSI), 2008.

Richardson, R. Computer Crime and Security Survey. Technical report, Computer Security Institute, 2011.

Rodgers, J. L. e Nicewander, W. Thirteen ways to look at the correlation coefficient. *The American Statistician*, (April 2013):37–41, 1988.

Rudolph, M. e Schwarz, R. A Critical Survey of Security Indicator Approaches. *2012 Seventh International Conference on Availability, Reliability and Security*, p. 291–300, August 2012.

Ryan, JJC and Ryan, D. Performance metrics for information security risk management. *Security & Privacy, IEEE*, 6:38–44, 2008.

Saaty, T. L. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1):9–26, September 1990.

Sademies, A. *Process Approach to Information Security Metrics in Finnish Industry and State Institutions*. PhD thesis, 2004.

Saisana, M. e Tarantola, S. State-of-the-art Report on Current Methodologies and Practices for Composite Indicator Development Prepared by. Technical report, Institute for the Protection and Security of the Citizen - European Commission, 2002.

Scarfone, K. e Grance, T. A framework for measuring the vulnerability of hosts. In *2008 1st International Conference on Information Technology*, number May, p. 1–4, 2008.

Scarfone, K. e Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). Technical report, NIST, 2007.

Stolfo, S.; Bellovin, S.; e Evans, D. Measuring Security. *IEEE Security and Privacy*, 9 (June):60–65, 2011.

Sullivan, F. Mercado de segurança de rede na América Latina movimentará 598.4 milhões de dólares em 2013. URL `http://www.frost.com/prod/servlet/press-release.pag?docid=128005764`.

Thalia, S.; Tuteja, A.; e Dutta, M. An algorithm design to evaluate the security level of an information system. In *Computer Networks and Information Technologies*, p. 69–75, 2011.

The Center for Internet Security, . The CIS Security Metrics. Technical Report 28, The Center for Internet Security, 2010.

Thompson, M. L. Selection of Variables in Multiple Regression : Part I . A Review and Evaluation. 46(1):1–19, 1978.

Thomson, G. BYOD: enabling the chaos. *Network Security*, 2012(2):5–8, February 2012.

Tibshirani, R.; Johnstone, I.; Hastie, T.; e Efron, B. Least angle regression. *The Annals of statistics*, 32(2):407–499, 2004a.

Tibshirani, R.; Johnstone, I.; Hastie, T.; e Efron, B. Least angle regression. *The Annals of Statistics*, 32(2):407–499, April 2004b.

Torres, J.; Sarriegi, J.; e Santos, J. Managing information systems security: critical success factors and indicators to measure effectiveness. In *Information Security Conference*, p. 530–545, 2006.

Torres, J.; Sarriegi, J.; Hernantes, J.; e Lauge, A. Steering Security through Measurement. *Trust, Privacy and Security in Digital Business*, p. 95–104, 2009.

Trzesniak, P. Indicadores quantitativos : reflexões que antecedem seu estabelecimento. *Ciência da Informação*, 27(2):159–164, 1998.

Vasiu, L. e Vasiu, I. Dissecting computer fraud: from definitional issues to a taxonomy. In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004*, volume 00, p. 1–8, 2004.

Vaughn, R. B. e Henning, R. Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. In *Proceedings of the 36th Hawaii International Conference on System Sciences*, 2002.

Verendel, V. Quantified security is a weak hypothesis. In *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, p. 37–49, 2009.

Verendel, V. *Some Problems in Quantified Security*. PhD thesis, Chalmers University of Technology, 2010.

Verizon, . 2012 Data Breach Investigations Report. Technical report, 2012.

Villarrubia, C.; Fern, E.; e Piattini, M. Towards a Classification of Security Metrics. In *Proceedings of the 2nd international workshop on security in information systems (WOSIS 2004)*, p. 342—-350, 2004.

W. Krag Brotby, . *Information security management metrics: a definitive guide to effective security monitoring and measurement*. Auerbach Publications, 2009.

Wang, C. e Wulf, W. A. Towards a framework for security measurement. In *Proceedings of the Twentieth National Information Systems Security Conference*, p. 522–533, 1997.

Wang, H.; Roy, S.; e Das, A. A framework for security quantification of networked machines. In *Second International Conference on Communication Systems and Networks (COMSNETS)*, 2010.

Wang, J. e Xiao, N. Drivers of information security search behavior: an investigation of network attacks and vulnerability disclosures. *ACM Transactions on Management Information*, 1(1), 2010.

Wang, J. A.; Guo, M.; Wang, H.; e Zhou, L. Measuring and ranking attacks based on vulnerability analysis. *Information Systems and e-Business Management*, 10(4):455–490, March 2011.

Wang, L. e Singhal, A. Measuring the overall security of network configurations using attack graphs. In *Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security*, p. 98–112, 2007.

Wang, L.; Islam, T.; Long, T.; e Singhal, A. An attack graph-based probabilistic security metric. In *Data and Applications Security XXII*, volume 5094, p. 283–296, 2008.

Wei, W. W.-S. *Time series analysis*. Addison-Wesley Redwood City, California, 1994.

Weissmann, O. A comprehensive and comparative metric for information security. In *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM 2005)*, 2005.

Wright, D. e London, K. *Modern regression techniques using R: A practical guide*. SAGE Publications Limited, 2009.

Xie, A.; Cai, Z.; Tang, C.; Hu, J.; e Chen, Z. Evaluating Network Security With Two-Layer Attack Graphs. In *2009 Annual Computer Security Applications Conference*, p. 127–136, December 2009.

Zhang, J.; Berthier, R.; Rhee, W.; e Bailey, M. Learning from early attempts to measure information security performance. In *Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test*, p. 1–10, Bellevue, WA, 2012a. USENIX Association.

Zhang, J.; Berthier, R.; Rhee, W.; Bailey, M.; Pal, P.; Jahanian, F.; e Sanders, W. H. Safeguarding Academic Accounts and Resources with the University Credential Abuse Auditing System. In *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2012b.

Zhen-yuan, X.; He, C.; Xiang-zhong, W.; Jian-ling, S.; e Yu-tao, F. Evaluation Model for Computer Network Information Security Based on Analytic Hierarchy Process. In *2009 Third International Symposium on Intelligent Information Technology Application*, p. 186–189, 2009.

Apêndice A - Levantamento bibliográfico dos trabalhos analisados

Título	Processo de interesse	Metodologia	Dados
Learning from early attempts to measure information security performance	SPE	STA	REA
Useful Cybersecurity Metrics	SPE	MET, STA	THE
Ideal based cyber security technical metrics for control systems	RSK	MET	REA
Managing information systems security: critical success factors and indicators to measure effectiveness	ORG	MET	THE
Cyber security quantification model	ORG	PRO	REA
Measuring Cyber Security in Intelligent Urban Infrastructure Systems	SPE	MET	THE
Model-Based Support for Information Technology Security Decision Making	ORG, RSK, EFF	STA, MET	REA, QUE
An Empirical Study on the Effectiveness of Common Security Measures	EFF	MET, STA	REA
Measuring Effectiveness of Information Security Management	EFF	MET	THE
Performance metrics for information security risk management	EFF	PRO	EXE
Metrics for characterizing the form of security policies	EFF	MET	QUE
Turing Assessor: A New Tool for Cyber Security Quantification	NET	PRO	EXE
Impact of vulnerability disclosure and patch availability-an empirical analysis	SPE	MET, STA	REA
Does information security attack frequency increase with vulnerability disclosure? An empirical analysis	SPE	MET, STA	REA, VUL
Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment	SPE	PRO	THE
Security metrics models and application with SVM in information security management	ORG	PRO	THE
Efficient Security Measurements and Metrics for Risk Assessment	ORG	STR, MET	EXE
A Comparison between Internal and External Malicious Traffic	SPE	MET, STA	REA
Measuring and ranking attacks based on vulnerability analysis	SPE	STR, MET, GRA	VUL
Prioritizing vulnerability remediation by determining attacker-targeted vulnerabilities	SPE	STA, MET	REA
A Novel Quantitative Approach For Measuring Network Security	NET	PRO, OTH	VUL, EXE
An attack graph-based probabilistic security metric	NET	GRA	THE
Evaluation Model for Computer Network Information Security Based on Analytic Hierarchy Process	NET	STR, MET	EXE
Evaluating Network Security With Two-Layer Attack Graphs	NET	GRA, OTH	EXE
Security Level Quantification and Benchmarking in Complex Networks	NET	STR, MET, GRA	EXE
Automatic security analysis using security metrics	NET	MET, STR	EXE

Figura 6.1: Levantamento bibliográfico dos trabalhos analisados - Parte 1

Attack graph based evaluation of network security	NET	GRA, MET	EXE
Information systems security criticality and assurance evaluation	ORG	PRO, MET	EXE
Measuring Network Security Using Bayesian Network-Based Attack Graphs	NET	GRA	THE
Measuring the overall security of network configurations using attack graphs	NET	GRA	EXE
A framework for security quantification of networked machines	NET	PRO, OTH	EXE
Finding corrupted computers using imperfect intrusion prevention system event data	SPE	MET, STA	REA
A Comprehensive Objective Network Security Metric Framework for Proactive Security Configuration	SPE	GRA, PRO, MET	THE
An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack	SPE	STA, MET	REA
Relationships Between Information Security Metrics: An Empirical Study	SPE	MET, STA	REA
Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value	ORG	PRO	THE
On Computing Enterprise IT Risk Metrics	RSK	GRA, MET	THE, VUL
Measuring IT security - a method based on common criteria's security functional requirements	SPE	PRO, MET	EXE
An algorithm design to evaluate the security level of an information system	ORG	STR, GRA, MET	EXE
On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks	NET	GRA, MET	THE
A Framework for Security Metrics Based on Operational System Attributes	ORG	PRO, OTH	THE
A comprehensive and comparative metric for information security	ORG	PRO, MET	REA
Metrics for mitigating cybersecurity threats to networks	ORG	STA, MET, OTH	VUL
A Flexible Approach to Measuring Network Security Using Attack Graphs	SPE	GRA	EXE
An Empirical Model for Quantifying Security Based on Services	SPE	MET, OTH	REA
Quantitative Assessment of Enterprise Security System	ORG	GRA, PRO, OTH	EXE
Towards Quantification of Information System Security	ORG	STR, PRO	EXE
Appraisal and reporting of security assurance at operational systems level	ORG	PRO, OTH	EXE
A weakest-adversary security metric for network configuration security analysis	NET	GRA	EXE
iMeasure Security (iMS): A Novel Framework for Security Quantification	ORG	GRA, PRO	THE
Quantifying Security Threats for E-learning Systems	SPE	PRO	EXE
Dependability and Security Metrics in Controlling Infrastructure	SPE	MET	EXE
Quantifying security threats and their potential impacts: a case study	ORG	PRO, OTH	EXE
Security Assurance Aggregation for IT Infrastructures	ORG	OTH, GRA	EXE
Estimating a System's Mean Time-to-Compromise	SPE	PRO, OTH	EXE
Untrustworthiness: A Trust-Based Security Metric	SPE	OTH	THE
A framework for measuring the vulnerability of hosts	SPE	STR, MET	THE

Figura 6.2: Levantamento bibliográfico dos trabalhos analisados - Parte 2

Legenda:

- Segurança da rede (NET)
- Segurança da organização ou sistema (ORG)
- Risco (RSK)
- Eficiência (EFF)
- Outros (SPE)
- Modelos probabilísticos (PRO)
- Estatística (STA)

- Métricas simples (MET)
- Grafos (GRA)
- Técnicas estruturadas - (STR)
- Outros - (OTH)
- Exemplos fictícios (EXE)
- Sistemas em funcionamento (REA)
- Vulnerabilidades (VUL)
- Opiniões de especialistas / Questionários - (QUE)
- Teóricos (THE)

Apêndice B - Taxonomia dos incidentes reportados pela University of Maryland

Abuse	Bot	Hacking	Spam	Virus	Worm	Spyware
copyright	bot_controller	defaced_site	spamrelay	backdoor_cag	bagle_worm	core
excessive_bandwidth	irc_bot	dos	spamsource	phish_webserver	conficker	marketscore
ip_conflict		hacked		virus_agobot	deadhat_worm	spyware
nethicsreq		hacking		virus_berbew	mssql_worm	
openproxy		mssql_bruteforce		virus_brid	mydoom_worm	
not_registered		port_scanning		virus_bugbear	netsky_worm	
		rogue_ftp		virus_codered	openssl_worm	
		security_ddos		virus_fizzer	sasser_worm	
		security_flood		virus_generic_bot	stormworm	
		security_probe		virus_im_bot	worm_msblast	
		d-root		virus_klez	worm_nachi	
				virus_mimail		
				virus_nimda		
				virus_palyh		
				virus_sircam		
				virus_sobig		
				virus_zafi		

Figura 6.3: Taxonomia dos incidentes reportados pela University of Maryland

Apêndice C - Conteúdo do questionário

Este apêndice fornece as telas do questionário online enviado para os administradores de rede da Unicamp, funcionários do CAIS/RNP, Sociedade Brasileira de Computação (SBC), Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CESeg), analistas do CERT.br e grupos de segurança e resposta a incidentes brasileiros.

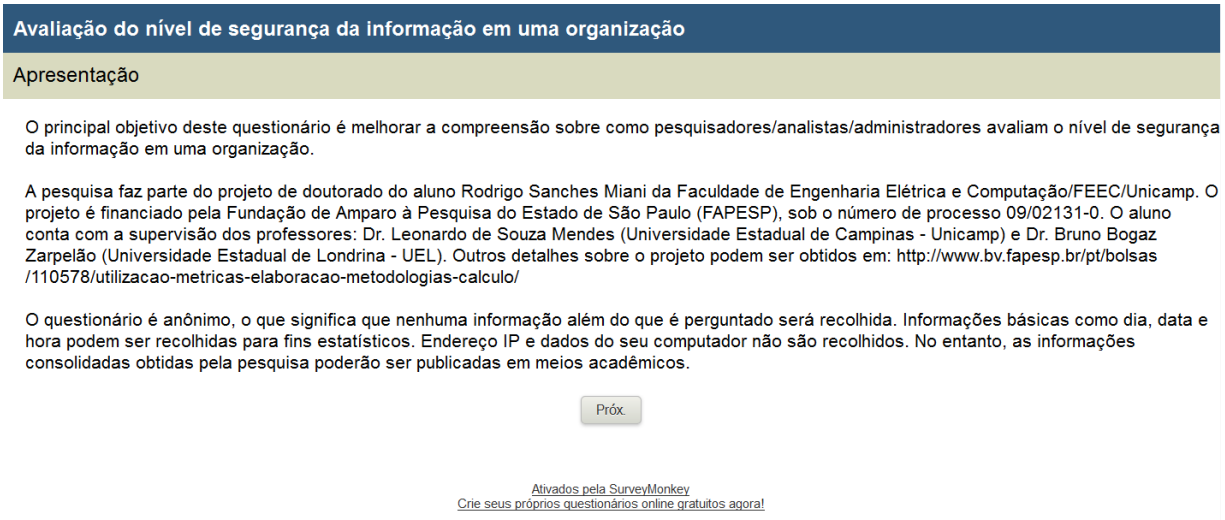
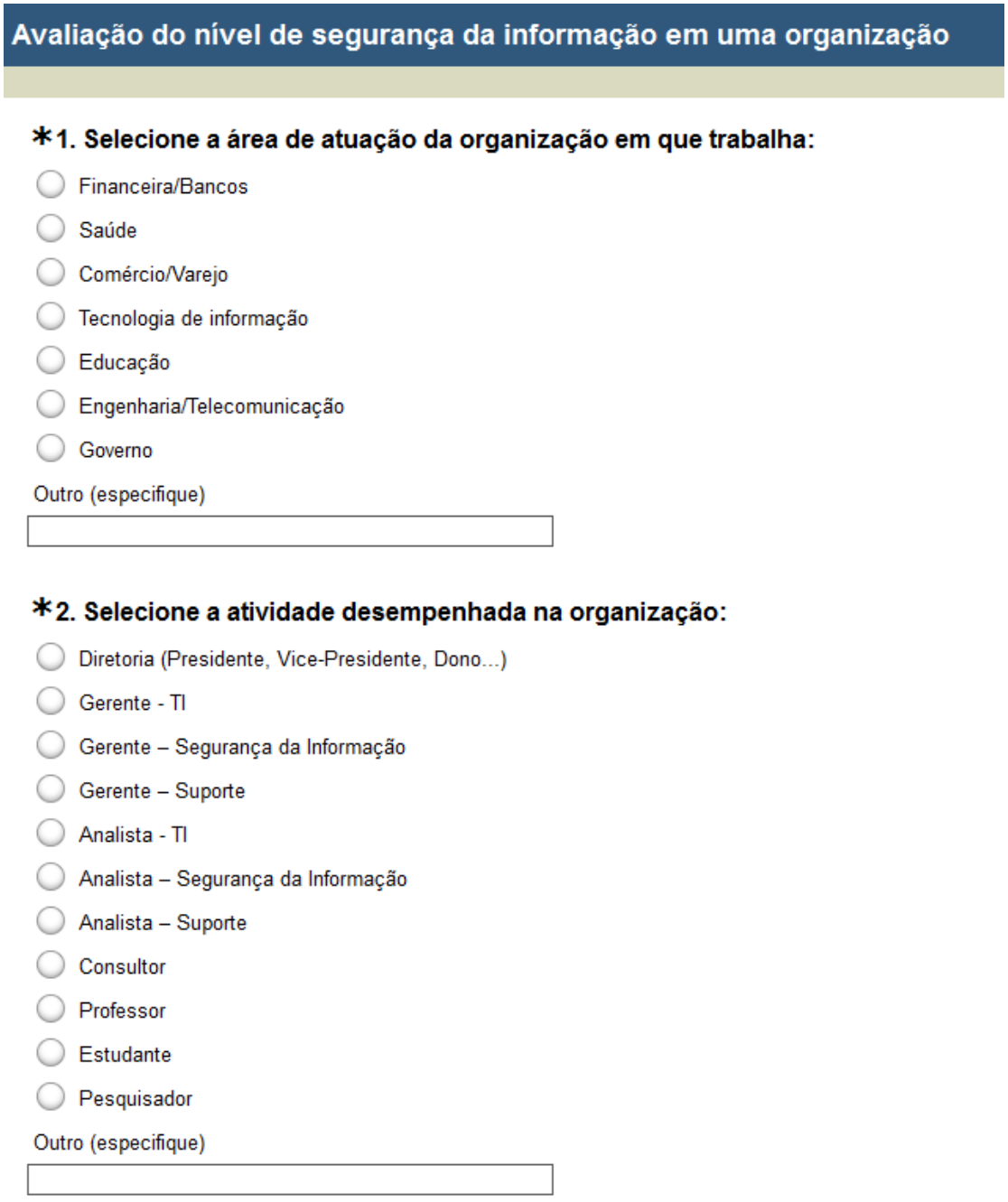


Figura 6.4: Tela inicial



Avaliação do nível de segurança da informação em uma organização

***1. Selecione a área de atuação da organização em que trabalha:**

- Financeira/Bancos
- Saúde
- Comércio/Varejo
- Tecnologia de informação
- Educação
- Engenharia/Telecomunicação
- Governo

Outro (especifique)

***2. Selecione a atividade desempenhada na organização:**

- Diretoria (Presidente, Vice-Presidente, Dono...)
- Gerente - TI
- Gerente – Segurança da Informação
- Gerente – Suporte
- Analista - TI
- Analista – Segurança da Informação
- Analista – Suporte
- Consultor
- Professor
- Estudante
- Pesquisador

Outro (especifique)

Figura 6.5: Primeira parte do questionário - Área de atuação da organização e atividade desempenhada.

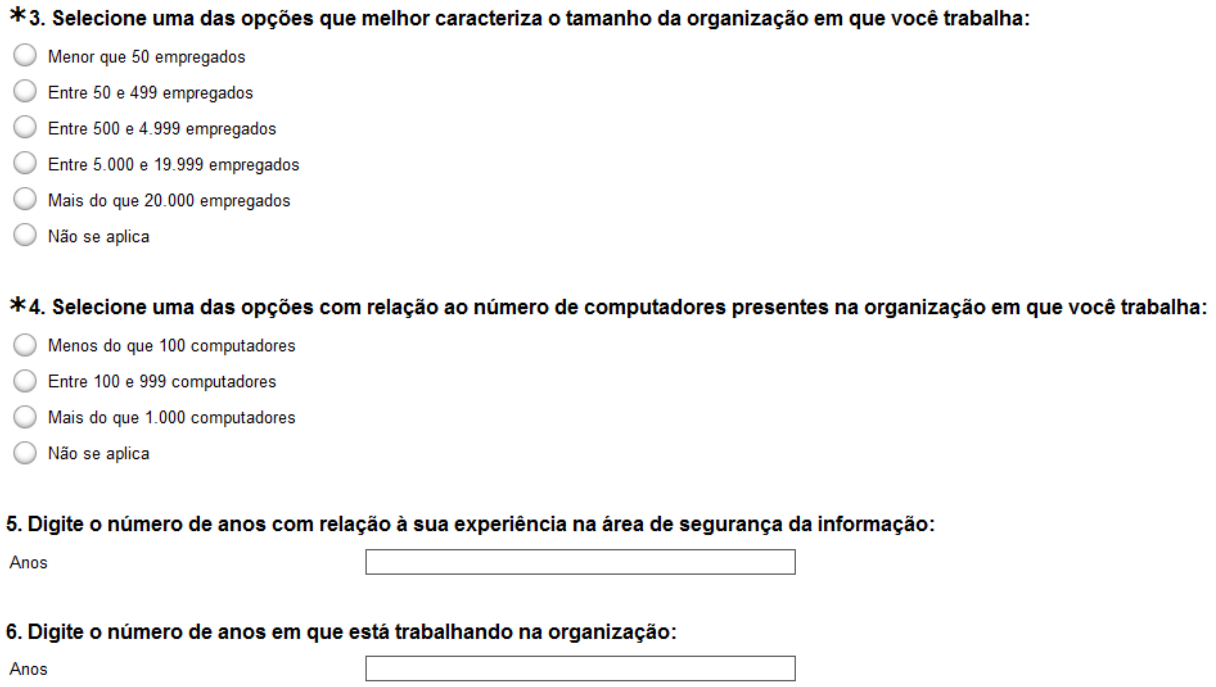


Figura 6.6: Segunda parte do questionário - Caracterização do local de trabalho e experiência profissional.

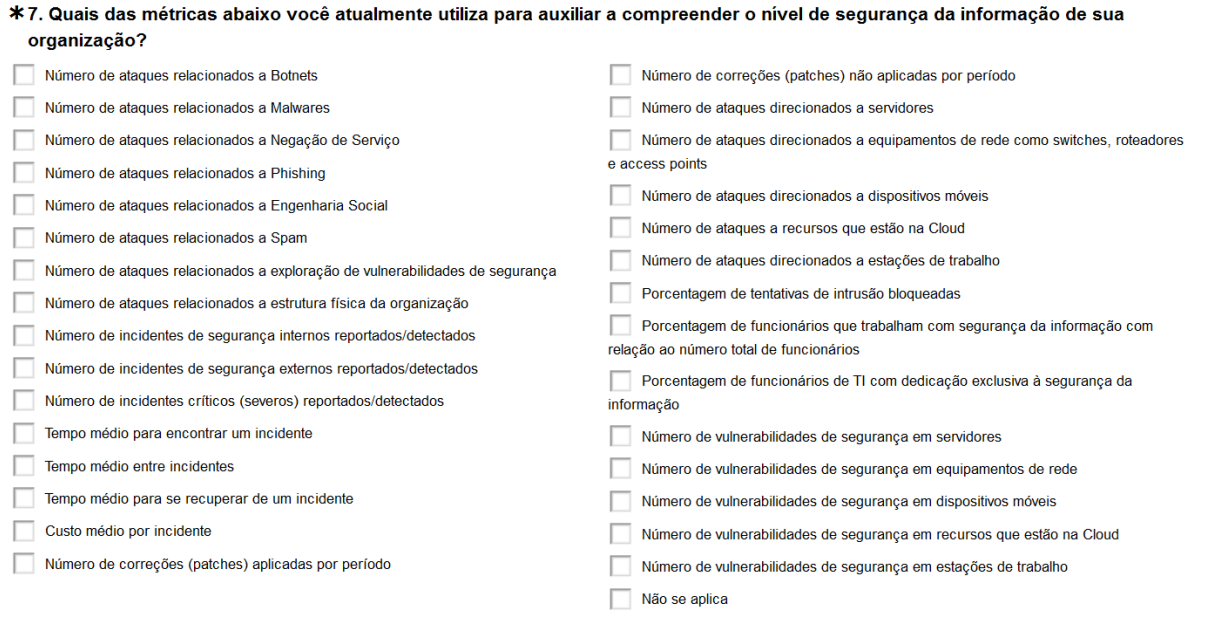


Figura 6.7: Terceira parte do questionário - Seleção das métricas.

***8. Em uma escala de 1 a 5 (com 5 para mais importante), analise as métricas de acordo com a sua importância em avaliar o nível de segurança da organização:**

	1	2	3	4	5
Número de ataques relacionados a Botnets	○	○	○	○	○
Número de ataques relacionados a Malwares	○	○	○	○	○
Número de ataques relacionados a Negação de Serviço	○	○	○	○	○
Número de ataques relacionados a Phishing	○	○	○	○	○
Número de ataques relacionados a Engenharia Social	○	○	○	○	○
Número de ataques relacionados a Spam	○	○	○	○	○
Número de ataques relacionados a exploração de vulnerabilidades de segurança	○	○	○	○	○
Número de ataques relacionados a estrutura física da organização	○	○	○	○	○
Número de incidentes de segurança internos reportados/detectados	○	○	○	○	○
Número de incidentes de segurança externos reportados/detectados	○	○	○	○	○
Número de incidentes críticos (severos) reportados/detectados	○	○	○	○	○
Tempo médio para encontrar um incidente	○	○	○	○	○
Tempo médio entre incidentes	○	○	○	○	○
Tempo médio para se recuperar de um incidente	○	○	○	○	○
Custo médio por incidente	○	○	○	○	○
Número de correções (patches) aplicadas por período	○	○	○	○	○
Número de correções (patches) não aplicadas por período	○	○	○	○	○
Número de ataques direcionados a servidores	○	○	○	○	○
Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	○	○	○	○	○
Número de ataques direcionados a dispositivos móveis	○	○	○	○	○
Número de ataques a recursos que estão na Cloud	○	○	○	○	○
Número de ataques direcionados a estações de trabalho	○	○	○	○	○
Porcentagem de tentativas de intrusão bloqueadas	○	○	○	○	○
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	○	○	○	○	○
Porcentagem de funcionários de TI com dedicação exclusiva à segurança da informação	○	○	○	○	○
Número de vulnerabilidades de segurança em servidores	○	○	○	○	○
Número de vulnerabilidades de segurança em equipamentos de rede	○	○	○	○	○
Número de vulnerabilidades de segurança em	○	○	○	○	○

Figura 6.8: Quarta parte do questionário - Avaliação da importância das métricas.

*** 9. Em uma escala de 1 a 5 (com 5 para mais complexo), avalie as métricas de acordo com a complexidade de sua utilização:**

	1	2	3	4	5
Número de ataques relacionados a Botnets	○	○	○	○	○
Número de ataques relacionados a Malwares	○	○	○	○	○
Número de ataques relacionados a Negação de Serviço	○	○	○	○	○
Número de ataques relacionados a Phishing	○	○	○	○	○
Número de ataques relacionados a Engenharia Social	○	○	○	○	○
Número de ataques relacionados a Spam	○	○	○	○	○
Número de ataques relacionados a exploração de vulnerabilidades de segurança	○	○	○	○	○
Número de ataques relacionados a estrutura física da organização	○	○	○	○	○
Número de incidentes de segurança internos reportados/detectados	○	○	○	○	○
Número de incidentes de segurança externos reportados/detectados	○	○	○	○	○
Número de incidentes críticos (severos) reportados/detectados	○	○	○	○	○
Tempo médio para encontrar um incidente	○	○	○	○	○
Tempo médio entre incidentes	○	○	○	○	○
Tempo médio para se recuperar de um incidente	○	○	○	○	○
Custo médio por incidente	○	○	○	○	○
Número de correções (patches) aplicadas por período	○	○	○	○	○
Número de correções (patches) não aplicadas por período	○	○	○	○	○
Número de ataques direcionados a servidores	○	○	○	○	○
Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	○	○	○	○	○
Número de ataques direcionados a dispositivos móveis	○	○	○	○	○
Número de ataques a recursos que estão na Cloud	○	○	○	○	○
Número de ataques direcionados a estações de trabalho	○	○	○	○	○
Porcentagem de tentativas de intrusão bloqueadas	○	○	○	○	○
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	○	○	○	○	○
Porcentagem de funcionários de TI com dedicação exclusiva à segurança da informação	○	○	○	○	○
Número de vulnerabilidades de segurança em servidores	○	○	○	○	○
Número de vulnerabilidades de segurança em equipamentos de rede	○	○	○	○	○
Número de vulnerabilidades de segurança em dispositivos móveis	○	○	○	○	○
Número de vulnerabilidades de segurança em recursos que estão na Cloud	○	○	○	○	○

Figura 6.9: Quinta parte do questionário - Avaliação da complexidade das métricas.

10. Cite outras métricas que podem ser utilizados para avaliar o nível de segurança da informação de uma organização:

Anter. Próx.

Ativados pela SurveyMonkey
Crie seus próprios questionários online gratuitos agora!

Figura 6.10: Sexta parte do questionário - Espaço para citar outras métricas.

Apêndice D - Resultados do questionário

Neste apêndice serão apresentadas as respostas das perquntas 7, 8 e 9 do questionário proposto.

Métrica	Resultado (Participantes que selecionaram a métrica)
Número de ataques relacionados a Spam	23
Número de ataques relacionados a Negação de Serviço	21
Número de incidentes de segurança internos reportados/detectados	21
Número de vulnerabilidades de segurança em servidores	20
Número de incidentes de segurança externos reportados/detectados	19
Número de ataques direcionados a servidores	18
Número de ataques relacionados a estrutura física da organização	16
Número de ataques relacionados a exploração de vulnerabilidades de segurança	16
Número de ataques relacionados a Malwares	16
Número de ataques relacionados a Phishing	15
Porcentagem de funcionários de TI com dedicação exclusiva à segurança da informação	15
Número de vulnerabilidades de segurança em equipamentos de rede	14
Número de incidentes críticos (severos) reportados/detectados	13
Tempo médio para se recuperar de um incidente	13
Número de ataques direcionados a estações de trabalho	12
Número de ataques relacionados a Engenharia Social	11
Número de vulnerabilidades de segurança em estações de trabalho	11
Porcentagem de tentativas de intrusão bloqueadas	10
Tempo médio para encontrar um incidente	10
Número de vulnerabilidades de segurança em dispositivos móveis	9
Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	8
Número de correções (patches) aplicadas por período	8
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	8
Tempo médio entre incidentes	8
Número de ataques relacionados a Botnets	7
Não se aplica	6
Custo médio por incidente	5
Número de ataques a recursos que estão na Cloud	5
Número de ataques direcionados a dispositivos móveis	5
Número de correções (patches) não aplicadas por período	5
Número de vulnerabilidades de segurança em recursos que estão na Cloud	4

Figura 6.11: Resultados da questão 7

Métrica	Resultado
Número de vulnerabilidades de segurança em servidores	3,87
Número de ataques direcionados a servidores	3,83
Número de incidentes críticos (severos) reportados/detectados	3,79
Número de incidentes de segurança internos reportados/detectados	3,79
Número de ataques relacionados a exploração de vulnerabilidades de segurança	3,74
Número de incidentes de segurança externos reportados/detectados	3,57
Tempo médio para encontrar um incidente	3,55
Número de ataques relacionados a estrutura física da organização	3,53
Tempo médio para se recuperar de um incidente	3,53
Número de vulnerabilidades de segurança em equipamentos de rede	3,49
Número de ataques relacionados a Phishing	3,43
Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	3,38
Número de ataques relacionados a Negação de Serviço	3,38
Número de ataques direcionados a estações de trabalho	3,34
Número de ataques relacionados a Malwares	3,34
Número de vulnerabilidades de segurança em estações de trabalho	3,32
Custo médio por incidente	3,21
Porcentagem de funcionários de TI com dedicação exclusiva à segurança da informação	3,21
Número de ataques relacionados a Engenharia Social	3,19
Porcentagem de tentativas de intrusão bloqueadas	3,19
Número de ataques relacionados a Spam	3,11
Tempo médio entre incidentes	3,09
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	3,06
Número de vulnerabilidades de segurança em dispositivos móveis	3,02
Número de ataques relacionados a Botnets	2,91
Número de vulnerabilidades de segurança em recursos que estão na Cloud	2,89
Número de correções (patches) aplicadas por período	2,87
Número de ataques a recursos que estão na Cloud	2,85

Figura 6.12: Resultados da questão 8

Métrica	Resultado
Número de ataques a recursos que estão na Cloud	3,55
Custo médio por incidente	3,43
Número de ataques direcionados a equipamentos de rede como switches, roteadores e access points	3,38
Tempo médio para encontrar um incidente	3,36
Tempo médio para se recuperar de um incidente	3,34
Número de ataques direcionados a dispositivos móveis	3,32
Número de vulnerabilidades de segurança em recursos que estão na Cloud	3,32
Número de ataques relacionados a Botnets	3,3
Número de ataques relacionados a exploração de vulnerabilidades de segurança	3,3
Número de vulnerabilidades de segurança em dispositivos móveis	3,28
Número de ataques relacionados a Engenharia Social	3,26
Número de incidentes críticos (severos) reportados/detectados	3,23
Tempo médio entre incidentes	3,19
Número de vulnerabilidades de segurança em servidores	3,19
Número de ataques direcionados a servidores	3,17
Número de ataques relacionados a Negação de Serviço	3,15
Número de vulnerabilidades de segurança em estações de trabalho	3,13
Número de incidentes de segurança externos reportados/detectados	3,11
Número de vulnerabilidades de segurança em equipamentos de rede	3,11
Número de ataques relacionados a estrutura física da organização	3,04
Número de incidentes de segurança internos reportados/detectados	3,02
Número de ataques direcionados a estações de trabalho	2,98
Número de correções (patches) não aplicadas por período	2,96
Número de ataques relacionados a Malwares	2,89
Número de correções (patches) aplicadas por período	2,89
Número de ataques relacionados a Phishing	2,87
Porcentagem de tentativas de intrusão bloqueadas	2,83
Número de ataques relacionados a Spam	2,77
Porcentagem de funcionários que trabalham com segurança da informação com relação ao número total de funcionários	2,49
Porcentagem de funcionários de TI com dedicação exclusiva à segurança da informação	2,38

Figura 6.13: Resultados da questão 9