UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E COMPUTAÇÃO

Rodrigo Sanches Miani

Aplicação de métricas à análise de segurança em Redes Metropolitanas de Acesso Aberto

Campinas, SP
2009

Rodrigo Sanches Miani

Aplicação de métricas à análise de segurança em Redes Metropolitanas de Acesso Aberto

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

Orientador: Leonardo de Souza Mendes

Campinas, SP
2009

Rodrigo Sanches Miani

Aplicação de métricas à análise de segurança em Redes Metropolitanas de Acesso Aberto

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

Banca Examinadora:
Prof. Dr. Leonardo de Souza Mendes - UNICAMP
Prof. Dr. Paulo Cardieri - UNICAMP
Prof. Dr. Waldeck Schützer - UFSCar

Campinas, SP
2009

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

M58a

Miani, Rodrigo Sanches
Aplicação de métricas à análise de segurança em redes metropolitanas de acesso aberto / Rodrigo Sanches Miani. --Campinas, SP: [s.n.], 2009.

Orientador: Leonardo de Souza Mendes.
Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Tecnologia da informação - Medidas de segurança. I. Mendes, Leonardo de Souza. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Metrics application in metropolitan broadband access network security analysis
Palavras-chave em Inglês: Information technology - Security measures
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Waldeck Schützer, Paulo Cardieri
Data da defesa: 05/03/2009
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Rodrigo Sanches Miani

Data da Defesa: 5 de março de 2009

Título da Tese: "Aplicação de Métricas à Análise de Segurança em Redes Metropolitanas de Acesso Aberto"

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

Prof. Dr. Waldeck Schutzer: _____

Prof. Dr. Paulo Cardieri: _____

Aos meus pais, João e Rosa

Agradecimentos

A Deus.

A toda a minha família. Em especial a meus pais, os grandes batalhadores João e Rosa. Obrigado pelo imenso esforço prestado na educação dos seus filhos. Sem esse esforço, carinho e dedicação nada disso seria possível. Vocês são minha grande inspiração.

Ao meu orientador Prof. Dr. Leonardo de Souza Mendes, pela confiança creditada e por todo o suporte dado durante os anos do mestrado. Obrigado pelas inúmeras oportunidades oferecidas. Devo uma grande parte de meu amadurecimento profissional e pessoal a você! E que venha o doutorado!

Aos colegas de trabalho: Meire, Maurício e Gean. Grandes companheiros que também fizeram parte desta caminhada.

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

Ao amigo Bruno Zarpelão, o meu co-orientador "extra-oficial" e grande conselheiro. Obrigado pelas dicas, correções, idéias, críticas... Enfim, por todo o esforço gasto com esta dissertação. Este trabalho também é seu!

Aos demais colegas de laboratório: Márlon, Geraldo, Dherik, Henrique, Lívia, Sérgio, Cubas, Zanoni, Ekler, Felipe, BrunoTx e Daniel. Os bons (e os maus!) momentos no Harpia nunca serão esquecidos!

A Prefeitura de Pedreira, pelo apoio e disposição com as informações disponibilizadas. Em especial ao colega Mateus, que com seus vastos conhecimentos sobre a rede, aliado ao seu bom-humor, foi fundamental para a realização da árdua tarefa de coletar os dados.

Aos professores Waldeck Schützer e Paulo Cardieri, membros da banca corretora. Pelas valiosas sugestões e dicas dadas durante o desenvolvimento deste trabalho.

Em especial a minha companheira e namorada Elisa. Graças a você que fiz a dura escolha de fazer mestrado e graças a você que nunca desisti! O tempo me mostrou o que você já sabia... Fizemos a escolha certa! Obrigado pelos conselhos, pelo carinho e por você ser essa pessoa que me faz tão bem e que me faz realizar coisas inimagináveis!

Ao Projeto Harpia, pelo apoio financeiro.

Resumo

As questões relacionadas à garantia de segurança influenciam diretamente o sucesso da implantação de redes metropolitanas de acesso aberto. Dessa forma, são necessários métodos eficientes para analisar a segurança destas redes em todos os níveis (organizacional, físico e de sistemas), a fim de propor soluções e implementar melhorias. Nossa proposta consiste em criar métricas de segurança específicas para as redes metropolitanas de acesso aberto que visam medir a eficiência dos programas de segurança e apoiar o planejamento das ações contra os problemas detectados. Este trabalho apresenta um conjunto de doze métricas de segurança para tais redes e os parâmetros para a sua definição, tais como dois modelos para o cálculo do indicador de segurança de uma métrica. Também serão apresentados os resultados obtidos com a aplicação de tais métricas para o estabelecimento de políticas de segurança na rede metropolitana de acesso aberto de Pedreira, cidade localizada no interior do estado de São Paulo. Os resultados mostraram que a aplicação de métricas bem definidas pode ser eficiente na detecção de vulnerabilidades e correção de problemas de segurança.

Palavras-chave: Redes metropolitanas de acesso aberto, Métricas de segurança, Segurança de redes, Análise de segurança.

Abstract

Information security has direct influence on any successful deployment of metropolitan broadband access networks. Efficient methods are required for security analysis of metropolitan networks in all levels: organization, structure and system. This work proposes the development and application of specific security metrics for metropolitan broadband access networks that aim to measure the efficiency of security programs and support action planning against detected problems. The approach presented in this work show metrics developed for these networks and parameters for metrics definition, such as a model for calculation of a security indicator of a metric. This paper also presents results achieved from application of the metrics reported here to establish security policies in the metropolitan broadband access network of Pedreira, a city located in the state of São Paulo, Brazil. These results show that well formed security metrics can be efficient in vulnerability detection and solutions of security issues.

Keywords: Metropolitan Broadband Access Networks, Security Metrics, Network Security, Security Analysis.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas

Abreviaturas em ordem alfabética.

ACL - *Access Control List*

ADSL - *Asymmetric Digital Subscriber Line*

CERT - *Computer Emergency Response Team*

CVSS - *Common Vulnerability Scoring System*

GNU/GPL - *GNU General Public License*

IDS - *Intrusion Detection System*

IEEE - *Institute of Electrical and Electronics Engineers*

IP - *Internet Protocol*

MAN - *Metropolitan Area Network*

NAT - *Network Address Translation*

NIST - *National Institute of Standards and Technology*

PIN - *Personal Identification Number*

SANS - *SysAdmin, Audit, Network, Security*

SQL - *Structured Query Language*

SSID - *Service Set Identifier*

TCP - *Transmission Control Protocol*

VLAN - *Virtual Local Area Network*

VoIP - *Voice Over Internet Protocol*

VPN - *Virtual Private Network*

WEP - *Wired Equivalent Privacy*

WPA - *Wi-Fi Protected Access*

Trabalhos Publicados Pelo Autor

1. Rodrigo S. Miani, Bruno B. Zarpelão, Leonardo de Souza Mendes and Mario L. Proença Jr. "Metrics Application in Metropolitan Broadband Access Network Security Analysis". *International Conference on Security and Cryptography* (SECRYPT 2008), Porto, Portugal, p. 473-476, Julho 2008.

Capítulo 1

Introdução

A evolução tecnológica exige o estabelecimento de redes de alta velocidade seja nas redes locais ou metropolitanas. O surgimento de novas demandas tais como o uso de voz sobre IP (VoIP), requisitos de segurança da informação e mobilidade, acabam por impactar na qualidade dos serviços prestados, culminando com a necessidade de aumentos consideráveis na velocidade de transmissão de dados tanto nas redes metropolitanas quanto nas redes locais [6].

Assim como a evolução tecnológica, mudanças significativas ocorreram nas estruturas da administração pública das prefeituras municipais. A municipalização de setores como o da saúde e a descentralização física e lógica da administração pública municipal, criaram novas demandas aos municípios, como por exemplo, a necessidade de intercomunicação de secretarias municipais ou então dos postos de saúde que estão espalhados pelo município. Um exemplo é o Sistema Municipal de Saúde (SMS) que é responsável por gerir toda a distribuição de medicamentos a todas as Unidades Básicas de Saúde (UBS) espalhadas pela cidade. Dessa forma, torna-se imprescindível o uso de sistemas de comunicação que interliguem todas estas unidades descentralizadas da prefeitura [7].

Uma alternativa viável e promissora para os municípios é a implantação de sistemas de comunicação próprios, utilizando-se as Redes Metropolitanas de Acesso Aberto (*Metropolitan Broadband Access Networks* - MBANs). As Redes Metropolitanas de Acesso Aberto, que também podem ser encontradas na literatura como Infovias Municipais ou Redes Municipais, nada mais são do que caminhos por onde trafegam as informações, com alta capacidade de transmissão e agregação de diferentes tipos de informação [7]. A MBAN compreende toda a infra-estrutura de comunicações necessária para possibilitar ao município a interligação de suas unidades através de uma rede de alta velocidade, sobre a qual irá operar um ambiente de comunicações baseado nos protocolos TCP/IP.

Apesar dos benefícios que uma MBAN pode proporcionar a um município, devemos ficar atentos aos problemas relacionados à segurança da informação neste tipo de rede. Novos desafios são impostos aos analistas de segurança por duas razões principais: o caráter multisserviço da rede metropolitana de acesso aberto leva à manipulação de dados sigilosos da prefeitura e da população e a universalização desejada faz com que a quantidade de usuários atinja níveis elevados.

Considere os seguinte cenários, comumente encontrados nas Infovias Municipais:

1. Pontos de acesso espalhados pela cidade com a função de disponibilizar serviços digitais ao cidadão;

2. Prédios públicos e da iniciativa privada utilizando-se da mesma estrutura e conexões de rede;

3. Distribuição de Internet para os prédios públicos e para população.

Para cada um destes cenários têm-se os seguintes problemas de segurança:

1. Pontos de acesso configurados com senhas "fracas" e sem a utilização de protocolos criptográficos;

2. Informação confidencial da prefeitura trafegando sem criptografia;

3. Uso abusivo da Internet distribuída.

Os gestores das redes metropolitanas de acesso aberto devem ser responsáveis por identificar as vulnerabilidades de segurança da rede e propor a implementação de controles para as falhas. Porém, o alto número de conexões e usuários, a segmentação da rede e o caráter multisserviço das MBANs, dificultam a tarefa de detecção desses problemas. São necessários então métodos específicos para o tratamento da segurança da informação nas redes metropolitanas de acesso aberto.

Um conceito atualmente difundido no escopo da segurança da informação é o de métrica de segurança. Métricas podem ser definidas como um grupo de medidas que geram uma abordagem quantitativa sobre um determinado problema. O objetivo primário de uma métrica é transformar dados brutos em informações passíveis de análise. Grandes organizações do mundo da segurança da informação como CERT (*Computer Emergency Response Team*) [8], SANS (*SysAdmin, Audit, Network, Security*) [9] e NIST (*National Institute of Standards and Technology*) [10] recomendam a implementação de programas de métricas de segurança nas corporações.

Dessa forma, a visualização dos problemas em uma rede metropolitana de acesso aberto pode ser facilitada com o desenvolvimento de um programa de implementação de métricas de segurança. Considere como exemplo, cada um dos cenários descritos anteriormente. A detecção de problemas, assim como a análise da eficiência dos controles de segurança implementados, em cada um dos cenários poderia ser feita realizando as seguintes medições na rede:

1. Número de pontos de acesso que não utilizam senha para autenticação, complexidade das senhas por ponto de acesso e protocolos de segurança habilitados por ponto de acesso;

2. Número de prédios sem proteção criptográfica entre as conexões, controles de acesso lógico por prédio (firewalls, *access lists*);

3. Taxa de utilização de banda de Internet por prédio.

Através da coleta e análise criteriosa dos dados acima, o nível atual de segurança de cada cenário pode ser mensurado corretamente, direcionando as ações tomadas pelos administradores da rede.

Em [11] são descritas potenciais vulnerabilidades de segurança que podem ocorrer nas redes metropolitanas de acesso aberto, assim como recomendações para o tratamento destes problemas. As vulnerabilidades são discutidas e classificadas em três grandes grupos: exploração de confiança, análise de tráfego/ataques de rede e reconhecimento da rede. Além das métricas, medidas preventivas como políticas de segurança específicas e avaliação dos riscos são citadas como parte das recomendação para o tratamento das vulnerabilidades de segurança em redes municipais.

1.1 Segurança da informação

O aumento do número de falhas em componentes, de vulnerabilidades descobertas em softwares e de ataques às redes de comunicações fazem com que haja uma preocupação crescente com as questões relacionadas à segurança da informação. Dados estatísticos sobre incidentes de segurança reportados no Brasil apontam esse crescimento e incentivam o estudo e desenvolvimento da segurança da informação. As Figuras 1.1 e 1.2 a seguir ilustram o crescimento de incidentes de segurança no Brasil a partir do início do ano 2000.

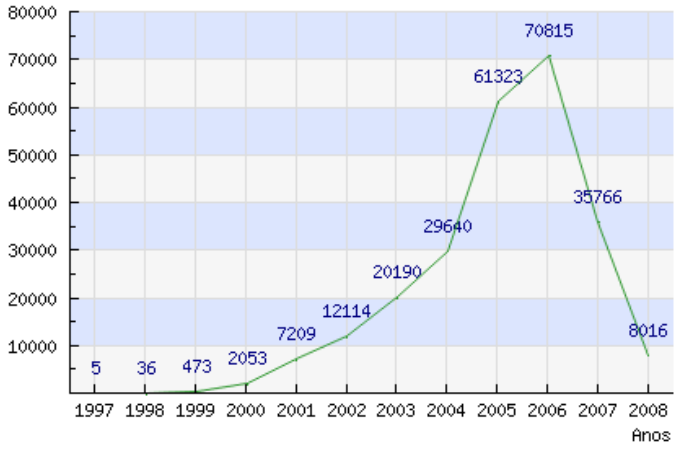

Fig. 1.1: Incidentes reportados ao CAIS por ano. Extraído de [1]

Os dados do gráfico 1.1 foram obtidos pelo CAIS (Centro de Atendimento a Incidentes de Segurança) que desde 1997 atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira [1]. O gráfico diz respeito ao número de incidentes na rede acadêmica brasileira reportado ao CAIS, no período entre 1997 a março de 2008.

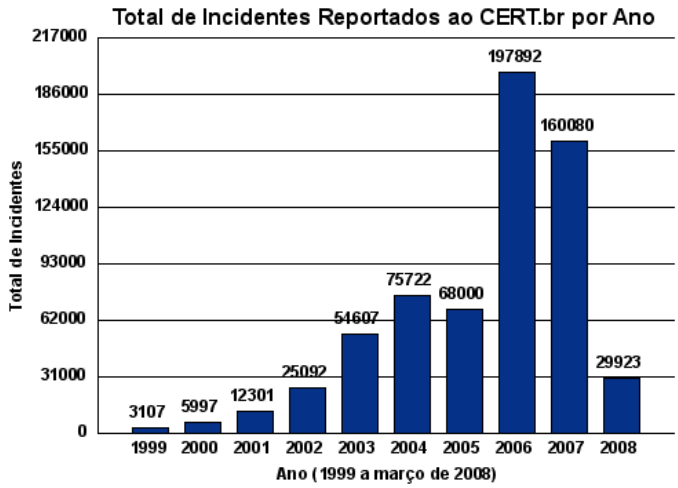

Fig. 1.2: Incidentes reportados ao CERT por ano. Extraído de [2]

Já os dados do gráfico 1.2 obtidos pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) representam os incidentes de segurança envolvendo redes conectadas à Internet em todo Brasil [2]. O CERT.br é o grupo de resposta a incidentes de segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.

Os dados de ambos os gráficos mostram que desde o fim dos anos 90 e até o ano de 2006 os incidentes de segurança cresceram de forma assustadora. A revolução digital e o crescimento das vendas de computadores, aliada a falta de informação são alguns dos fatores que podem explicar este crescimento. Porém, em 2007 esse número caiu e as expectativas para 2008 também indicam que os valores alcançados até o ano 2006 dificilmente se repetirão. Isto se deve, em especial, a quatro fatores: maior capacidade de identificação dos sistemas comprometidos e a conseqüênte redução do número de "falsos-positivos", preocupação crescente das instituições acadêmicas, empresas e institutos de pesquisas em preservarem a operação e a integridade das suas redes, o aumento na disseminação da informação sobre segurança digital e finalmente o aumento de investimentos em soluções de segurança. De acordo com o estudo da Frost & Sullivan [12], 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.

De acordo com a norma NBR ISO/IEC 17799 [13], que é uma versão em português da norma britânica que trata de práticas para a gestão da segurança da informação, a informação é um ativo que tem um valor para a organização e conseqüêntemente necessita ser adequadamente protegido. A segurança da informação protege diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

A garantia da segurança da informação é dada pela preservação dos seguintes atributos [13], [14]:

- Confidencialidade - garantia de que a informação é accessível somente para entidades autorizadas pelo proprietário da informação;
- Integridade - garantia de que a informação manipulada mantenha as características originais estabelecidas pelo proprietário da informação;
- Disponibilidade - garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário.

Geus e Nakamura [15] citam exemplos de falhas que, se exploradas corretamente, podem comprometar a segurança de sistemas da informação:

- Exploração de vulnerabilidades em sistemas operacionais, aplicativos, protocolos e serviços. Exemplos: falhas em sistemas operacionais como Windows podem permitir a execução remota de códigos maliciosos [15] e o protocolo TCP pode sofrer ataques conhecidos como SYN *flood* [16].
- Exploração dos aspectos humanos dos envolvidos. Exemplos: utilização de senhas ineficientes, engenharia social [15].
- Falha no desenvolvimento e implementação da política de segurança. Exemplos: elaboração de política de segurança que não prevê o uso cópias de segurança (*backups*).

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

1.2 Contribuições da dissertação

O objetivo deste trabalho é o desenvolvimento de um programa de implementação de métricas de segurança em redes metropolitanas de acesso aberto, capaz de mensurar com eficiência os diversos aspectos de segurança da rede auxiliando o desenvolvimento sustentável das MBANs. As principais contribuições desta dissertação são:

- Definição de um modelo para a criação de métricas de segurança para redes metropolitanas de acesso aberto;
- Padronização da nomenclatura dos termos relativos a métricas de segurança;
- Criação de um modelo para o cálculo das fórmulas de uma métrica de segurança;
- Criação de indicadores de segurança para as métricas, baseados no cálculo da sua fórmula;
- Apresentação de doze métricas de segurança para MBANs;
- Definição de um modelo para a análise dos dados coletados;
- Resultados da aplicação de métricas propostas nesta dissertação na rede metropolitana de acesso aberto de Pedreira, SP.

1.3 Estrutura da dissertação

O capítulo 2 apresenta os conceitos básicos de uma rede metropolitana de acesso aberto suas vantagens, aplicações, motivações para o estudo da segurança da informação e alguns exemplos de implantações com sucesso de tais redes. Apresenta também uma proposta de classificação para MBANs com objetivo de agrupar os diversos problemas de segurança possivelmente encontrados em áreas comuns.

O capítulo 3 contém definições e exemplos de métricas de segurança. Quais as vantagens e desvantagens em sua aplicação e as motivações para o tratamento quantitativo da segurança de uma rede.

O capítulo 4 apresenta a metodologia de construção das métricas de segurança para redes metropolitanas de acesso aberto, a modelagem do cálculo da fórmula de uma métrica e as doze métricas de segurança para MBANs.

O capítulo 5 apresenta a metodologia para a coleta e análise dos dados das métricas de segurança para MBANs.

O capítulo 6 detalha o estudo de caso da aplicação das técnicas apresentadas nesta dissertação na rede metropolitana de Pedreira, SP.

O capítulo 7 apresenta as considerações finais e sugestões para trabalhos futuros.

Capítulo 2

Redes metropolitanas de acesso aberto

O objetivo desse capítulo é descrever os conceitos básicos de uma rede metropolitana de acesso aberto. Serão apresentados os benefícios que uma MBAN pode trazer ao município, assim como as aplicações disponibilizadas sobre ela e exemplos de implantações com sucesso de redes metropolitanas de acesso aberto. Por fim, será proposto um modelo de classificação de MBANs com objetivo de agrupar os diversos problemas de segurança possivelmente encontrados em áreas comuns.

2.1 Definição

As redes metropolitanas de acesso aberto podem ser definidas como a convergência dos serviços, das aplicações e da infra-estrutura da rede de comunicações comunitária de um município. Elas representam vias públicas da informação, caracterizadas pela alta capacidade de transmissão e agregação de dados de diferentes naturezas [7]. A construção e manutenção das MBANs passam a fazer parte da demanda de infra-estrutura do município tal qual a construção de ruas e avenidas, das redes de água e esgoto ou da rede de energia elétrica.

As MBANs diferem das redes de comunicações convencionais pelo seu caráter universalizante e por serem uma rede multiserviço, que possibilitaria a distribuição de todos os serviços oferecidos separadamente pelos sistemas atuais. Isto significa que ela é capaz de tratar com igual eficiência tanto o tráfego de dados como os de telefonia, vídeo e áudio.

O principal objetivo deste paradigma de comunicações é estabelecer um ambiente de comunicação que leve à modernização do município. Essa infra-estrutura tem como uma de suas grandes vantagens a possibilidade de convergência e democratização dos diferentes meios de comunicação e informação, permitindo o fluxo de dados multimídia tais como imagens médicas, video-conferência, educação à distância (*e-learning*), bancos de dados educacionais e serviços de transporte de voz para comunicação interna (VoIP) em um único ambiente de acesso livre para os cidadãos [6].

A implantação de MBANs promove impactos econômicos e sociais em todos os setores da gestão de um município pois, ao possuir um sistema próprio de comunicações há economia de recursos que poderão ser investidos em outras áreas. Os custos administrativos podem ser reduzidos com o uso de ferramentas computacionais. Além disso o salto tecnológico que uma MBAN pode causar na gestão do município motiva a inclusão digital.

Porém, a implantação em larga escala de uma MBAN representa um investimento muito alto, o

qual habitualmente não está disponível nas prefeituras. Uma alternativa que algumas prefeituras têm optado é a implantação inicial da MBAN em pontos prioritários para depois expandir os nós da rede utilizando tecnologias mais econômicas como por exemplo redes sem fio *wi-fi*.

Tradicionalmente, as redes metropolitanas de acesso aberto podem ser baseadas em quatro tecnologias de rede: fibras ópticas, acessos sem-fio, acessos dedicados (ADSL e *Frame Relay*) ou então híbrida. A escolha por uma destas opções passa por diversas considerações, incluindo a limitação de recursos e as demandas por banda que serão exigidas do sistema. Já do ponto de vista do modelo lógico de operação da rede, a tecnologia de interconexão de rede utilizada é a *Ethernet* [17]. O protocolo de comunicação utilizado entre os nodos da rede em uma MBAN é o TCP/IP.

A Figura 2.1 ilustra um exemplo de uma MBAN e sua respectiva estrutura física. Aqui, a rede é composta por prédios públicos (prefeitura, delegacia, hospital e escola) e residências. A tecnologia de rede utilizada neste caso é híbrida com o uso de enlaces ópticos e links de rádio.

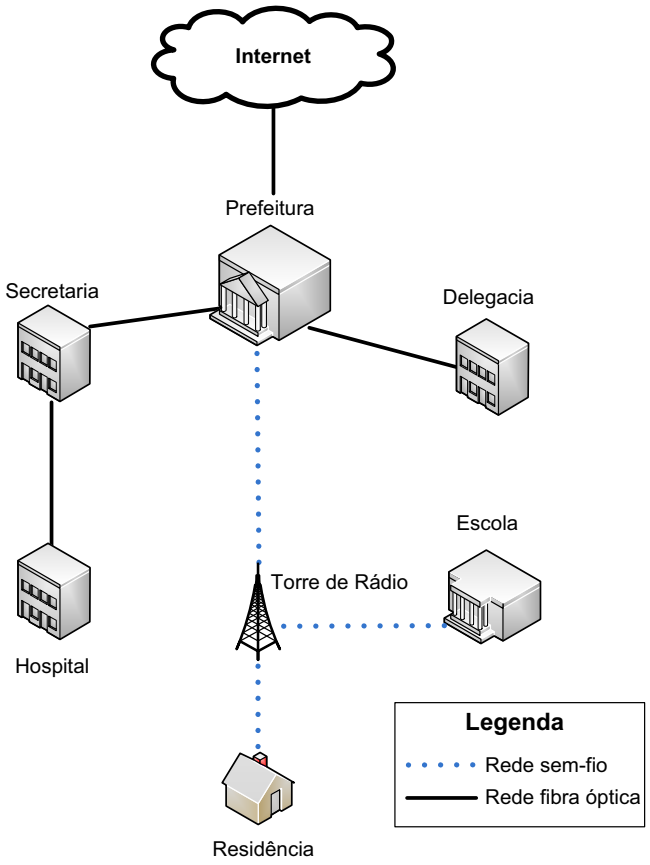

Fig. 2.1: Exemplo de rede metropolitana de acesso aberto

2.2 Aplicações

Uma motivação econômica para a implantação de uma rede metropolitana de acesso aberto é a possibilidade do munícipio se transformar em provedor de serviços de acesso às comunicações, criando novas alternativas em captações de recursos. Por ser uma rede construída sobre o protocolo

TCP/IP, virtualmente qualquer aplicação desenvolvida para essa plataforma pode operar em uma rede metropolitana de acesso aberto. A seguir alguns exemplos de aplicações que podem ser disponibilizadas pela MBAN:

- Acesso à Internet para população;
- VoIP corporativo;
- Sistema municipal de vigilância pública;
- Sistemas de gestão municipal ou *e-Gov*;
- Tele-medicina (*e-health*);

Acesso à Internet

A Internet é o elo de comunicação entre o município e o mundo externo. Podemos destacar a importância atual da Internet com relação à pesquisa de conteúdo e rapidez na divulgação da informação. Inserir o cidadão neste contexto, significa contribuir para a inclusão digital além de acelerar o processo de desenvolvimento do município. Outro exemplo é a possibilidade de atendimento via *e-mail*. Este serviço já substitui vários outros serviços outrora dependentes de processos tediosos e burocráticos, como SAC (serviço de atendimento ao consumidor) e *Call-centers*.

O acesso à Internet pode ser feito à partir de todos os pontos da rede metropolitana por meio do centro de distribuição da MBAN. O cenário tradicional é o prédio da Prefeitura, onde freqüêntemente o CPD (Central de Processamento de Dados) está localizado, funcionar como centro de distribuição. Geralmente um ou mais *links* de Internet são contratados e a prefeitura passa a funcionar como um provedor de acesso à Internet.

VoIP corporativo

Voz sobre IP, também chamado VoIP, significa o transporte da voz sob uma infra-estrutura IP tornando a transmissão de voz mais um dos serviços suportados pela rede de dados [18].

O principal objetivo da implantação do sistema de VoIP sobre uma MBAN, é o barateamento de custo devido ao uso de uma única rede para carregar dados e voz, que pode transportar dados VoIP sem custo adicional. Chamadas realizadas de VoIP para VoIP em geral são gratuitas, enquanto chamadas VoIP para as redes de telefonia convencional, podem ter custo para o utilizador VoIP. Um exemplo é a utilização de ramais VoIP para a comunicação interna e entre prédios ligados à administração pública, substituindo a telefonia convencional com economia de até 76% nas ligações [19].

Sistema municipal de vigilância pública

O sistema municipal de vigilância pública consiste de um ambiente integrado de coleta e análise de informação em tempo real para supervisão e vigilância de determinados locais no munícipio. O sistema é composto de câmeras, alarmes e central de monitoramento, todos interligados através da MBAN. Uma variante desse sistema é o programa de segurança de trânsito em tempo real, permitindo efetivo controle de tráfego em larga escala.

Sistemas de gestão municipal ou *e-Government*

A implantação de sistemas de gestão municipal em redes metropolitanas de acesso aberto possibilita a integração e o aproveitamento de informações entre as diferentes secretarias municipais. Sistemas de gestão específicos para cada setor do município podem ser desenvolvidos. São vários os benefícios para saúde, educação e administração municipal dentre os quais podemos destacar:

- Gestão e gerenciamento de almoxarifados;
- Gestão e gerenciamento de medicamentos;
- Integração de cadastros sociais;
- Prontuários digitais de atendimento;
- Educação digital - biblioteca digital, sistema de administração escolar e ensino apoiado por ferramentas tecnológicas;
- Implantação da transparência na gestão pública por meio do livre acesso a informações como prestações de contas, licitações eletrônicas e etc.

Tele-medicina (e-health)

Tele-medicina é o fornecimento de serviços de assistência médica, informações clínicas ou educação médica utilizando tecnlogias de telecomunicação. Existem dois tipos de serviços de tele-medicina: síncrono (aplicações em tempo real) e assíncrono (aplicações do tipo "store-and-forward", sem requisitos de tempo).

Algumas aplicações da tele-medicina que podem usar os recursos tecnológicos das redes metropolitanas de acesso aberto são [20]:

- Tele-diagnósticos;
- Tele-ultrasom;
- Tele-monitoração;
- Tele-consultas;

2.3 Exemplos

Nesta seção serão apresentados exemplos de implantações com sucesso de MBANs. Projetos de municípios que adotaram esta tecnologia de comunicação são encontrados em grande parte do mundo como América [21], [22] [23], Europa [24], [25], [26], Ásia [27] e Oceania [28]. A Tabela 2.1 mostra exemplos de cidades com a tecnologia de MBAN implantanda e as principais contribuições para o município.

Tab. 2.1: Exemplos de MBANs

Cidade	Tecnologia de rede	Contribuições
Patras, Grécia	Híbrida - Fibra óptica e sem fio	Interconexão de instituições de Educação, Pesquisa e Administração Pública.
Leiden, Holanda	Sem fio	Programa de distribição de vídeo, servidores de jogos e VoIP.
Kutztown, Estados Unidos	Fibra óptica	Fornecimento de conexões de fibra óptica de alta velocidade para residências, escolas, prédios públicos e privados;
Granbury, Estados Unidos	Sem fio	Criação de uma rede que une serviços de segurança pública (polícia, bombeiros e serviços de emergência) e da administração municipal.
Cheynne, Estados Unidos	Sem fio	Gerenciamento de controle de tráfego e trânsito.
Spokane, Estados Unidos	Sem fio	Aplicações de *e-Government*
Shangai, China	Híbrida - Fibra óptica e sem fio	Aplicações de *e-Government*, Informatização dos setores da Educação e Saúde, Implementação de sistema de pagamento eletrônico.
Pedreira, Brasil	Híbrida - Fibra óptica e sem fio	Interconexão de prédios públicos, distribuição de Internet para a população e VoIP corporativo.

Duas destas MBANs serão abordadas com maior nível de detalhes: Patras [25] e Leiden [24]. Patras por apresentar uma formação híbrida em sua tecnologia de rede e por interligar prédios com diferentes níveis de controle de acesso. Já Leiden foi escolhida por ser uma rede formada somente por conexões sem fio, uma tendência atual nas redes metropolitanas de acesso aberto devido a facilidade e seu baixo custo de implementação, quando comparado às redes constituídas por fibra óptica [29].

O objetivo aqui, além de elucidar conceitos e aplicações das MBANs, é motivar discussões acerca dos problemas de segurança da informação em MBANs.

MBAN de Patras

A cidade de Patras é situada na região oeste da Grécia e atualmente é a terceira maior cidade do país. A MBAN de Patras é constituída por 300 prédios públicos, dentre eles 3 universidades, 6 centros de pesquisa, 4 hospitais e 120 escolas. A tecnologia de interconexão é híbrida, formada por enlaces de fibra óptica e conexões sem fio.

A topologia da rede óptica de Patras é baseada em um modelo de três níveis: rede principal, rede de distribuição e rede de acesso. Os tipos de nós do sistema são, portanto, divididos em: nós principais, nós de distribuição e nós de acesso.

A rede principal consiste em um número de nós principais que são conectados diretamente entre si, formando o núcleo da rede.

A rede de distribuição forma a segundo nível do modelo. Um nó de distribuição deve ser conectado a um nó principal e também possuir uma conexão redundante com outro nó principal. Ou seja, as conexões entre os nós de distribuição e os nós principais respeitam a relação 2:1. Alternativamente os nós de distribuição podem ser conectados entre si, quando necessário.

O último nível do modelo é a rede de acesso. Os nós de acesso são conectados aos nós de distribuição e também a outros nós de acesso. Por fim, os prédios são conectados à rede de acesso.

A Figura 2.2 ilustra a arquitetura da rede óptica de Patras.

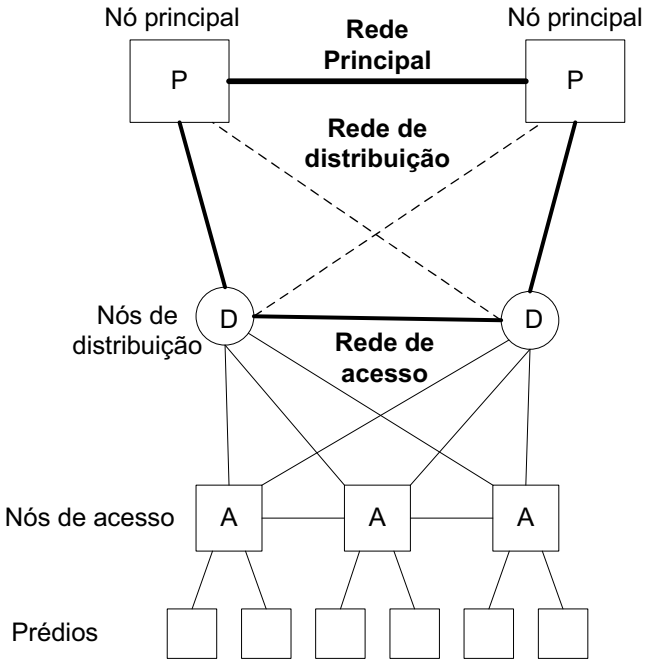

Fig. 2.2: Arquitetura da MBAN de Patras

A MBAN de Patras consiste de:

- 3 nós principais;
- 10 nós de distribuição;
- 30 nós de acesso;
- 9 nós de acesso sem fio;

Algumas considerações preliminares sobre a segurança da MBAN de Patras podem ser traçadas. Quatro tipos importantes de prédios estão conectados entre si: universidades, centro de pesquisas, hospitais e escolas. A confidencialidade e integridade dos dados que trafegam em toda MBAN devem ser garantidas. Um exemplo são os dados sigilosos de pacientes que não podem trafegar na rede a ponto de serem lidos por usuários em uma escola. Um modelo de segurança deve ser proposto com o propósito de cuidar desse tipo de vulnerabilidade.

Outro ponto está relacionado a disponibilidade e redundância dos dados. Note que o modelo de rede é flexível o suficiente para permitir conexões redundantes. Porém, medições e testes na rede são necessários para verificar as necessidades reais de tais conexões e assim alcançar um nível satisfatório de transmissão de dados que não comprometa a disponibilidade do sistema.

MBAN de Leiden

O projeto da MBAN de Leiden, uma cidade holandesa com aproximadamente 118.000 pessoas, originou-se de uma iniciativa de três moradores locais em criar uma pequena rede sem fio doméstica para a troca de dados. Assim que a primeira rede foi estabelecida, eles decidiram conectar mais nós e assim iniciou-se o plano de criação de uma rede municipal sem fio que atendesse intereses do munícipio e também da população. Atualmente escolas, bibliotecas, centros de saúde e residências de Leiden e outros sete munícipios vizinhos são conectados pela "Wireless Leiden" que é o nome dado ao projeto.

A grande diferença aqui é o modo com que é MBAN de Leiden é gerida. O projeto Wireless Leiden não possui fins lucrativos e é mantido por voluntários, doações e patrocínios de diversas organizações. A prefeitura de Leiden somente colabora com a isenção de taxas das locações.

A estrutura da MBAN de Leiden é baseada nos padrões IEEE 802.11b. A rede engloba mais de 100 nós, os quais roteiam tráfego entre si, entre os usuários e para Internet. Cada nó consiste de uma ou mais interfaces de comunicação para outros nós, e também de um ponto de acesso onde os usuários se conectam a MBAN utilizando uma antena externa. O acesso a Internet é realizado através de três *gateways* cada um com uma capacidade de 8mbps.

Os serviços disponibilizados pela "Wireless Leiden" incluem distribuição de vídeo de artistas locais, sincronização de tempo, servidores de jogos e VoIP.

Por se tratar de uma rede inteiramente sem fio, os riscos de segurança aumentam, pois se nas redes cabeadas um invasor tinha de ter pelo menos o acesso a um ponto da rede para acessar os pacotes, com as redes sem-fio esse requisito não é necessário. Basta que ele esteja dentro da área de cobertura para que os pacotes chegem até ele e assim seja possível ler, modificar ou inserir novos pacotes [15]. Portanto, os cuidados com a segurança da informação em uma rede sem-fio devem ser redobrados.

Considere um nó da MBAN de Leiden. Sabemos que os nós possuem dois tipos de interfaces de comunicação: uma para a comunicação entre os nós e a outra para a comunicação do usuário final com o ponto de acesso. A Figura 2.3 ilustra a situação.

Neste tipo de rede, diversos problemas de segurança podem ocorrer. Abaixo são listados alguns desses problemas.

- Usuário 1 e Usuário 2 estão conectados no mesmo ponto de acesso. A primeira vulnerabilidade de segurança que pode ser explorada é o Usuário 1 explorar o mesmo canal de conexão para capturar dados do Usuário 2 (ou vice-versa) ou até mesmo tomar controle de sua máquina. Ou

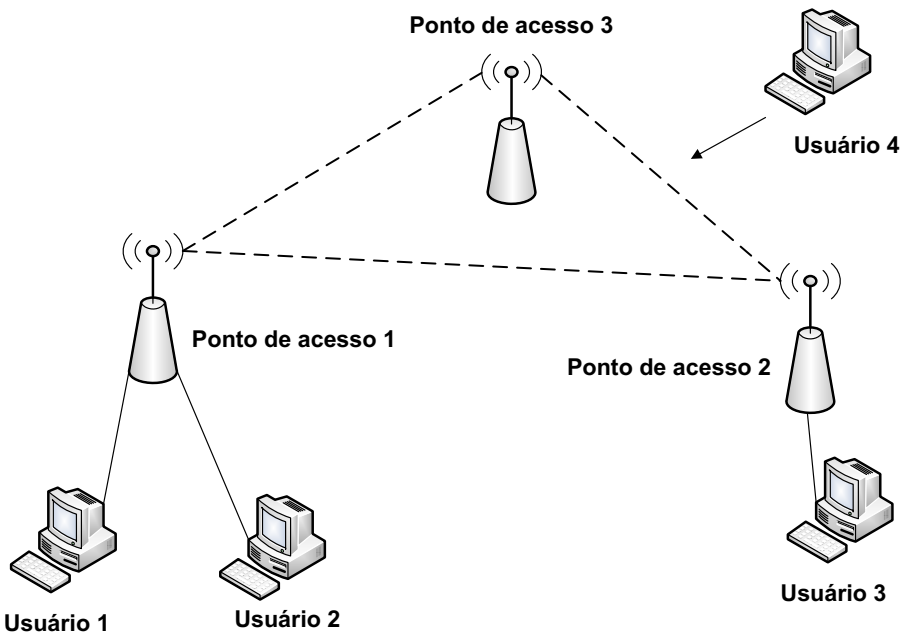

Fig. 2.3: Exemplos de acessos à MBAN de Leiden

seja, devem existir controles de acesso no ponto de acesso 1 que restrinja esse tipo de ataque, como por exemplo o isolamento do ponto de acesso através de um conjunto de regras de um *firewall*.

- Usuário 1 e Usuário 3 estão conectados em pontos de acesso distintos, porém não deve ser possível para o Usuário 1 à partir do ponto de acesso 1 obter qualquer tipo acesso ao computador do Usuário 2.
- Usuário 4 não é registrado para o acesso à MBAN de Leiden. Assim, ferramentas de controle de acesso devem impedir que um usuário não registrado consiga acesso a qualquer um dos pontos de acesso de Leiden.
- Por ser um usuário não registrado no domínio de Leiden, a leitura, manipulação ou troca de pacotes do Usuário 4 com qualquer outro usuário da rede incluindo o ponto de acesso, não deve ser possível. Este último caso ilustra a situação em que o Usuário 4 manipulando ferramentas de *sniffer* de rede, capture os dados que estão trafegando entre os pontos de acesso 2 e 3.

Existem tecnologias e boas práticas como a adoção de protocolos criptográficos como WPA [30], [31] e uso de senhas fortes que podem amenizar os problemas citados acima. Porém, o objetivo deste trabalho é somente mostrar a existência de vulnerabilidades de segurança em redes metropolitanas de acesso aberto e motivar o estudo da detecção das mesmas.

2.4 Classificação de uma MBAN

Vimos que as redes metropolitanas de acesso aberto podem ter diversas características como: ser constituídas de uma ou mais tecnologias de rede, possuir uma grande diversidade de serviços e abrigar

usuários de todos os setores do munícipio. Esssa flexibilidade na formação da rede proporciona os fundamentos para a definição de um modelo de classificação para as MBANs. Através da agregação de atributos em comum, o modelo de classificação facilita a compreensão das particularidades de MBANs.

Podemos classificar uma MBAN de acordo com o modelo de três camadas apresentado na Figura 2.4.

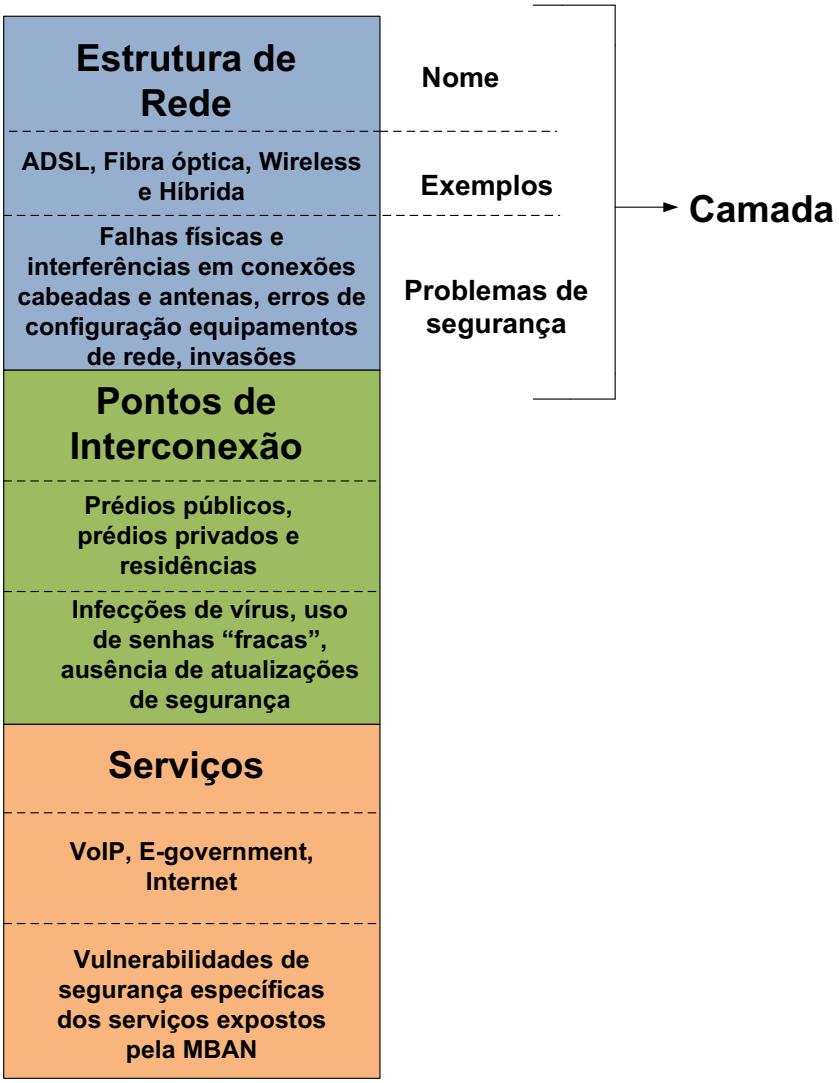

Fig. 2.4: Modelo três camadas - MBAN

Essa classificação possibilita a divisão dos problemas de segurança de acordo com cada uma das camadas da rede metropolitana de acesso aberto. Assim, têm-se um melhor entendimento sobre cada camada e seus respectivos problemas em potencial. As métricas aplicadas na segurança da MBAN que serão abordadas na seção 5 devem tratar as três camadas presentes na classificação apresentada.

Nas próximas subseções serão detalhadas as definições que envolvem cada uma das três camadas apresentadas.

2.4.1 Estrutura de Rede

Uma rede municipal pode ser baseada em quatro tecnologias: óptica, sem fio, acessos dedicados (ADSL e *Frame Relay* por exemplo) ou híbrida. A escolha por uma destas opções passa por diversos critérios incluindo a limitação de recursos e as demandas por capacidade de transmissão que serão exigidas do sistema. Esta categoria é importante na definição das métricas, pois algumas tecnologias, como as redes sem fio, podem trazer maiores problemas em relação à segurança.

Um exemplo é a Infovia da cidade de Pedreira, localizada no interior do estado de São Paulo, Brasil. O modelo de rede é híbrido e consiste de uma espinha-dorsal (*backbone*) de fibra óptica e pontos de rádio. Mais detalhes sobre a Infovia de Pedreira são expostos no capítulo 6. A Figura 2.5 mostra o mapa da cidade, onde em vermelho temos a conexão óptica e em amarelo as conexões de rádio:

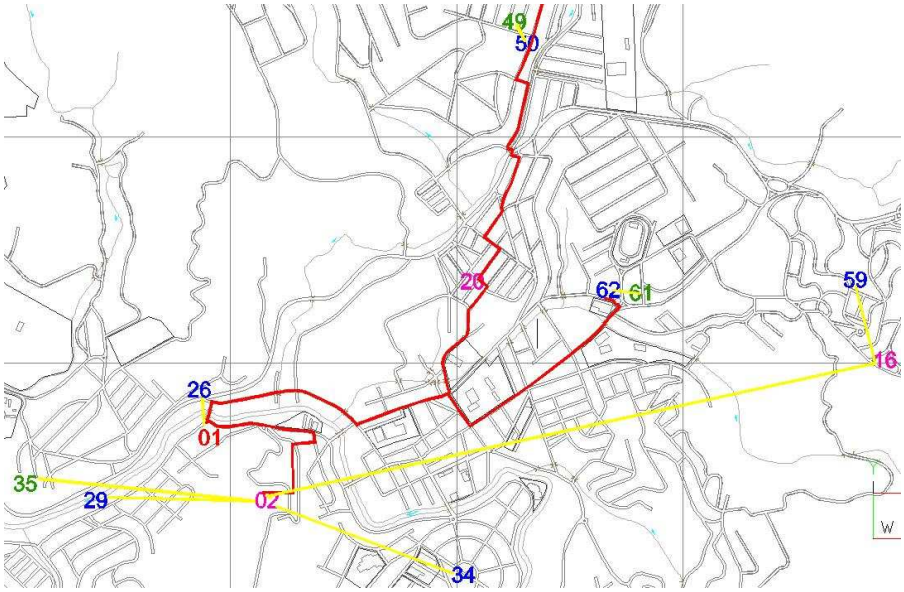

Fig. 2.5: Mapa *links* de rede - Pedreira

Com relação a segurança, a camada de estrutura de rede trata dos problemas físicos e lógicos que podem comprometer a infra-estrutura da rede metropolitana de acesso aberto. Alguns exemplos de problemas de segurança na camada de estrutura de rede são: invasões aos computadores e equipamentos de rede do perímetro da MBAN, erros de configuração em roteadores, *switches* e pontos de acesso, erros de configuração em firewalls, falhas físicas em conexões cabeadas e etc.

2.4.2 Pontos de Interconexão

A MBAN pode ser classificada de acordo com os tipos de pontos que são conectados à ela:

- prédios públicos (prefeitura, escolas, hospitais, delegacias, bibliotecas);
- prédios privados (empresas, indústrias);

- residências;

No caso dos prédios públicos, cada ponto possui suas próprias necessidades e deve ser tratado especificamente. No modelo da MBAN de Pedreira, por exemplo, o prédio da prefeitura desempenha o papel de servidor de roteamento, concentrando os data centers e tratando todo o fluxo de dados e informações através de *firewalls* e *proxies*. Portanto, devem ser criadas regras para que usuários da rede de uma escola não consigam capturar ou manipular dados da prefeitura ou hospitais, por exemplo. Essas regras devem ser definidas na camada de estrutura de rede.

A inserção da população nesse contexto e as conexões chegando até as residências aumenta a complexidade da rede, que deve ser configurada de maneira precisa evitando brechas que permitam a captura e alteração de dados sensíveis do município.

As empresas poderiam usufruir das instalações físicas da rede sejam elas ópticas ou *wireless*; geralmente neste caso, algum tipo de acordo é realizado, seja financeiro ou de outra natureza. Assim, uma rede metropolitana de acesso aberto pode ser vista como atrativo para indústrias e grandes empresas.

Um termo que será utilizado no decorrer deste artigo é centro de interconexão. Pode-se definir o *centro de interconexão* de uma MBAN como sendo o local físico dos servidores e de grande parte da estrutura de conexão de rede e segurança. Por concentrar grande parte dos ativos de TI da MBAN, é natural que a localização desse centro deve ser estratégica, afim de facilitar o gerenciamento e manutenção. Em redes metropolitanas de acesso aberto, frequentemente o centro de interconexão é posicionado dentro da Prefeitura.

Com relação a segurança, a camada de pontos de interconexão trata das possíveis falhas e vulnerabilidades de todos os nós (desktops, notebooks, servidores, PDA's - Personal digital assistants...) conectados à rede metropolitana de acesso aberto. Alguns exemplos de problemas de segurança da camada de pontos de interconexão são: grande número de usuários com privilégios administrativos, infecções de vírus, *spams*, *malware* e trojans, uso de senhas "fracas" ou de baixa complexidade, falta de atualizações de patches segurança e falhas na configuração dos servidores tais como uso de portas padrão, portas abertas e serviços rodando desnecessariamente.

2.4.3 Serviços

Com a infra-estrutura de rede construída, vários serviços podem ser disponibilizados para os usuários da rede metropolitana, dentre os quais podemos citar [21], [20] e [32]:

- Acesso à Internet;
- VoIP;
- Quiosques de auto-atendimento de serviços públicos para o cidadão;
- Sistemas de gestão da administração municipal;
- Programa de informatização para as secretárias de educação;

Alguns tipos de serviços causam um impacto significativo na maneira como a estrutura de segurança da Infovia Municipal é construída. Um exemplo é a classe de serviços que necessitam de dados

sensíveis, muitas vezes mantidos sob sigilo por lei, e que por isso devem receber um tratamento especial dentro do ambiente que está sendo projetado.

Com relação a segurança, a camada de serviços trata das vulnerabilidades dos serviços expostos pela MBAN. Exemplos: falhas de segurança e problemas de latência com o VoIP, alto número de spams detectados no servidor de email, congestionamentos no link de Internet e *bugs* nos sistemas de gestão municipal.

Capítulo 3

Métricas de segurança

Neste capítulo serão definidos os conceitos de métricas de segurança, seus objetivos, os benefícios da utilização e alguns exemplos. O objetivo é apresentar o embasamento teórico das métricas de segurança e os termos técnicos desta área, para auxiliar a compreensão do modelo de métricas de segurança para redes metropolitanas de acesso aberto que será definido nos próximos capítulos.

3.1 Introdução

Todo chefe de equipe de segurança da informação (também conhecido como CISO - *Chief Information Security Officer*) deveria ser capaz de responder o seguinte conjunto de perguntas sobre a segurança da organização onde trabalha:

- Quão efetivos são os processos de segurança?
- Os controles de segurança implementados em minha empresa obtiveram melhores resultados este ano do que o ano passado?
- Como estamos se comparado aos concorrentes/companheiros?
- Estamos gastando a quantidade correta de dinheiro?

Uma maneira de responder tais perguntas de maneira eficiente é a utilização de métricas de segurança.

O estudo de métricas de segurança e suas aplicações em cenários de TI são alvos de diversas discussões [33]. O aumento do número de falhas em componentes, vulnerabilidades de softwares e ataques fazem com que as corporações se preocupem cada vez mais com as questões relacionadas à segurança da informação. Para lidar com tais problemas é necessário investir em implementação de controles e políticas de segurança. As características destes investimentos podem ser definidas a partir da realização de medições e análises da estrutura de segurança de informação da corporação. Neste cenário ocorre a aplicação das métricas de segurança [34]. Através da combinação de objetivos pré-definidos com coleta e análise de dados, as métricas podem indicar o nível atual de certa meta de segurança e direcionar as ações a serem tomadas pela organização [35].

A definição de métrica passa por dois importantes conceitos: a métrica, propriamente dita e medida. 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.

Dentre os autores que utilizam o primeiro modo para definir o conceito de métrica estão: Lowans [36], Anni [3] e Payne [35].

Payne em [35] utiliza a seguinte definição: medidas são geradas através de contagem enquanto métricas são geradas através de análises. Em outras palavras, medidas são dados "puros" e métricas são interpretações humanas, objetivas ou subjetivas de tais dados. Lowans [36] define métrica como sendo um conjunto de medidas que geram uma abordagem quantitativa de algo (uma rede ou um software por exemplo) ao longo de um período de tempo. As medidas nesse caso são representadas por números ou instruções binárias. O exemplo a seguir ilustra a diferença entre métrica e medida:

- Métrica: relação entre os alertas de vírus e infecções comparado com o semestre passado.

- Medidas: quantidade de alertas de vírus disparados, quantidade de vírus reportado.

Já o segundo modo de definição de métricas é empregado por Jaquith [37], Swanson [38] e Kovacich [39].

Jaquith, em [37], afirma que qualquer quantificação de um problema e seus resultados em um valor numérico pode ser considerado uma métrica. Kovacich [39] define métrica como sendo um padrão de medidas utilizando análises quantitativas, estatísticas ou matemáticas. Outra definição interessante é encontrada em [38]: métricas são ferramentas projetadas para facilitar a tomada de decisões e aumentar a performance e prestação de contas através da coleta, análise e divulgação de dados.

Ao longo desta dissertação será utilizado o conceito de métrica e de medida separadamente. Dividir o que será medido (medida) e o que será analisado (métrica) facilita a compreensão dos conceitos, além de abrir possibilidades para o desenvolvimento de modelos específicos de métricas de segurança, como o que será apresentado no capítulo 4. Portanto, podemos definir métricas de segurança como a análise quantitativa de um conjunto específico de medidas ao longo de um período de tempo, dentro do escopo da segurança da informação.

É importante observar que em todas as definições existe um consenso de que métricas devem ser expressas de maneira quantitativa. Esta abordagem difere do habitual tratamento qualitativo que a análise da segurança da informação recebe. Um exemplo clássico é a divulgação de resultados de problemas de segurança em classificações ou faixas como por exemplo, fraco, regular e alto. Esta forma é extremamente simples e oculta detalhes que para a segurança da informação podem ser essenciais.

A diferença entre as duas abordagens, quantitativa e qualitativa para um problema pode ser resumida no exemplo a seguir.

A Tabela 3.1 ilustra o resultado do problema da detecção de vírus em estações de trabalho por trimestre. A diferença da informação entre as abordagens é muito clara e evidencia a necessidade de utilizar números para expressar resultados de análises. O tratamento qualitativo muitas vezes é subjetivo, ou seja, o que significam os atributos baixo, médio e bom? Os números, entretanto, expressam com clareza a situação do problema.

Tab. 3.1: Vírus detectados nas estações - Abordagem quantitativa e qualitativa

Abordagem qualitativa - balanço final	**Abordagem quantitativa - balanço final**
1^o trimestre: médio	1^o trimestre: 43 % das estações infectadas
2^o trimestre: baixo	2^o trimestre: 16 % das estações infectadas
3^o trimestre: bom	3^o trimestre: 77 % das estações infectadas

3.2 Requisitos

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 através de investimentos mal aplicados. Mas o que torna uma métrica "boa"? Quais atributos uma métrica deve possuir? E as medidas? Elas também devem possuir propriedades para serem efetivas? Nesta seção serão definidos os atributos para a avaliação da qualidade de métricas e medidas de segurança.

Jaquith [37] propôs 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;

Medida de maneira consistente

Métricas possuem credibilidade somente se medidas de maneira consistente. Ou seja, se diferentes pessoas aplicarem o método ao mesmo conjunto de dados os resultados devem ser equivalentes. Métricas podem ser calculadas utilizando-se dois métodos: manual ou computacional. Em ambos os casos, a consistência deve ser assegurada pela documentação transparente dos processos de medida.

O emprego de métodos computacionais no cálculo das métricas ajuda a combater possíveis erros humanos consequentemente aumentando a confiabilidade das medições. Após programadas as máquinas executam as tarefas da mesmo modo em cada repetição.

Fácil de coletar

As métricas, em geral, levam tempo para serem calculadas. Em alguns casos apenas uma entrevista com o administrador da rede ou a execução de uma consulta SQL já é o suficiente. Porém, a coleta dos dados exige na maioria dos casos o uso de ferramentas complexas de auditoria, rotinas analisadoras de logs e até a execução de testes de penetração. Métodos ineficientes para coletar tais dados podem prejudicar o planejamento da empresa com relação ao tempo a ser utilizado pela análise dos resultados obtidos.

Expressa em números ou porcentagem

Métricas sólidas devem ser expressas em números cardinais (indica o número ou quantidade dos elementos constituintes de um conjunto) ou porcentagem. Números ordinais (usados para assinalar uma posição numa sequência ordenada) e "barras coloridas" (vermelha-amarela-verde, retratando níveis: alto, médio e baixo) não devem ser utilizados para expressar uma métrica.

Por exemplo, considere uma métrica que trata dos problemas de vírus em uma determinada organização. Vimos que uma possível métrica é a "relação entre os alertas de vírus e infecções comparada com medições anteriores". Considere que a organização emitiu 30 alertas de vírus e ocorreram 12 infecções. A métrica pode ser expressa então pela razão $\frac{12}{30} = 0.4$ ou seja, 40% dos alertas de vírus resultaram em infecções.

Outra forma de expressar a mesma relação é o desenvolvimento de uma "barra colorida" com os níveis alto, médio e baixo e colocar o resultado como médio, por exemplo. Note que nesse caso os detalhes são perdidos e a análise se torna subjetivo pois os dados da métrica possuem mais precisão do que três simples gradações.

Expressa utilizando ao menos uma unidade de medida

Já vimos que uma métrica deve ser expressa em números. Além disso, ela deve deve ser associada a uma unidade de medida que caracteriza o que está sendo contado. Por exemplo, a métrica "relação entre os alertas de vírus e infecções comparada com medições anteriores" é expressa em duas unidades de medida: alerta de vírus e infecções.

Suficientemente relevante

As métricas devem possuir significado para as pessoas que a analisam. Com o escopo claro e bem definido, um leitor pode obter a quantidade de informação necessária para tomar decisões a partir dos resultados da métrica.

Algumas vantagens na utilização de métricas em segurança da informação, incluem [37]: compreensão dos riscos de segurança, alertas para os problemas iminentes, compreensão das fraquezas na infra-estrutura de segurança, medição da performance dos processos de contra-medida e incentivo no uso da tecnologia para melhoria nos processos.

3.3 Classificação

A seção irá tratar das diversas classificações que as métricas de segurança podem receber. Serão apresentados três modelos de classificação de acordo com os trabalhos de Sademies [3], Jaquith [37]

e Swanson [38].

3.3.1 Modelo 1 - Sademies

O objetivo do trabalho de Sademies [3] é estudar a aplicação de métricas de segurança em empresas finlandesas. Utilizando como referências os trabalhos [40] e [41], o autor define um modelo de classificação de métricas de segurança. A seguir, o modelo será detalhado.

O modelo de métricas de segurança deve consistir de três componentes:

- O objeto a ser medido (por exemplo, um produto ou sistema),
- Os objetivos de segurança, ou seja, os parâmetros de segurança que serão usados para a comparação do objeto que está sendo medido. Os parâmetros de segurança podem ser obtidos através de: i) Requisitos de segurança, documentos específicos tais como especificações e padronizações. *Common Criteria* por exemplo [42]; ii) Boas práticas; iii) Dados históricos de segurança (*baselines*); iv) Gerenciamento de segurança baseado em experiências anteriores e v) Modelos de maturidade de processo (Maturity models) tais como SSE-CMM (*Systems Security Engineering Capability Maturity Model*) [43] e IA-CMM (INFOSEC Assessment Capability Maturity Model) [44].
- O método de medida. Exemplo: testes diretos, observações do sistema e avaliação de vulnerabilidades.

O modelo, ilustrado na Figura 3.1, propõe uma divisão das métricas de segurança em quatro categorias: técnicas, organizacionais, operacionais, "brainstormers", individuais e de ambiente. A Tabela 3.2 apresenta a descrição de cada uma das categorias, além de exemplos e os principais problemas para a implementação de cada uma delas.

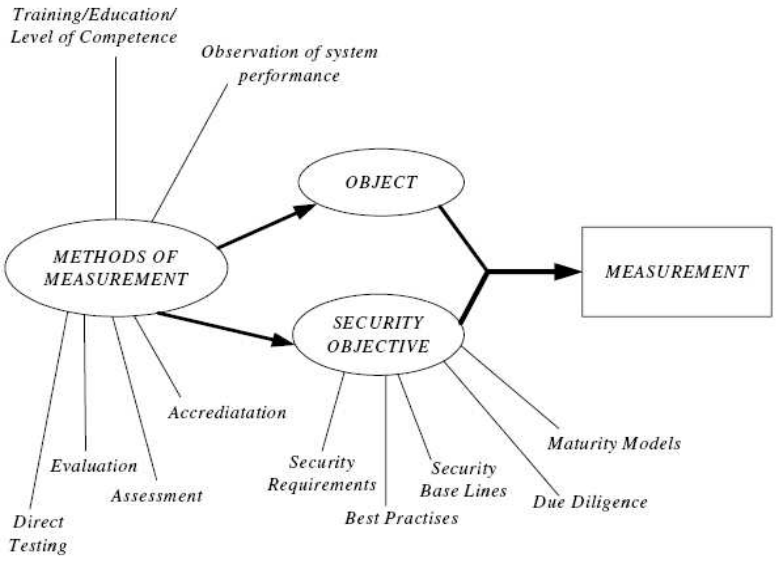

Fig. 3.1: Modelo de Katzke para métricas de segurança. Extraído de [3]

Tab. 3.2: Classificação de métricas de segurança

	Técnicas	Organizacionais	Operacionais	Brainstormers	Individuais	Ambiente
Descrição	Objetos técnicos; algoritmos, especificações e arquiteturas	Eficiência de programas e processos da organização	Riscos para os ambientes funcionais	Problemas globais e relativos a necessidade de síntese de uma ou mais categoria de métricas	Capacidade individual de funcionários, colaboradores, etc	Aspectos de segurança relevantes ao ambiente da organização
Exemplos	Logs do sistema	Porcentagem de sistemas autorizados	Ativos da empresa	Junção de três categorias em uma só métrica	Conhecimento do nível educacional de um empregado	Falhas na rede elétrica
Desafios	Pode conter grande quantidade de dados inúteis que devem ser filtrados	Exige uma visão global da organização	Exige a compreensão do ambiente operacional e seus efeitos	Exige uma visão global de todo o ciclo de vida do sistema	Dificuldade em nivelar o quadro da organização	Possíveis dificuldades para modelar funções de um ambiente que pode conter fatores e combinações inesperadas

3.3.2 Modelo 2 - Jaquith

Jaquith [37] propõe uma divisão das métricas de segurança em dois grandes grupos: métricas técnicas para identificação e diagnóstico de problemas e métricas de eficiência de programas de segurança, também chamada de métricas de eficiência de processos. Cada um dos grupos possui sub-classificações próprias. A seguir serão apresentadas as duas classes de métricas assim como as respectivas sub-divisões.

Métricas técnicas para identificação e diagnóstico de problemas

As métricas técnicas para identificação e diagnóstico de problemas são caracterizadas pela tentativa de detecção de problemas de segurança em toda a infra-estrutura (física e lógica) da organização. Tais métricas podem ser classificadas em:

- Defesa do perímetro: Ajuda a compreender os riscos que estão fora do perímetro da organização. Medem a efetividade de antivírus, anti-spam, firewalls e sistemas de detecção de intrusão.
- Cobertura e controle: Métricas de cobertura e controle caracterizam o nível de sucesso que uma organização obteve na extensão do alcance das políticas de segurança. Exemplos: número de estações e servidores com anti-vírus instalado, número de *patches* de segurança aplicado por máquina, número de estações em conformidade com as configurações de segurança pré-definidas.
- Disponibilidade e confiabilidade: Incidentes de segurança freqüentemente implicam em quedas do sistemas e conseqüentemente em tempo fora do ar (*downtime*). Aumentar o tempo de um

sistema no ar (*uptime*) exige minimização de problemas dos segurança relacionados ao *downtime*. As métricas de disponibilidade e confiabilidade tratam da relação entre incidentes de segurança e o *uptime* ou *downtime*. Exemplos: tempo médio para recuperação de um sistema e porcentagem de *uptime* de um sistema.

- Riscos em aplicações: Contabiliza o número de defeitos, complexidade e índices de riscos em aplicações personalizadas ou desenvolvidas diretamente pela organização.

Métricas de eficiência de processos

O desenvolvimento e implementação da política de segurança da informação de uma organização é de fundamental importância para a minimização de riscos e até custos. Porém, como saber se os processos estão funcionando de maneira correta? Esse é o objetivo das métricas de eficiência de processos, medir a eficiência dos programas de segurança implementados.

Programas ou políticas de segurança são elaborados baseados em normas, guias e práticas definidas em documentos propostos por grandes organizações de TI. Quatro dos mais populares documentos com orientações sobre segurança da informação são os seguintes, também chamados de *security frameworks*:

- COBIT - Control Objectives for Information Technology é um guia para a gestão de TI publicado pelo ISACF (Information Systems Audit and Control Foundation) em 1996. O COBIT inclui recursos tais como um sumário executivo, um framework, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento [45]. As práticas de gestão do COBIT são recomendadas pelos peritos em gestão de TI pois ajudam a otimizar os investimentos e fornecem métricas para avaliação dos resultados. O COBIT está dividido em quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte e monitoração. A última versão do COBIT foi lançada em 2008.

- ISO/IEC 17799: uma compilação de recomendações para melhores práticas de segurança, que podem ser aplicadas por empresas, independentemente do seu porte ou setor [46]. Ela foi criada com a intenção de ser um padrão flexível, nunca guiando seus usuários a seguirem uma solução de segurança específica em detrimento de outra. A versão original foi publicada em 2000, que por sua vez era uma cópia fiel do padrão britânico (BS) 7799-1:1999.

- ITIL - Information Technology Infrastructure Library: É um modelo de referência para gerenciamento de processos de TI. A metodologia foi criada pela secretaria de comércio (Office of Government Commerce, OGC) do governo Inglês, a partir de pesquisas realizadas por Consultores, Especialistas e Doutores, para desenvolver as melhores práticas para a gestão da área de TI nas empresas privadas e públicas [47]. Atualmente se tornou a norma BS-15000, sendo esta um anexo da ISO 9000/2000. O foco deste modelo é descrever os processos necessários para gerenciar a infra-estrutura de TI eficientemente e eficazmente de modo a garantir os níveis de serviço acordados com os clientes internos e externos.

- NIST - Documentos da série 800: As publicações 800-18 e 800-30 especificam em alto nível dezessete classes de controles de segurança. O NIST - National Institute of Standards and

Technology - é uma agência governamental não-regulatória da Administração de Tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia.

Jaquith divide as métricas de eficiência de processo de acordo com cada um dos quatro domínios do COBIT:

- Planejamento e organização: Processos para a definição de planos de segurança estratégicos com o escopo em todos os níveis de investimento, avaliando os riscos e gerenciando os recursos empresariais e humanos. Exemplos de métrica: porcentagem de bens da empresa com avaliações de risco documentadas, alocações de recursos para segurança e porcentagem de usuários submetidos a avaliação de passado, ou *background check*.

- Aquisição e implementação: Processos para identificação, aquisição, desenvolvimento e instalação de soluções de segurança. Exemplos: métricas derivadas da seguinte questão: como e com qual freqüencia a equipe de segurança da informação participa da definição do requisitos dos novos sistemas de informação? Número de reuniões da equipe de segurança com analistas de negócio.

- Entrega e suporte: Processos para a definição de níveis de serviço, gerenciando o acesso interno e a terceiros; treinamento de usuários finais, tratamento de incidentes e funcionamento de programas para a proteção de dados, instalações e operações. Exemplos: porcentagem de novos empregados com treinamento em segurança da informação, porcentagem da equipe de segurança que possui certificações profissionais em segurança, porcentagem de sistemas que verificam as políticas de senhas, porcentagem de backups armazenados em locais remotos e prejuízos financeiros causados por incidentes de segurança.

- Monitoração: Processos para a monitoração de sistemas, avaliando a eficiência dos controles de segurança e auxiliando processos de auditoria. Exemplos: porcentagem de sistemas com eventos monitorados e logs de atividades, número de auditorias completadas com sucesso e porcentagem de controles funcionando como projetado.

3.3.3 Modelo 3 - NIST

O modelo de classificação de métricas de segurança proposto por [38] leva em consideração o nível de maturidade do programa de segurança da informação da organização. A Figura 3.2 ilustra os diferentes estágios de maturidade de um programa de segurança.

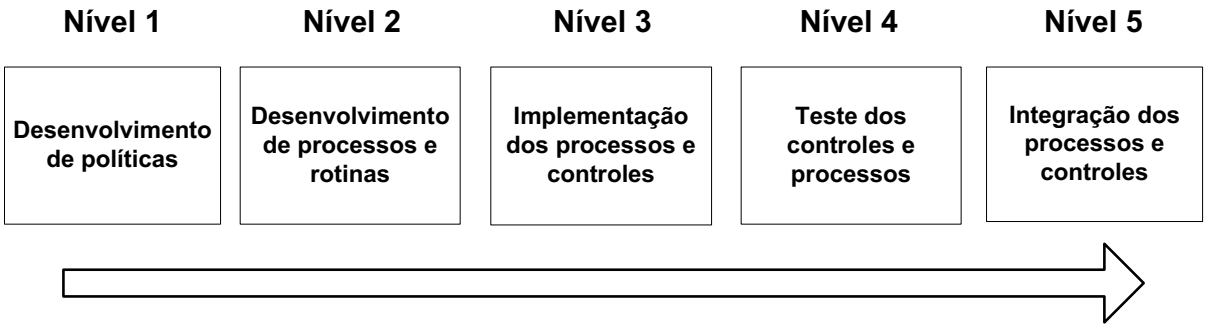

Fig. 3.2: Maturidade do programa de segurança e tipos de medida.

A maturidade de um programa de segurança é definida pela existência de processos e rotinas. Conforme a maturidade do programa de segurança aumenta, as políticas se tornam mais detalhadas e melhor documentadas, os processos se tornam padronizados e os dados produzidos podem ser utilizados para a medir performance em grande quantidade.

São propostos três tipos de métricas: implementação, eficiência/efetividade e impacto. Cada tipo de métrica é obtido de acordo com o nível de maturidade do programa de segurança. Apesar de ser possível utilizar diferentes tipos de métricas simultâneamente, o objetivo principal das métricas de segurança é a implementação de cada fase do processo ilustrado em 3.2.

Considere a seguinte métrica: porcentagem de sistemas com planos de segurança aprovados. A Tabela 3.3 mostra o desenvolvimento da métrica em cada uma das fases do programa de maturidade.

Tab. 3.3: Tipos de métrica e níveis de maturidade

Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Quais os sistemas serão observados e medidos? Desenvolvimento de políticas. A porcentagem de sistemas com planos de segurança aprovados é menor 100%	Identificação e estabelecimento dos objetivos de segurança para os sistemas medidos. Os resultados das medições ainda não atingiram 100%.	O nível 3 representa que os resultados da métrica alcançaram e se mantiveram em 100%. Ou seja, os controles de segurança propostos foram implementados por completo.	Medir a eficiência dos controles de segurança implementados. O quão efetivos são os planos de segurança dos sistemas?	Impacto dos controles de segurança implementados.

3.4 Dificuldades no desenvolvimento de métricas de segurança

Nas seções anteriores foi mostrada a importância que as métricas de segurança desempenham na visualização de problemas relacionados a segurança da informação. Porém, por ser um campo de pesquisa relativamente novo [3] e pela própria natureza dos problemas de segurança da informação, existem diversas dificuldades na geração de métricas de segurança e na aplicação das mesmas no contexto desejado.

Um dos grandes problemas das métricas de segurança é o chamado problema fundamental da medição [48]. 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? Ou seja, como interpretar corretamente os dados? O exemplo a seguir ilustra esse problema.

Considere as medições obtidas por uma métrica com relação a ataques de modificação de web-sites (*defacements*). Esse tipo de ataque não é tão comum quanto foi alguns anos atrás. Os web-sites 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.

A Tabela 3.3 mostra alguns dos principais problemas relacionados às métricas de segurança.

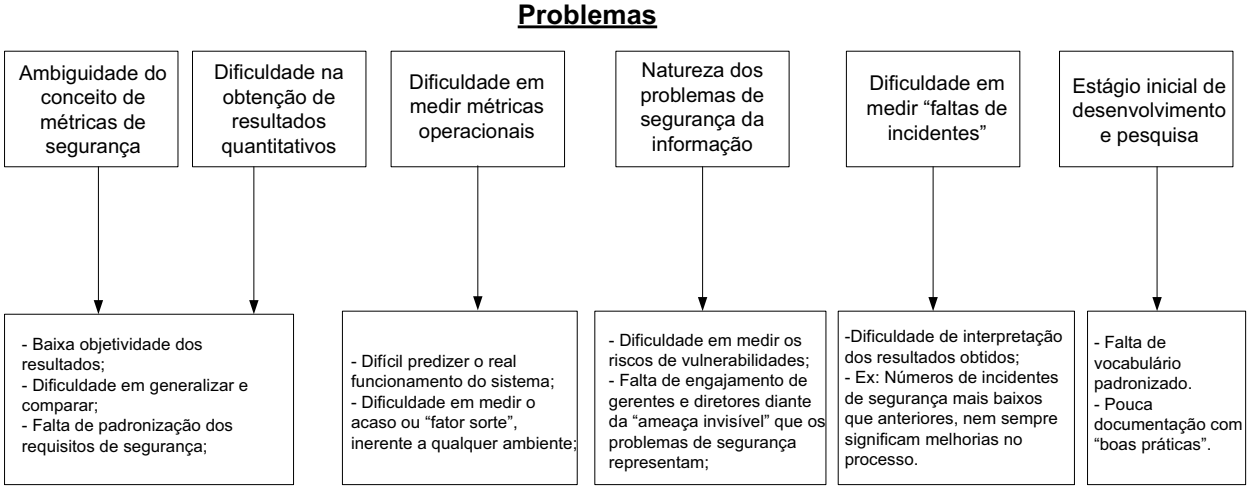

Fig. 3.3: Problemas no desenvolvimento e aplicação de métricas de seguranças

3.5 Pesquisas recentes

A Figura 3.4 ilustra o crescimento de produção científica envolvendo o conceito de métricas de segurança para TI. Os dados para a geração do gráfico foram coletados utilizando os seguintes portais de pesquisa acadêmica: *ACM Portal*, *IEEE Xplore*, *SpringerLink*, *ScienceDirect* e *Scirus*.

Uma área de pesquisa atual é relacionada ao desenvolvimentos de indicadores de segurança utilizando as métricas. Weissmann et. al. [34] propõe uma técnica para avaliar a segurança global de uma organização. A técnica consiste em identificar diversos cenários de ameaça a segurança da organização e criar um indicador de segurança para tais cenários. Os cenários teriam o mesmo papel que as métricas de segurança, ou seja, prover dados para análises.

O indicador é calculado utilizando a porcentagem de perda de bens com os possíveis cenários de ataque, pois o autor afirma que a segurança total é alcançada somente se nenhum bem foi perdido (através de um longo período de tempo). A avaliação da segurança de toda a organização é dada pela

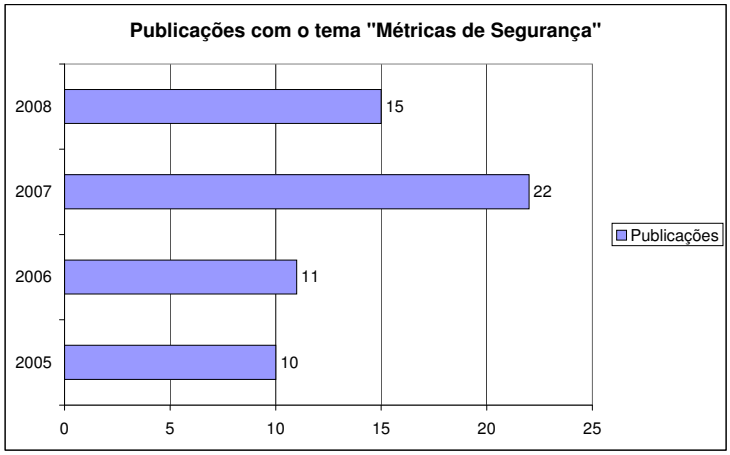

Fig. 3.4: Publicações recentes com o termo “Métricas de segurança”.

combinação dos cenários e de seus indicadores. A abordagem de indicadores utilizando a porcentagem de perda de bens é válida, mas não completa. A porcentagem de perda de um certo bem pode ser baixa o que não necessariamente assegura um alto nível de segurança já que as vulnerabilidades podem simplesmente não ter sido exploradas corretamente. Nossa proposta, consiste na criação de indicadores levando em consideração o estado atual dos componentes de segurança de uma métrica.

Outra importante área de pesquisa em métricas de segurança é o desenvolvimento de taxonomias para os diferentes tipos de métricas de segurança. Savola [49] afirma que os estudos sobre a definição das métricas de segurança ainda estão no início. O autor afirma ainda que para fazer avanços no campo das métricas de segurança o atual estado da arte deve ser cuidadosamente investigado. A partir dessa investigação e experiência do autor na área, foi proposta a criação de uma árvore de classificação, ou taxonomia, para métricas de segurança. A taxonomia proposta leva em consideração os seguintes níveis: métricas de segurança para análise de custo-benefício, métricas de confiança, métricas de segurança para análise de risco em nível de negócio, métricas de segurança para gerenciamento da segurança da informação e métricas SDT (*Security, Dependability and Trust* ou segurança, dependabilidade[1] e confiança) para produtos, sistemas e serviços.

Frameworks de segurança, como NIST e ISO/IEC também propõem taxonomias para métricas de segurança com o objetivo de facilitar o desenvolvimento do processo de composição de métricas. As métricas propostas nesta dissertação são classificadas usando as camadas de classificação da rede metropolitana de acesso aberto.

Um projeto interessante sobre métricas de segurança é o “Metrics Center” mantido pelo portal SecurityMetrics.org [4]. Com início em junho de 2008, seu objetivo é promover o uso eficiente das métricas de segurança. O projeto possui atualmente dois serviços disponíveis: “Metrics Catalog” e “YouAreHere-Benchmarks”.

[1]Dependabilidade é um termo traduzido literalmente do inglês “*dependability*” que reúne diversos conceitos que servem de medida, tais como confiabilidade (reliability), disponibilidade (*availability*), segurança (*safety*), mantenabilidade (*maintainability*), comprometimento do desempenho (*performability*), e testabilidade (*testability*)

Fig. 3.5: Tela do Metrics Catalog, um serviço do projeto Metrics Center. Extraído de [4]

O "Metrics Catalog" ou catálogo de métricas é uma ferramenta destinada a pesquisadores e utilizadores de métricas de segurança que possibilita a organização e compartilhamento de definições de métricas. As métricas do catálogo estão divididas de acordo com os seguintes documentos/padronizações de segurança: PCI DSS-1.1 (*Payment Card Industry Data Security Standard*), NIST, Controles propostos em NIST SP800-53, ISO/IEC 27002 e CISWG (*Computer Information Security Working Group*). A Figura 3.5 mostra a tela de navegação do sistema de catalogação de métricas.

Cada uma das métricas catalogadas possui diversos atributos que definem a métrica como por exemplo, a respectiva unidade de medida, objetivo, fórmula e freqüência.

O outro serviço do "Metrics Center" é o "YouAreHere-Benchmarks". Esse serviço permite que empresas comparem o desempenho de seus programas de métricas de segurança com o desempenho dos programas de outras empresas. Esse tipo de comparação é importante para que as empresas tenham conhecimento dos investimentos de segurança que estão sendo feitos no mercado além de ajudar em eventuais tomadas de decisão sobre os rumos da segurança da informação dentro da empresa.

3.6 Exemplos

Para finalizar este capítulo, serão apresentadas algumas métricas de segurança na Tabela a seguir 3.4. Elas foram escolhidas a fim de ilustrar da melhor forma possível todos os conceitos que foram mostrados até aqui.

Tab. 3.4: Exemplos de métricas de segurança

Métrica	**Documento de referência**
Taxa de patches de segurança aplicados por período ou por nó da rede.	Jaquith, [37]
Downtime, período de tempo em que um recurso computacional não está funcionando ou operacional , não planejado.	Jaquith, [37]
Porcentagem total de sistemas para os quais os controles de segurança foram testados em um determinado período de tempo.	Nist, [38]
Porcentagem de notebooks com capacidade de cifragem para arquivos confidenciais.	Nist, [38]
Porcentagem de bens considerados críticos que utilizam autenticação forte.	Metrics Center
Porcentagem de senhas e PINs que são armazenados em hashs criptográficos.	Metrics Center [50]
Porcentagem de anti-vírus, anti-spam instalado em desktops, servidores e notebooks.	Berinato, [51]
Aplicação de testes de segurança (benchmarks, como o CIS - *Center for Internet Security*) em desktops e notebooks. Porcentagem de computadores que estão dentro do patamar definido pela organização.	Berinato, [51]

Capítulo 4

Métricas de segurança para Redes Metropolitanas de Acesso Aberto

O presente capítulo será dividido em três seções:

1. Definição do conjunto de atributos que forma o modelo de métricas de segurança para MBANs.
2. Modelagem do cálculo do indicador de segurança para um métrica.
3. Apresentação das métricas de segurança para MBANs.

4.1 Definição dos requisitos

Existem diversas referências sobre como definir e implementar métricas de segurança. Neste trabalho, será utilizada uma abordagem que une conceitos de metodologias propostas nos seguintes documentos: Swanson [38], Payne [35] e Jaquith [37]. Conforme o processo de criação de métricas for descrito as contribuições de cada um dos documentos acima será explicitada.

O processo de definição e criação das métricas de segurança para MBANs, foi baseado no programa de estabelecimento de métricas de segurança proposto por Payne em [35]. O programa consiste em um total de sete passos:

1. Definir os objetivos e metas do programa de métricas;
2. Decidir quais métricas gerar;
3. Desenvolver estratégias para a geração das métricas;
4. Estabelecer testes de performance e alvos para as melhorias;
5. Determinar quais métricas serão reportadas;
6. Criar e executar um plano de ação;
7. Estabelecer um programa formal de revisão e reciclagem das métricas;

Todos os sete passos apresentados anteriormente são recomendados para a criação de um programa completo de implementação de métricas de segurança. Nosso objetivo neste momento porém é somente definir os requisitos das métricas de segurança para MBANs, dessa forma, somente os três primeiros passos serão utilizados. A seguir, cada um dos três tópicos utilizados será discutido.

Definir os objetivos do programa de métricas

Aqui, deve-se claramente expor o objetivo de um certo conjunto de métricas. Todas as métricas propostas neste trabalho foram desenvolvidas de acordo com o seguinte objetivo primário:

Gerar métricas capazes de analisar eficientemente os riscos de segurança e as respectivas medidas preventivas em uma rede metropolitana de acesso aberto, sobre todos seus níveis: estrutura de rede, serviços e pontos de interconexão.

Dessa forma, os investimentos na área de segurança podem ser balanceados apropriadamente e as precauções com relação aos riscos de segurança tomadas, possibilitando o desenvolvimento sustentável das redes metropolitanas de acesso aberto. Note também que por se tratar de um objetivo genérico, ele pode ser utilizado para a criação de outras métricas de segurança para MBANs.

Além do objetivo primário, têm-se as metas ou objetivos secundários. Eles consistem em um conjunto de ações que se executadas, podem levar ao cumprimento do objetivo primário. A Figura 4.1 ilustra o relacionamento das metas com o objetivo.

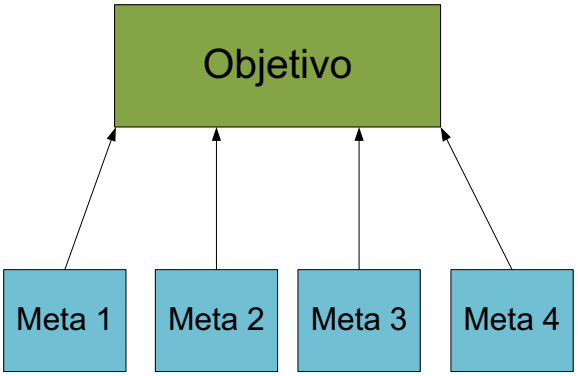

Fig. 4.1: Objetivo e metas de uma métrica de segurança.

Ao longo da seção, o processo de desenvolvimento de uma métrica de segurança será ilustrado com a construção gradual de um exemplo. O exemplo inicia com a definição de um objetivo secundário a partir do objetivo primário citado anteriormente. Uma meta para o objetivo primário acima poderia ser: “Analisar e aumentar o nível de segurança das conexões entre os prédios da Rede Metropolitana de Acesso Aberto”. À partir desta meta será construída a primeira métrica de segurança para MBANs.

Decidir quais métricas gerar

Payne [35], utiliza duas abordagens para a geração de métricas: *top-down* e *bottom-up*. A abordagem *top-down* funciona da seguinte maneira: primeiro, deve-se listar todos os objetivos específicos

Tab. 4.1: Abordagem *Top-Down*

1) Listar todos os objetivos do programa de segurança.	Exemplo de objetivo: Reduzir o número de infecções de vírus em 30% dentro da empresa.
2) Identificar métricas que indiquem progresso para cada objetivo.	Exemplo de métrica: Taxa de alertas de vírus e infecções.
3) Determinar as medidas necessárias para cada métrica.	Exemplo de medida: Número de alertas de vírus disparado pela organização. Número de infecções de vírus reportada.

Tab. 4.2: Abordagem *Bottom-Up*

1) Identificar medidas que podem ser coletadas.	Exemplo de medida: Média de vulnerabilidades críticas detectadas em servidores por departamento.
2) Determinar as métricas que podem ser geradas à partir das medidas.	Exemplo de métrica: Alterações no número de vulnerabilidades críticas detectadas em servidores por departamento.
3) Determinar a associação entre as métricas derivadas e os objetivos específicos estabelecidos pelo objetivo final.	Exemplo de objetivo: Reduzir o nível de vulnerabilidades detectadas em servidores por departamento.

de seu programa de segurança, depois identificar métricas que podem ajudar a determinar se tais objetivos estão sendo cumpridos e por último as medidas que vão gerar as métricas. A Tabela 4.1 ilustra o funcionamento da abordagem *top-down*:

A abordagem *bottom-up* faz o caminho inverso. Primeiro são identificados os processos de segurança, produtos, serviços, etc que estão aptos a serem medidos. Das medidas são extraídas as respectivas métricas e por fim, avaliar quais os objetivos que as métricas geradas podem realizar. A Tabela 4.2 ilustra o funcionamento da abordagem *bottom-up*:

Todas as métricas propostas no trabalho foram geradas utilizando tais abordagens. Em certos casos foi usado a *top-down*, em outros casos a *bottom-up*, dependendo da dificuldade de identificação do que seria medido ou do objetivo específico de segurança.

Continuando com a construção do exemplo, dois atributos podem ser agregados ao objetivo: métrica e medida.

- **Objetivo:** Analisar e aumentar o nível de segurança das conexões entre os prédios da Infovia.
- **Métrica:** Taxa de prédios que são interconectados utilizando-se tecnologias com suporte à segurança (criptografia, VPNs, VLANs e etc).
- **Medidas:** i) Número de prédios conectados a rede municipal, ii) tipo de tecnologia de interconexão de rede por prédio, iii) número de prédios que possuem criptografia entre as conexões, iv) número de prédios que possuem recursos de firewall entre as conexões, v) protocolo criptográfico utilizado..

Desenvolver estratégias para a geração das métricas

Depois da decisão sobre o que terá de ser medido, estratégias para a coleta de dados devem ser desenvolvidas. Estas estratégias devem ser capazes de responder tais perguntas: De onde e como os dados serão coletados? Qual o melhor período para a coleta dos dados? As respostas para essas perguntas estão em dois atributos fundamentais para o desenvolvimento de técnicas para a geração das métricas: origem dos dados e freqüência.

Origem dos dados pode ser definida como a localização dos dados que serão utilizados no cálculo da métrica. A origem do dado engloba desde entrevistas com os administradores da rede até *logs* de sistemas, bases de dados, auditorias e ferramentas de rastreamento [38].

A freqüência, por sua vez, define os períodos de tempo em que os dados serão coletados. A freqüência pode ser semanal, mensal, trimestral e etc.

Com base nestas informações podemos atualizar o nosso exemplo:

- **Objetivo:** Analisar e aumentar o nível de segurança das conexões entre os prédios da Infovia.
- **Métrica:** Taxa de prédios que são interconectados utilizando-se tecnologias com suporte à segurança (criptografia, VPNs, VLANs e etc).
- **Medidas:** i) Número de prédios conectados a rede municipal, ii) tipo de tecnologia de interconexão de rede por prédio, iii) número de prédios que possuem criptografia entre as conexões, iv) número de prédios que possuem recursos de firewall entre as conexões.
- **Origem dos dados:** Entrevistas e auditoria nos equipamentos de rede que fazem as conexões.
- **Freqüência:** Semestral.

Para completar a descrição do modelo que descreve as métricas de segurança para Redes Metropolitanas de Acesso Aberto, serão definidos mais dois atributos: classificação da métrica e fórmula.

A criação de um atributo relativo a taxonomia da métrica foi inspirada na classificação de métricas proposta por Jaquith [37]. Enquanto Jaquith [37] divide suas métricas utilizando critérios técnicos, nossa abordagem de classificação tem como objetivo relacionar métricas com redes metropolitanas de acesso aberto.

A classificação da métrica está relacionada com um ou mais componentes da Rede Metropolitana de Acesso Aberto, definidos no capítulo 2: estrutura de rede, pontos de interconexão e serviço. A classificação é detalhada a seguir.

Estrutura de rede - métricas que tratam dos problemas físicos e lógicos da rede metropolitana de acesso aberto. Alguns exemplos de problemas de segurança que as métricas de estrutura de rede lidam são: falhas físicas em conexões cabeadas e antenas, falhas em conexões sem fio, erros de configuração em roteadores e firewall e comunicação não-segura entre prédios.

Pontos de interconexão - métricas que tratam dos problemas de segurança dos nós que formam a rede metropolitana de acesso aberto. Esses nós podem ser prédios públicos, comerciais e também residências. Tal diversidade contribui para que as vulnerabilidades de segurança aumentem. Alguns exemplos de problemas de segurança que as métricas deste tipo devem tratar são: infecções de vírus, utilização de senhas fracas e ausência de *patches* de segurança.

Serviços - métricas que tratam dos problemas de segurança dos diversos serviços que são executados sobre a plataforma da rede metropolitana de acesso aberto. Exemplos de problemas de segurança que tais métricas tratam são: congestionamento e falta de autenticação na distribuição de Internet; latência, alto número de ligações não concluídas e falta de criptografia no uso do VoIP.

Por fim, temos o atributo fórmula, que descreve os cálculos que devem ser realizados para a quantificação da métrica em uma expressão numérica [38]. Os dados de entrada da fórmula são obtidos através das medições realizadas. A partir do resultado da fórmula, têm-se um valor ou indicador para a métrica que irá variar de 0 a 1, com 0 para o mais baixo e 1 para o mais alto valor. A próxima seção irá apresentar dois modelos com a generalização do cálculo das fórmulas para as métricas de segurança para Redes Metropolitanas de Acesso Aberto.

Portanto, o conjunto de atributos que definem uma métrica de segurança para MBANs serão os seguintes: Objetivo, Métrica, Medida, Origem do dado, Freqüência, Classificação e Fórmula. Abaixo, o exemplo com todos os atributos.

- **Objetivo:** Analisar e aumentar o nível de segurança das conexões entre os prédios da Infovia.
- **Métrica:** Taxa de prédios que são interconectados utilizando-se tecnologias com suporte à segurança (criptografia, VPNs, VLANs e etc).
- **Medidas:** i) Número de prédios conectados a rede municipal, ii) tipo de tecnologia de interconexão de rede por prédio, iii) número de prédios que possuem criptografia entre as conexões, iv) número de prédios que possuem recursos de firewall entre as conexões.
- **Origem dos dados:** Entrevistas e auditoria nos equipamentos de rede que fazem as conexões.
- **Freqüência:** Semestral.
- **Classificação:** Estrutura de rede.
- **Fórmula:** A ser definida na próxima seção.

4.2 Cálculo do indicador de segurança para uma métrica

Nesta seção serão definidos dois modelos para o cálculo das fórmulas das métricas de segurança para Redes Metropolitanas de Acesso Aberto. Os modelos também podem ser extendidos para o uso em qualquer métrica de segurança definida nos padrões propostos em [38] e [35].

Os modelos propostos, padronizam a nomenclatura dos termos relativos a métricas de segurança e definem o cálculo das fórmulas de uma maneira genérica, contribuindo para a diminuição de critérios subjetivos na formulação das métricas [52].

O primeiro modelo baseia-se na simplicidade ao tratamento matemático dos requisitos [53]. As fórmulas foram definidas utilizando basicamente o conceito de média aritmética. Apesar de sujeita a falhas na interpretação, a média em nosso caso se comporta bem, pois o objetivo da fórmula é a criação de um indicativo global que represente o nível de segurança de uma métrica. O modelo permite a alteração da ferramenta matemática utilizada para o cálculo da fórmula, dando flexibilidade para permitir outras aborgadens teóricas nesse sentido.

Já o segundo modelo pode ser considerado mais complexo e foi embasado na teoria dos conjuntos e análise combinatória. Este modelo procurou corrigir as possíveis falhas de interpretação com o uso somente da média aritmética e a contagem dos elementos das métricas encontradas no modelo anterior.

4.2.1 Modelo 1

Considere uma métrica M. As *medidas* ou *componentes* da métrica M são denotados por a_1, a_2, a_3 , ..., a_n e $a_i \in \Re^*$ onde $\Re^*$ denota o conjunto dos números reais não-negativos. A fórmula F de uma métrica pode ser definida como uma relação entre os componentes $a_1, a_2, a_3, ..., a_n$ satisfazendo a condição $0 \leq F \leq 1$. A fórmula representa um indicador quantitativo de segurança da métrica, com 0 representando o valor mínimo e 1 representando o valor máximo. Dessa forma temos um primeiro parâmetro de comparação entre diferentes métricas. Uma métrica com fórmula igual a 0 representa que nenhum dos requisitos de segurança foram cumpridos, analogamente uma métrica com fórmula igual a 1 representa que os requisitos de segurança da métrica foram cumpridos, o que não necessariamente signifique que a segurança é completa.

Tomemos um conjunto de componentes $a_1, a_2, a_3, ..., a_n$. Para cada a_i, temos um a_t que corresponde ao valor máximo de a_i. Essa propriedade é válida pois se tratando de um conjunto de métricas de segurança sempre têm-se uma medida que representa o valor máximo e outras medidas derivadas desse valor.

Exemplo 1 - Considere uma métrica $M = \{$Controle da segurança dos pontos de acesso da Rede Municipal$\}$. Podemos ter então um conjunto de medidas ou componentes formado por a_1 = número de pontos de acesso que usam WEP, a_2 = número de pontos de acesso que usam WPA ou WPA2 e a_3 = número de pontos de acesso que não fazem uso de qualquer protocolo criptográfico. O a_t correspondente deve ser o valor máximo para cada a_i que neste caso é o número total de pontos de acesso da Rede Municipal.

Podemos ter casos em que um componente possui o mesmo valor do seu respectivo total ou seja $a_t = a_i$. Note também que como a_t representa o valor máximo de a_i então $\left(\frac{ai}{at} \times 100\right)$ representa o valor da medida em termos de porcentagem.

Definição 1: *Um componente a_n de uma métrica é dito inseguro se quando seu valor aumenta, os riscos de problemas de segurança relacionados aos objetivos da métrica também aumentam.*

Um exemplo de componente inseguro, é o número de vírus detectado. Quanto maior o número de vírus, maiores são os riscos de problema de segurança.

Considere um componente inseguro a_i. Seja a_t seu valor máximo, então temos $CI = \left(\frac{a_i}{a_t} \times 100\right)$ como a representação em forma de porcentagem de a_i. Se fizermos $CI = \frac{(\frac{a_i}{a_t})\times 100}{100}$ vamos ter $0 \leq CI \leq 1$. Chamaremos CI de *componente inseguro normalizado*.

Note que, de acordo com a definição acima, quando CI assume valores próximos de 1 temos que o nível de segurança do componente está muito abaixo do desejado ou seja, a chance de riscos de segurança aumentam. Analogamente, quando CI assume valores próximos de 0 temos que o nível de segurança do componente está próximo do desejado.

Definição 2: *Um componente a_n de uma métrica é dito seguro se quando seu valor aumenta, os riscos de problemas de segurança relacionados aos objetivos da métrica diminuem.*

Um exemplo de componente seguro, é o número de conexões com recursos criptográficos habilitados. Quanto maior o número de conexões cifradas, menores são os riscos de segurança.

Considere um componente seguro a_s. Seja a_t seu valor máximo, então temos $CS = \left(\frac{a_s}{a_t} \times 100\right)$ como a representação em forma de porcentagem de a_s. Se fizermos $CS = \frac{(\frac{a_s}{a_t})\times 100}{100}$ vamos ter $0 \leq CS \leq 1$. Chamaremos CS de *componente seguro normalizado*.

Note que, de acordo com a definição acima, quando CS assume valores próximos de 1 temos que o nível de segurança do componente está próximo do desejado ou seja, a chance de riscos de segurança diminuem. Analogamente, quando CS assume valores próximos de 0 temos que o nível de segurança do componente está abaixo do desejado.

A fórmula F de uma métrica, como já foi dito, deve expressar um valor entre 0 e 1 e servir como um indicativo para o nível de segurança da métrica proporcionando uma visão global acerca do cumprimento dos objetivos da métrica. Valores próximos de 0 devem indicar baixo nível de segurança e valores próximos de 1 alto nível de segurança.

Seja uma métrica M. Considere os possíveis casos sobre M:

1. M é composta somente por componentes seguros;
2. M é composta somente por componentes inseguros;
3. M é composta por componentes seguros e inseguros;

Em cada caso teremos uma fórmula diferente para M, daí a importância da classificação dos componentes da métrica.

Caso 1 - *M é composta somente por componentes seguros.*

Considere X o conjunto dos componentes seguros normalizados. A fórmula de M será dada pela média aritmética dos componentes seguros normalizados:

$$F_M = \overline{X}$$

donde $0 \leq F_M \leq 1$ com 0 representando o valor mínimo e 1 o valor máximo.

Calcular a média aritmética $\overline{X}$ do conjunto X é uma maneira de representar o resultado de todos os componentes em somente um número. Apesar da média aritmética induzir a erros de interpretação, em nosso caso ela é uma boa medida, pois irá mostrar o comportamento geral dos componentes de segurança. Além disso, a média irá preservar o resultado final em um valor entre 0 e 1.

Exemplo 2 - Considere uma métrica que trata da relação de disponibilidade e confiabilidade dos servidores da Rede Municipal. Um conjunto possível de componentes pode ser: $a_1 =$ número de servidores que possuem serviços de redundância, $a_2 =$ número de servidores que estão no programa de backup e $a_3 =$ número de servidores que possuem cópias de segurança em locais fisicamente distantes. O valor total a_t de cada componente é o número de servidores. Vamos analisar os componentes a fim de dividí-los em seguros ou inseguros.

$a_1 =$ componente seguro, pois quanto maior a quantidade de servidores com serviços de redundância, maior a segurança do sistema.

$a_2 =$ componente seguro, pois quanto maior a quantidade de servidores no programa de backup, maior a segurança do sistema.

$a_3 =$ componente seguro, pois quanto maior a quantidade de servidores com cópias de segurança em locais fisicamente distantes, maior a segurança do sistema.

Aqui podem ser definidos, se necessário, os pesos de cada componente. Neste exemplo vamos considerar os componentes com pesos iguais.

Portanto temos que todos os componentes dessa métrica são seguros ou seja podemos usar a fórmula descrita no caso 1.

Para efeitos de ilustração, serão adicionados os seguintes valores hipotéticos ao exemplo: $a_t = 13$, $a_1 = 3$, $a_2 = 11$ e $a_3 = 4$.

O conjunto dos componentes seguros normalizados será formado por:

$$X = \left(\frac{3}{13}, \frac{11}{13}, \frac{4}{13}\right)$$

A média aritmética dos componentes seguros normalizados e conseqüêntemente a fórmula da métrica será dada por:

$$F = \overline{X} = \left(\frac{\frac{3}{13} + \frac{11}{13} + \frac{4}{13}}{3}\right) = \left(\frac{0,2307 + 0,8461 + 0,3076}{3}\right) = \frac{1,3844}{3} = 0,4614$$

Esse valor mostra que os recursos de disponibilidade e confiabilidade dos servidores da Infovia necessitam de melhorias. Tais melhorias devem ser dedicadas a redundância dos servidores (0,2307) e nos backups fisicamente distantes (0,3076). Um ponto positivo é a relação dos servidores que estão no programa de backup $0,8461$, mas neste caso o ideal é que esse número fique próximo do valor máximo.

Caso 2 - *M é composta somente por componentes inseguros.*

Considere Y o conjunto dos componentes seguros normalizados. A fórmula de M também será dada pela média aritmética dos componentes seguros normalizados. Porém, um detalhe aqui deve ser notado. Seja CI um componente inseguro qualquer. Quando CI assume valores próximos de 1, os

riscos de segurança aumentam, ou seja, para preservarmos a relação 0 = baixa segurança e 1 = alta segurança, a fórmula deve sofrer a seguinte adequação:

$$F_M = \left(1 - \overline{Y}\right)$$

donde $0 \leq F_M \leq 1$ e 0 representando o valor mínimo e 1 o valor máximo.

Caso 3 - *M é composta por componentes seguros e inseguros.*

Nesse caso devemos considerar dois conjuntos, X o conjunto dos componentes seguros normalizados e Y o conjunto dos componentes seguros normalizados. Aplicando as fórmulas dos casos 1 e 2 em cada conjunto vamos ter:

$$F_{seg} = \overline{X} \; e \; F_{ins} = \left(1 - \overline{Y}\right)$$

onde F_{seg} denota o resultado da média aritmética dos componentes seguros normalizados e F_{ins} denota o resultado da média aritmética dos componentes inseguros normalizados.

A fórmula de M será dada então pela média aritmética entre F_{seg} e F_{ins}:

$$F_M = \frac{F_{seq} + F_{ins}}{2}$$

A média aritmética entre os componentes normalizados cumpre os requisitos da fórmula pois como $0 \leq F_{seq} \leq 1$ e $0 \leq F_{ins} \leq 1$ então $0 \leq F_M \leq 1$. Além disso, a análise dos valores máximos e mínimos de F_{seq} e F_{ins} mostra que a média aritmética preserva as relações entre os valores e seu respectivo significado para a segurança:

- Quando $F_{seq} \approx 1$ e $F_{ins} \approx 1$ ou seja, o nível de segurança está alto em ambos componentes então $F_M \approx 1$ também.
- Quando $F_{seq} \approx 1$ e $F_{ins} \approx 0$ ou seja, somente um dos componentes está com um bom nível de segurança então $F_M \approx 0,5$. Resultado análogo para $F_{seq} \approx 0$ e $F_{ins} \approx 1$.
- Quando $F_{seq} \approx 0$ e $F_{ins} \approx 0$ ou seja, o nível de segurança está demasiadamente baixo em ambos componentes então $F_M \approx 0$ também.

Exemplo 3 - Considere a métrica que trata das infecções de vírus no perímetro da Rede Municipal. O conjunto de componentes será o seguinte: $a_1 =$ número de computadores infectados, $a_2 =$ número de computadores com antivírus instalado, $a_3 =$ número de computadores com antivírus e assinaturas de vírus atuais, $a_4 =$ número de vírus reportado de alta criticidade, a_5 número de computadores com *antispyware* instalado e a_6 número de computadores com *antispyware* com assinaturas atuais . Os valores para a_t serão: $a_{t1} =$ número de computadores, $a_{t2} =$ número de vírus reportado e para os componentes a_3 e a_6, os respectivos valores totais serão a_2 e a_5.

Vamos analisar os componentes a fim de dividí-los em seguros ou inseguros.

$a_1 =$ componente inseguro, pois quanto mais computadores infectados, maiores são os riscos de problemas de segurança.

$a_2 =$ componente seguro, pois quanto mais computadores com antivírus instalados, menores são os riscos de problemas de segurança.

$a_3 =$ componente seguro, pois quanto mais antivírus com assinaturas de vírus atuais, menores são os riscos de segurança.

$a_4 =$ componente inseguro, pois um alto número de vírus de alta criticidade pode representar um aumento nos riscos de segurança.

$a_5 =$ componente seguro, pois quanto mais computadores com *antispyware* instalado, menores são os riscos de problemas de segurança.

$a_6 =$ componente seguro, pois quanto mais *antispyware* com assinaturas atuais, menores são os riscos de segurança.

Para efeito de ilustração serão adicionados os seguintes dados hipotéticos ao exemplo: $a_{t1} = 70$, $a_{t2} = 30$, $a_1 = 48$, $a_2 = 58$, $a_3 = 40$, $a_4 = 10$, $a_5 = 44$ e $a_6 = 40$.

Os cálculos de F_{seg} e F_{ins} serão:

$$F_{seg} = \overline{X} = \left(\frac{\frac{a_2}{a_{t1}} + \frac{a_3}{a_2} + \frac{a_5}{a_{t1}} + \frac{a_6}{a_5}}{4} \right) = \left(\frac{\frac{58}{70} + \frac{40}{58} + \frac{44}{70} + \frac{40}{44}}{4} \right) = \left(\frac{0{,}8285 + 0{,}6896 + 0{,}6285 + 0{,}9090}{4} \right) = 0,7639$$

$$F_{ins} = \left(1 - \overline{Y}\right) \Rightarrow \overline{Y} = \left(\frac{\frac{a_1}{a_{t1}} + \frac{a_4}{a_{t2}}}{2} \right) = \left(\frac{\frac{48}{70} + \frac{10}{30}}{2} \right) = \left(\frac{0,6857 + 0,3333}{2} \right) = 0,5095$$

Portanto, $F_{ins} = (1 - 0,5095) = 0,4905$

Assim,

$$F_M = \left(\frac{F_{seg} + F_{ins}}{2} \right) = \left(\frac{0,7639 + 0,6247}{2} \right) = 0,6943$$

Uma rápida análise dos resultados acima mostra que apesar dos bons resultados obtidos nos componentes de segurança, aproximadamente 83% dos computadores possuem antivírus, 69% possuem assinaturas de vírus atualizadas, 63% dos computadores possuem *antispyware* e 90% estão com as assinaturas antispam atualizadas. O alto número de computadores infectados, 68%, diminuiu o resultado final da métrica. Tais números podem sugerir que o antivírus utilizado pode ser ineficaz ou então que as configurações de scaneamento periódicas estão desabilitadas. O resultado só não foi pior devido ao baixo número de vírus considerados críticos, 0.333% que foram reportados.

4.2.2 Modelo 2

O modelo 2 apresenta algumas melhorias com relação ao tratamento das relações entre os diferentes componentes de uma métrica. Ao tratar tais relações, o modelo prevê alterações no cálculo da fórmula de uma métrica. O modelo 2 será apresentado utilizando conceitos já definidos no modelo 1.

Considere cada um dos componentes $a_1, a_2, a_3, ..., a_n$ como um conjunto próprio. O a_t correspondente será o conjunto que contém os respectivos a_i. Assim, $a_1 \subset a_{t1}$, $a_2 \subset a_{t2}$ e assim por diante.

Seja M uma métrica que visa medir a segurança das conexões entre os prédios da Rede Metropolitana de Acesso Aberto. Tomemos por X, o conjunto formado pelos prédios da MBAN. X é o

chamado valor total ou componente máximo da métrica M. Considere dois componentes seguros a_1 e a_2 da métrica tais que:

a_1 é um subconjunto de X ($a_1 \subset X$) onde a_1 representa o número de prédios que possuem recursos de firewall ou algum outro controle de acesso lógico.

a_2 é um subconjunto de X ($a_2 \subset X$) onde a_2 representa o número de prédios que possuem criptografia entre as conexões.

O modelo 1 afirma que a fórmula da métrica, nesse caso, é dada simplesmente pela média aritmética entre os componentes. Entretanto, podemos considerar a existência de um outro subconjunto a_3 com $a_3 = a_1 \cap a_2$, ou seja a_3 é o conjunto dos prédios que possuem recursos de firewall e criptografia entre as conexões. No modelo anterior, não consideramos a existência de um componente que agregasse as propriedades de um ou mais outros componentes, que neste caso seria representado pela intersecção entre conjuntos.

Vamos analisar em termos de segurança a existência de componentes que representem intersecções de conjuntos. No modelo 1, a situação ideal para obter a segurança máxima de uma métrica, é que ambos os componentes (a_1 e a_2) atinjam seus valores máximos. Porém, a inserção de um novo componente altera a situação que representa a segurança máxima para o modelo 2. O cálculo da fórmula agora, deve privilegiar os componentes que possuem, por exemplo, ao mesmo tempo recursos de firewall e criptografia, ou seja, os componentes que representam a intersecção. Quanto maior o número de recursos, ou intersecções, que um componente possui, maior deve ser o seu peso em relação aos outros componentes.

Cálculo da fórmula

O objetivo do modelo é aumentar a confiabilidade do cálculo do indicador de segurança. Para isso, os componentes presentes na fórmula serão balanceados utilizando diferentes pesos e um outro fator será apresentado: o componente relativo a intersecção entre os conjuntos.

O primeiro passo para a atualização da fórmula é verificar se a métrica possui algum componente máximo, ou conjunto de valor máximo, com dois ou mais subconjuntos. Em seguida, deve-se classificar cada um dos componentes da métrica.

O modelo 1 afirma que dada uma métrica M,

1. M é composta somente por componentes seguros;
2. M é composta somente por componentes inseguros;
3. M é composta por componentes seguros e inseguros;

Vamos analisar o caso em que a métrica é composta somente por componentes seguros e a partir daí serão deduzidas as fórmulas para os demais casos.

M é composta somente por componentes seguros

No caso em que não existem conjuntos de valor máximo com dois ou mais subconjuntos relacionados, o cálculo da fórmula se reduz ao cálculo da média aritmética entre os componentes, conforme

definido no modelo 1 [53]. O caso a ser considerado aqui é o da existência de conjuntos de valor máximo com ao menos dois subconjuntos relacionados.

Iniciaremos a construção da fórmula com o caso em que o número de subconjuntos de um conjunto de valor máximo é igual a 2, passaremos para o caso em que este número é igual a 3 e depois a fórmula será generalizada. Considere uma métrica M, composta por um conjunto de valor máximo T e dois conjuntos A_1 e A_2 tal que $A_1 \subset T$ e $A_2 \subset T$. Seja $I_{1,2}$ o conjunto formado pela intersecção entre os conjuntos A_1 e A_2. O número de elementos, ou cardinalidade, de cada um dos conjuntos acima é o seguinte:

- $a_1 = \#A_1$
- $a_2 = \#A_2$
- $i_{1,2} = \#I_{1,2}$
- $t = \#T$

onde $\#X$ denota a cardinalidade do conjunto X.

A fórmula para o caso em que o número de subconjuntos é igual a 2, será construída utilizando a média ponderada entre os subconjuntos. Os pesos serão distribuídos da seguinte forma: peso 2 para o conjunto da intersecção e peso 1 para os demais conjuntos. O peso para o conjunto da intersecção foi escolhido com base no número de subconjuntos de T que em nosso caso é 2. Os demais subconjuntos foram definidos com peso 1. Abaixo a fórmula,

$$F_2 = \frac{(2)(\frac{i_{1,2}}{t}) + (1)(\frac{a_1}{t}) + (1)(\frac{a_2}{t})}{(2+1+1)}$$

É importante que se faça uma análise dos máximos e mínimos da fórmula. O valor máximo atingido pela fórmula é 1 e significa que todos os requisitos de segurança estão sendo cumpridos. Em contrapartida, o valor mínimo é 0 e significa que nenhum requisito de segurança da métrica está sendo cumprido.

A segurança máxima é atingida quando o número de elementos de $I_{1,2}$ é igual ao número de elementos T, ou seja, que $i_{1,2} = t$. Porém, isso só será possível quando $A_1 = A_2$. Se $A_1 = A_2$ então $I_{1,2} = A_1 = A_2$ e $a_1 = a_2 = i_{1,2} = t$. Calculando a fórmula, vamos ter que:

$$F_2 = \frac{(2)(\frac{t}{t}) + (1)(\frac{t}{t}) + (1)(\frac{t}{t})}{(2+1+1)} = \frac{4}{4} = 1$$

A segurança mínima é atingida se nenhum dos requisitos de segurança foi cumprido, ou seja, se $A_1 = A_2 = I_{1,2} = \varnothing$. Nestas condições, o número de elementos de A_1, A_2 e $I_{1,2}$ será 0. Calculando a fórmula, vamos ter que:

$$F_2 = \frac{(2)(\frac{0}{t}) + (1)(\frac{0}{t}) + (1)(\frac{0}{t})}{(2+1+1)} = \frac{0}{4} = 0$$

A análise dos máximos e mínimos, mostrou que a fórmula é consistente com os requisitos definidos. Vamos então prosseguir com a construção da fórmula.

Considere agora uma métrica M, composta por um conjunto de valor máximo T e três conjuntos A_1, A_2 e A_3 tal que $A_1 \subset T$, $A_2 \subset T$ e $A_3 \subset T$. Seja $I_{1,2}$ o conjunto formado pela intersecção entre os conjuntos A_1 e A_2, $I_{1,3}$ o conjunto formado pela intersecção entre os conjuntos A_1 e A_3, $I_{2,3}$ o conjunto formado pela intersecção entre os conjuntos A_2 e A_3 e $I_{1,2,3}$ o conjunto formado pela intersecção entre os conjuntos A_1, A_2 e A_3. O número de elementos, ou cardinalidade, de cada um dos conjuntos acima é o seguinte:

- $a_1 = \#A_1$
- $a_2 = \#A_2$
- $a_3 = \#A_3$
- $i_{1,2} = \#I_{1,2}$
- $i_{1,3} = \#I_{1,3}$
- $i_{2,3} = \#I_{2,3}$
- $i_{1,2,3} = \#I_{1,2,3}$
- $t = \#T$

Os pesos serão distribuídos da seguinte forma: peso 3 para o conjunto $I_{1,2,3}$, peso 2 para os outros conjuntos que representam intersecções e peso 1 para os demais conjuntos.

$$F_3 = \frac{(3)(\frac{i_{1,2,3}}{t}) + (2)(\frac{i_{1,2}}{t}) + (2)(\frac{i_{1,3}}{t}) + (2)(\frac{i_{2,3}}{t}) + (1)(\frac{a_1}{t}) + (1)(\frac{a_2}{t}) + (1)(\frac{a_3}{t})}{(3+2+2+2+1+1+1)}$$

A mesma análise de máximos e mínimos deve novamente ser feita neste caso. Note que os resultados não mudam já que os requisitos para o nível máximo de segurança são que $i_{1,2,3} = t$ ou seja, que $A_1 = A_2 = A_3$. Assim, teremos que o número de elementos de todos os conjuntos envolvidos é t. Aplicando este valor a fórmula vamos chegar que para o nível máximo de segurança o resultado será 1.

Analogamente, para o nível mínimo de segurança nenhum dos requisitos é respeitado o que significa que $A_1 = A_2 = A_3 = \varnothing$. A intersecção entre conjuntos vazios é o próprio conjunto vazio. Esse fato implica que todos os conjuntos não possuem elementos. Fazendo $a_1 = a_2 = a_3 = i_{1,2} = i_{1,3} = i_{2,3} = i_{1,2,3} = 0$ vamos ter que o resultado será 0.

Vamos agora generalizar o cálculo da fórmula para o caso em que o número de subconjuntos de T é igual a n.

Considere uma métrica M formada por um conjunto de valor máximo T com $A_1, A_2, ..., A_n$ subconjuntos de T. A cardinalidade de cada um dos subconjuntos será denotada da seguinte forma: $a_j = \#A_j$.

Os conjuntos que representam as intersecções serão denotados da seguinte maneira: $I_{1,2}$ indica a intersecção entre os conjuntos A_1 e A_2; $I_{2,4,7}$ indica a intersecção entre os conjuntos A_2, A_4 e A_7; $I_{4,5,8,10}$ indica a intersecção entre os conjuntos A_4, A_5, A_8 e A_{10} e assim sucessivamente. Analogamente, a cardinalidade dos conjuntos de intersecção será denotada por $i_{1,2}$, $i_{2,4,7}$ e assim em diante.

A fórmula será construída utilizando uma regra geral para a obtenção de cada um dos termos. O termo de peso n da fórmula é obtido pela razão entre a cardinalidade da intersecção entre os n subconjuntos e a cardinalidade do conjunto T. O termo de peso $(n-1)$ é obtido somando todas as razões entre a cardinalidade da intersecção dos $n-1$ conjuntos e a cardinalidade do conjunto T. Continuando tal processo, todos os termos serão obtidos. O denominador é formado pela soma dos pesos de cada um dos termos. Cada uma das combinações C_k^n representa a quantidade de subconjuntos em cada um dos termos 1 até n. A versão generalizada da fórmula é a seguinte:

$$F_n = \frac{n\left(\frac{i_{1,\ldots,n}}{t}\right) + (n-1)\left(\frac{i_{1,\ldots,n-1}}{t} + \ldots + \frac{i_{2,\ldots,n}}{t}\right) + \ldots + 2\left(\frac{i_{1,2}}{t} + \ldots + \frac{i_{n,n-1}}{t}\right) + \left(\frac{a_1}{t} + \ldots + \frac{a_n}{t}\right)}{n\left(C_n^n\right) + (n-1)\left(C_{n-1}^n\right) + \ldots + (2)\left(C_2^n\right) + (1)\left(C_1^n\right)}$$

Podemos ainda simplificar o denominador relembrando que $C_n^n = 1$ e $C_1^n = n$.

Porém, falta um último detalhe para que a construção da fórmula seja finalizada. A fórmula é válida para somente um conjunto de valor máximo. Para m conjuntos de valores máximos devemos fazer o cálculo individualmente para cada m e depois calcular a média aritmética entre os resultados.

M é composta somente por componentes inseguros

A fórmula para o caso em que M é composta somente por componentes inseguros será calculado nos mesmos moldes do modelo 1, para que a relação 0 = baixa segurança e 1 = alta segurança seja mantida, a fórmula sofrerá a seguinte adequação:

$$F_n = 1 - \left(\frac{n\left(\frac{i_{1,\ldots,n}}{t}\right) + (n-1)\left(\frac{i_{1,\ldots,n-1}}{t} + \ldots + \frac{i_{2,\ldots,n}}{t}\right) + \ldots + 2\left(\frac{i_{1,2}}{t} + \ldots + \frac{i_{n,n-1}}{t}\right) + \left(\frac{a_1}{t} + \ldots + \frac{a_n}{t}\right)}{n\left(C_n^n\right) + (n-1)\left(C_{n-1}^n\right) + \ldots + (2)\left(C_2^n\right) + (1)\left(C_1^n\right)}\right)$$

M é composta por componentes seguros e inseguros

Assim como para o caso em que M é composta somente por componentes inseguros, a fórmula para o caso em que a métrica possui componentes seguros e inseguros deverá ser adequada.

Primeiramente devem ser realizados todos os cálculos, separadamente, para os componentes seguros e inseguros, utilizando as fórmulas descritas acima. Os resultados podem ser divididos em dois conjuntos: X e Y. A média aritmética entre os elementos de cada um dos conjuntos é denotada por: $F_{seg} = \overline{X}$ e $F_{ins} = \overline{Y}$.

A fórmula será então calculada aplicando a média aritmética entre F_{seg} e F_{ins}:

$$F_n = \frac{F_{seg} + F_{ins}}{2}$$

Exemplo 2 - Considere o exemplo 3 apresentado na descrição do modelo 1. Vamos utilizá-lo para identificar as diferenças entre os modelos. Considere a métrica que trata das infecções de vírus no perímetro da Rede Municipal. O conjunto de componentes será o seguinte: a_1 = número de computadores infectados, a_2 = número de computadores com antivírus instalado, a_3 = número de computadores com antivírus e assinaturas de vírus atuais, a_4 = número de vírus reportado de alta

criticidade, a_5 o número de computadores com *antispyware* instalado e a_6 o número de computadores com *antispyware* com assinaturas atuais . Os valores para a_t serão: a_{t1} = número de computadores, a_{t2} = número de vírus reportado e para os componentes a_3 e a_6, os respectivos valores totais serão a_2 e a_5.

A divisão dos componentes é a seguinte, componentes seguros = a_2, a_3, a_5 e a_6 e componentes inseguros = a_1 e a_4.

Os valores dos componentes são: $a_{t1} = 70$, $a_{t2} = 30$, $a_1 = 48$, $a_2 = 58$, $a_3 = 40$, $a_4 = 10$, $a_5 = 44$ e $a_6 = 40$.

Seja o conjunto $I_{2,5}$ formado pela intersecção entre os conjuntos A_2 e A_5. O conjunto retrata o número de computadores que possui antivírus e *antispyware* instalado. A cardinalidade do conjunto $i_{2,5} = 32$. Vamos refazer os cálculos levando em consideração tal componente.

O cálculo da fórmula será dividido em duas partes. A primeira parte é o cálculo de F_2 entre os componentes a_2 e a_5 que é o caso em que temos a intersecção entre estes dois conjuntos. Na outra parte, os componentes restantes devem ser divididos em seguros e inseguros aplicando o mesmo método do modelo 1.

$$F = \frac{F_2 + F_{seg} + F_{ins}}{3}$$

$$F_2 = \frac{2\left(\frac{i_{2,5}}{a_{t1}}\right) + \frac{a_2}{a_{t1}} + \frac{a_5}{a_{t1}}}{2+1+1} = \frac{2\frac{32}{70} + \frac{58}{70} + \frac{44}{70}}{4} = 0,5928$$

$$F_{seg} = \frac{\frac{a_3}{a_2} + \frac{a_6}{a_5}}{2} = \frac{\frac{40}{58} + \frac{40}{44}}{2} = 0,7993$$

$$F_{ins} = \frac{\frac{a_1}{a_{t1}} + \frac{a_4}{a_{t2}}}{2} = \frac{\frac{48}{70} + \frac{10}{30}}{2} = 0,5095$$

$$F = \frac{F_2 + F_{seg} + F_{ins}}{3} = \frac{0,5928 + 0,7993 + 0,5095}{3} = 0,6338$$

O modelo 1 aplicado neste mesmo exemplo teve como resultado $0,6943$. Já o modelo 2 obteve $0,6338$. Comparando os resultados entre os modelos nota-se que apesar de próximos, a inserção de pesos no cálculo da fórmula tornou o modelo 2 mais rigoroso. Na seção a seguir este resultado será demonstrado.

4.3 Diferenças entre os modelos

O exemplo 2 construído na subseção 4.2.2 mostrou uma comparação entre os resultados obtidos pelos modelos 1 e 2. Naquele caso, o resultado do modelo 2 foi numericamente inferior ao resultado do modelo 1. A presente seção tem como objetivo demonstrar este resultado, ou seja, que a inserção dos pesos no modelo 2 o torna mais rigoroso que o modelo 1. A demonstração será construída para o caso em que o número de conjuntos é igual a 2 e também para o caso em que o número de conjuntos é igual 3.

Primeiramente, vamos considerar o caso em que o número de conjuntos é igual a 2 e com 1 conjunto de intersecção. Seja M uma métrica, composta por um conjunto de valor máximo T e dois conjuntos A_1 e A_2 tal que $A_1 \subset T$ e $A_2 \subset T$. Seja $I_{1,2}$ o conjunto formado pela intersecção entre os

conjuntos A_1 e A_2. O número de elementos, ou cardinalidade, de cada um dos conjuntos acima é o seguinte:

- $a_1 = \#A_1$
- $a_2 = \#A_2$
- $i_{1,2} = \#I_{1,2}$
- $t = \#T$

Note também, que as seguintes desigualdades são válidas: $i_{1,2} \leq a_1$ e $i_{1,2} \leq a_2$.
A fórmula para o modelo 1 é dada da seguinte forma:

$$F_1 = \frac{\frac{a_1}{t} + \frac{a_2}{t}}{2} = \frac{a_1 + a_2}{2t}$$

Enquanto que a fórmula para o modelo 2 é:

$$F_2 = \frac{2\left(\frac{i_{1,2}}{t}\right) + \frac{a_1}{t} + \frac{a_2}{t}}{4} = \frac{2(i_{1,2}) + a_1 + a_2}{4t}$$

Portanto, gostaríamos de demonstrar que $\frac{a_1+a_2}{2t} \geq \frac{2t+a_1+a_2}{4t}$. Vamos utilizar a demonstração por absurdo, supondo o contrário, ou seja, a inversão da desigualdade, para chegar em um absurdo. Suponha então que:

$$\begin{aligned}
\frac{a_1 + a_2}{2t} &< \frac{2(i_{1,2}) + a_1 + a_2}{4t} \\
4t(a_1 + a_2) &< 2t(2(i_{1,2}) + a_1 + a_2) \\
4ta_1 + 4ta_2 &< 4ti_{1,2} + 2ta_1 + 2ta_2 \\
2ta_1 + 2ta_2 &< 4ti_{1,2} \\
2t(a_1 + a_2) &< 4ti_{1,2} \\
a_1 + a_2 &< 2i_{1,2}
\end{aligned}$$

Este resultado nos leva a um absurdo, pois tomemos as seguintes desigualdades: $i_{1,2} \leq a_1$ e $i_{1,2} \leq a_2$. Somando-as vamos ter que: $a_1 + a_2 \geq 2i_{1,2}$, ou seja, uma contradição. Portanto,

$$\frac{a_1 + a_2}{2t} \geq \frac{2t + a_1 + a_2}{4t}$$

E concluímos que para o caso com dois conjuntos, o resultado do modelo 1 é sempre maior ou igual ao resultado do modelo 2.

Considere o caso em que o número de conjuntos é igual a 3. Seja M uma métrica, composta por um conjunto de valor máximo T e três conjuntos A_1, A_2 e A_3 tal que $A_1 \subset T$, $A_2 \subset T$ e $A_3 \subset T$. Seja $I_{1,2}$ o conjunto formado pela intersecção entre os conjuntos A_1 e A_2, $I_{1,3}$ o conjunto formado pela intersecção entre os conjuntos A_1 e A_3, $I_{2,3}$ o conjunto formado pela intersecção entre os conjuntos A_2 e A_3 e $I_{1,2,3}$ o conjunto formado pela intersecção entre os conjuntos A_1, A_2 e A_3. O número de elementos, ou cardinalidade, de cada um dos conjuntos acima é o seguinte:

- $a_1 = \#A_1$
- $a_2 = \#A_2$
- $a_3 = \#A_3$
- $i_{1,2} = \#I_{1,2}$
- $i_{1,3} = \#I_{1,3}$
- $i_{2,3} = \#I_{2,3}$
- $i_{1,2,3} = \#I_{1,2,3}$
- $t = \#T$

As seguintes desigualdades são válidas:

- $i_{1,2,3} \leq a_1$, $i_{1,2,3} \leq a_2$ e $i_{1,2,3} \leq a_3$
- $i_{1,2} \leq a_1$ e $i_{1,2} \leq a_2$
- $i_{1,3} \leq a_1$ e $i_{1,3} \leq a_3$
- $i_{2,3} \leq a_2$ e $i_{2,3} \leq a_3$

A este conjunto de desigualdades chamaremos de (1).
A fórmula para o modelo 1 é dada da seguinte forma:

$$F_1 = \frac{\frac{a_1}{t} + \frac{a_2}{t} + \frac{a_3}{t}}{3} = \frac{a_1 + a_2 + a_3}{3t}$$

Enquanto que a fórmula para o modelo 2 é:

$$F_2 = \frac{3\left(\frac{i_{1,2,3}}{t}\right)+2\left(\frac{i_{1,2}}{t}\right)+2\left(\frac{i_{1,3}}{t}\right)+2\left(\frac{i_{2,3}}{t}\right)+\frac{a_1}{t}+\frac{a_2}{t}+\frac{a_3}{t}}{12} = \frac{3(i_{1,2,3})+2(i_{1,2})+2(i_{1,3})+2(i_{2,3})+a_1+a_2+a_3}{12t}$$

Portanto, gostaríamos de demonstrar que:

$$\frac{a_1 + a_2 + a_3}{3t} \geq \frac{3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3}) + a_1 + a_2 + a_3}{12t}$$

Será utilizada a mesma técnica de demonstração por absurdo. Vamos supor que esta desigualdade não é verdadeira, ou seja, que o primeiro membro é menor que o segundo, e chegar em um absurdo.

$$\begin{aligned}
\frac{a_1 + a_2 + a_3}{3t} &< \frac{3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3}) + a_1 + a_2 + a_3}{12t} \\
12t(a_1 + a_2 + a_3) &< 3t(3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3}) + a_1 + a_2 + a_3) \\
12ta_1 + 12ta_2 + 12ta_3 &< 9ti_{1,2,3} + 6ti_{1,2} + 6ti_{1,3} + 6ti_{2,3} + 3ta_1 + 3ta_2 + 3ta_3 \\
9t(a_1 + a_2 + a_3) &< 3t(3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3})) \\
3(a_1 + a_2 + a_3) &< 3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3})
\end{aligned}$$

Mas isto é um absurdo, pois somando as desigualdades (1) vamos ter que: $3(a_1 + a_2 + a_3) \geq 3(i_{1,2,3}) + 2(i_{1,2}) + 2(i_{1,3}) + 2(i_{2,3})$. Portanto, para o caso de 3 conjuntos, o resultado do modelo 1, é sempre maior ou igual ao resultado do modelo 2.

Para o caso com n conjuntos, a demonstração pode ser feita de maneira análoga aos casos para 2 e 3 conjuntos.

4.4 Métricas de segurança para MBANs

A seguir serão apresentadas doze métricas de segurança para Redes Metropolitanas de Acesso Aberto, utilizando o modelo proposto na primeira seção deste capítulo. A padronização permite a criação de outras métricas de segurança para Infovias Municipais além das citadas aqui. É interessante citar que a quantidade e diversidade de métricas que serão aplicadas na Rede Municipal influencia diretamente no conhecimento sobre a segurança da rede.

As métricas propostas neste trabalho possuem uma característica diferente de abordagens tradicionalmente utilizadas, que é a partir do agrupamento de várias métricas de acordo com um grupo comum, calcular o indicador de segurança deste grupo. Considere, por exemplo, as seguintes métricas de segurança propostas pelo ISO/IEC 27002:

- Porcentagem de canais de comunicação seguros de acordo com a política definida.
- Porcentagem de usuários móveis que acessam as instalações da empresa usando métodos seguros de comunicação.
- Porcentagem de firewalls de estações, servidores, e de perímetros de rede configurados de acordo com a política vigente.

Apesar das métricas estarem organizadas em um grupo comum chamado de "Controle de acesso a rede", elas são tratadas individualmente. Cada métrica possui sua própria fórmula e não existem recomendações sobre como analisar o grupo "Controle de acesso a rede". Nossa proposta consiste em agrupar as três métricas em somente uma, visando a análise global do grupo através do cálculo da fórmula. Ou seja, a partir do resultado de cada uma das métricas, calcular um único índice para as três métricas que, neste caso, representaria o nível do "Controle de acesso a rede" da organização.

O agrupamento é importante pois unifica diversos resultados em somente um número, facilitando a interpretação de resultados do corpo não-técnico da organização. Quando necessário o cálculo individual das métricas também pode ser realizado.

Métrica 1 - Segurança entre os prédios da MBAN

- **Objetivo:** Analisar e aumentar o nível de segurança das conexões entre os prédios da Infovia.
- **Métrica:** Taxa de prédios que são interconectados utilizando-se tecnologias com suporte à segurança (criptografia, VPNs, VLANs e etc).

- **Medidas:** i) Número de prédios conectados a rede municipal, ii) tipo de tecnologia de interconexão de rede por prédio, iii) número de prédios que possuem criptografia entre as conexões, iv) número de prédios que possuem recursos de firewall entre as conexões, v) protocolo criptográfico utilizado.
- **Origem dos dados:** Entrevistas e auditoria nos equipamentos de rede que fazem as conexões.
- **Freqüência:** Semestral.
- **Classificação da métrica:** Estrutura de rede.
- **Fórmula:** Seja a_{t1} = número total de prédios, a_1 = número de prédios que possuem recursos de firewall ou controles de acesso lógico entre as conexões, a_2 = número de prédios que possuem criptografia entre as conexões e $i_{1,2}$ = número de prédios que possuem recursos de firewall e criptografia entre as conexões. Note que: a_1 e a_2 são componentes seguros. Antes de apresentar as fórmulas, serão definidos diferentes pesos para o tipo de criptografia utilizado. Considere a Tabela 4.2 [5].

Level	Protection	Symmetric	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals *Only acceptable for authentication tag size*	32	-	-	-	-	-
2	Very short-term protection against small organizations *Should not be used for confidentiality in new systems*	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations *Smallest general-purpose level,* *Use of 2-key 3DES restricted to 2^{40} plaintext/ciphertexts, protection from 2008 to 2011*	80	1248	160	1248	160	160
5	Legacy standard level *Use of 2-key 3DES restricted to 10^6 plaintext/ciphertexts, protection from 2008 to 2018*	96	1776	192	1776	192	192
6	Medium-term protection *Use of 3-key 3DES,* *protection from 2008 to 2028*	112	2432	224	2432	224	224
7	Long-term protection *Generic application-independent recommendation, protection from 2008 to 2038*	128	3248	256	3248	256	256
8	"Foreseeable future" *Good protection against quantum computers*	256	15424	512	15424	512	512

Fig. 4.2: Tamanho de chave - Recomendado pelo ECRYPT. Extraída de [5]

Tab. 4.3: Pesos de acordo com o tamanho da chave criptográfica

Nível	Peso (p)
1	0,125
2	0,250
3	0,375
4	0,5
5	0,625
6	0,75
7	0,875
8	1

A Tabela 4.2, desenvolvida pela ECRYPT - *European Network of Excellence for Cryptology* [54], fornece diferentes níveis de segurança de acordo com o tamanho da chave e o tipo de protocolo criptográfico utilizado (simétrico, assimétrico, logaritmo discreto, curva elíptica e hash). Para saber o peso p da fórmula, deve-se associar o nível encontrado na Tabela 4.2, com o da Tabela 4.3.

Então, as fórmulas serão dadas por:

$$\text{Modelo 1: } F_1 = \overline{X} \text{ com } X = \left\{ \frac{a_1}{a_{t1}}, \left(p \frac{a_2}{a_{t1}} \right) \right\}$$

$$\text{Modelo 2: } F_1 = \frac{2\frac{i_{1,2}}{t_1} + \frac{a_1}{t_1} + p\frac{a_2}{t_1}}{2+1+1}$$

Note que o valor de $i_{1,2}$ já leva em consideração o peso dado pelo tipo de criptografia utilizada.

Métrica 2 - Requisitos de segurança da rede VoIP

- **Objetivo:** Analisar requisitos de segurança da rede VoIP da Rede metropolitana de acesso aberto.
- **Métrica:** Taxa de ramais VoIP que utilizam criptografia e que estão separados da rede de dados. Porcentagem de ligações não concluídas.
- **Medidas:** i) Número total de ramais VoIP, ii) Número de ramais VoIP por prédio, iii) Número de ramais VoIPs cifrados, iv) Número de ramais VoIP que estão em redes separadas da rede de dados, v) Número total de ligações, vi) Número de ligações completadas com sucesso.
- **Origem dos dados:** Auditoria no servidor VoIP, ferramentas de gerência para redes VoIP, entrevistas com administradores da rede.
- **Freqüência:** Mensal ou Trimestral.
- **Classificação da métrica:** Serviço.

- **Fórmula:** Seja a_{t1} = número total de ramais VoIP, a_{t2} = número total de ligações VoIP em um determinado período, a_1 = número de ramais VoIP cifrados, a_2 = número de ramais VoIP que estão em redes separadas da rede de dados, a_3 = número de ligações não concluídas e $i_{1,2}$ = número de ramais VoIP cifrados e em redes separadas da rede de dados. Os componentes a_1 e a_2 são seguros. Já o componente a_3 é inseguro. Então:

$$F_2 = \left(\frac{F_{seg}+F_{ins}}{2}\right) \text{ com } F_{seg} = \overline{X} \text{ e } X = \left\{\frac{a_1}{a_{t1}}, \frac{a_2}{a_{t1}}\right\} \text{ e } F_{ins} = \left(1-\overline{Y}\right) \text{ com } Y = \left\{\frac{a_3}{a_{t2}}\right\}$$

$$\textbf{Modelo 2} \Rightarrow F_2 = \frac{\left(\frac{2\left(\frac{i_{1,2}}{a_{t1}}\right)+\left(\frac{a_1}{a_{t1}}\right)+\left(\frac{a_2}{a_{t1}}\right)}{(2+1+1)}\right)+\left(1-\left(\frac{a_3}{a_{t2}}\right)\right)}{2}$$

Métrica 3 - Gerenciamento das contas de usuários

- **Objetivo:** Diminuição do número de usuários com privilégios administrativos nos prédios públicos da Infovia. Usuários com privilégios de administrador podem realizar qualquer tipo de operação no sistema operacional. Assim, se um atacante consegue o domínio de um usuário com tais privilégios, todo o sistema estará comprometido.
- **Métrica:** Relação de usuários administradores por máquina.
- **Medidas:** i) Número total de estações de trabalho, ii) Número total de contas de usuário, iii) Número de contas com privilégios totais de administrador, iv) Número de computadores que utilizam a conta de Administrador (root) como conta primária do sistema.
- **Origem dos dados:** Ferramentas de auditoria tais como: WinAudit [55], RemoteAssetTracker [56] e CACIC [57].
- **Freqüência:** Trimestral
- **Classificação da métrica:** Tipo de ponto.
- **Fórmula:** Seja a_{t1} = número total de contas de usuários, a_{t2} = número total de computadores, a_1 = número de usuários com privilégios de administrador, a_2 = número de computadores utilizando a conta de Administrador como conta de trabaho. Então:

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_3 = \left(1-\overline{Y}\right) \text{ com } Y = \left\{\frac{a_1}{a_{t1}}, \frac{a_2}{a_{t2}}\right\}$$

Métrica 4 - Disseminação de vírus/trojans/spams

- **Objetivo:** Diminuição da disseminação de vírus/*trojans*/*spams* dentro do perímetro da rede municipal.

- **Métrica:** Taxa atual de infecções de vírus por prédio, comparada com medições anteriores.
- **Medidas:** i) Quantidade de computadores infectados (total e por prédio), ii) Número de computadores por prédio e total, iii) Porcentagem do nível de criticidade (em comparação com a base da Symantec, por exemplo) dos vírus reportados, iv) Número de computadores com anti-vírus e anti-spams e v) Número de computadores com as assinaturas de vírus atuais.
- **Origem dos dados:** se o antivírus for gerenciável, basta checar os logs e alertas de contaminação e coletar os devidos dados; senão, rodar o antivírus remotamente nas máquinas desejadas e coletar os dados.
- **Freqüência:** Mensal ou bimestral.
- **Classificação da métrica:** Tipo de ponto.
- **Fórmula:** Seja a_{t1} = número total de computadores, a_{t2} = número total de vírus reportado, a_1 = número de computadores infectados, a_2 = número de computadores com antivírus instalado, a_3 = número de computadores com assinaturas de vírus desatualizadas, a_4 = número de vírus com alta criticidade, a_5 o número de computadores com *antispyware* instalado, a_6 o número de computadores com *antispyware* com assinaturas atuais e $i_{2,5}$ = número de computadores com antivírus e antispam instalado. Para os componentes a_3 e a_6, os respectivos valores totais serão a_2 e a_5.

  Os componentes são divididos em seguros = a_2, a_3, a_5 e a_6 e inseguros = a_1 e a_4. Então:

$$\textbf{Modelo 1} \Rightarrow F_4 = \left(\frac{F_{seg}+F_{ins}}{2}\right)$$

$$\text{com } F_{seg} = \overline{X} = \left\{\frac{a_2}{a_{t1}}, \frac{a_3}{a_2}, \frac{a_5}{a_{t1}}, \frac{a_6}{a_5}\right\} \text{ e } F_{ins} = \left(1 - \overline{Y}\right) \Rightarrow \overline{Y} = \left\{\frac{a_1}{a_{t1}}, \frac{a_4}{a_{t2}}\right\}$$

$$\textbf{Modelo 2} \Rightarrow F_4 = \left(\frac{F_{2,5}+F_{seg}+F_{ins}}{3}\right)$$

$$\text{Com } F_{2,5} = \frac{2\left(\frac{i_{2,5}}{a_{t1}}\right)+\left(\frac{a_2}{a_{t1}}\right)+\left(\frac{a_5}{a_{t1}}\right)}{(2+1+1)}, F_{seg} = \frac{\frac{a_3}{a_2}+\frac{a_6}{a_5}}{2} \text{ e } F_{ins} = \frac{\frac{a_1}{a_{t1}}+\frac{a_4}{a_{t2}}}{2}$$

Métrica 5 - Tentativas de invasões ao perímetro da MBAN

- **Objetivo:** Dimensionar as tentativas de invasões (com ou sem sucesso) ao perímetro da rede municipal e atestar a efetividade das ferramentas e políticas de defesa do perímetro.
- **Métrica:** Taxa de tentativas de invasão dos últimos períodos e relação de tentativas de invasões entre os diversos prédios que compõem a Infovia.
- **Medidas:** i) Número de computadores expostos à Internet (Com IP fixo ou não), ii) Número de firewalls em todo o perímetro da Infovia, iii) Taxa de tentativa de invasão por VLAN (ou prédio), iv) Número de tentativas de ataques por servidor e v) Relação tentativa sem sucesso / tentativas com sucesso.

- **Origem dos dados:** Instalação de algum Intrusion Detection System (IDS), como o SNORT em diversos pontos da rede. Análise dos logs gerados pela ferramenta.
- **Freqüência:** Mensal.
- **Classificação da métrica:** Estrutura de Rede.
- **Fórmula:** Seja a_{t1} = número total de ataques, a_1 = número de ataques bem sucedidos. Está claro que o componente a_1 é inseguro, portanto:

$$\text{Modelo 1 = Modelo 2} \Rightarrow F_5 = \left(1 - \overline{Y}\right) \text{ com } Y = \left\{\frac{a_1}{a_{t1}}\right\}$$

Métrica 6 - Configurações de segurança da rede sem fio

- **Objetivo:** Aumentar as configurações de segurança das conexões sem fio.
- **Métrica:** Relação das conexões sem fio com criptografia. Taxa de pontos de acesso que utilizam autenticação segura e WPA.
- **Medidas:** i) Número total de pontos de acesso, ii) Número de pontos de acesso que estão habilitados WEP , iii) Número de pontos de acesso que usam WPA ou WPA2 iv) Número de pontos de acesso que não foram trocadas as senhas padrão.
- **Origem dos dados:** Auditoria nos equipamentos, ferramentas de scaneamento em equipamentos sem fio como NetStumbler e AirSnort.
- **Freqüência:** Trimestral ou semestral.
- **Classificação da métrica:** Estrutura de rede.
- **Fórmula:** Seja a_t = número total de pontos de acesso, a_1 = número de pontos de acesso com protocolos de segurança habilitados (incluindo o uso do WEP), a_2 = número de pontos de acesso que não foram trocadas as senhas padrão, a_3 = número de pontos de acesso com o SSID padrão, a_4 = número de pontos de acesso com versões desatualizadas de firmware e software, a_5 = número de pontos de acesso com autenticação aberta.

  O protocolo de segurança para redes sem fio WEP já está obsoleto [58] e não possui os mesmos requisitos de segurança que o de seus sucessores WPA e WPA-2. Porém, muitos especialistas consideram que o WEP ainda trabalha suficientemente bem para ambientes domésticos ou pequenas empresas, e seu desempenho não influi muito na velocidade da rede além de evitar

Wardrivings[1]. Por esse motivo que o componente a_1 sofrerá a atuação de um peso p: se o protocolo de segurança habilitado for o WEP o peso será $0,2$, se o protocolo for o WPA ou WPA-2 o peso será 1. O componente a_1 é seguro, já a_2, a_3, a_4 e a_5 são classificados como inseguros. Portanto a fórmula será calculada da seguinte maneira:

$$\textbf{Modelo 1} \Rightarrow F_6 = \frac{\left(1-\overline{Y}\right)+\left(p\frac{a_1}{a_{t1}}\right)}{2} \text{ com } Y = \left\{\frac{a_2}{a_t}, \frac{a_3}{a_t}, \frac{a_4}{a_t}, \frac{a_5}{a_t}\right\}$$

Considerando a existência de intersecção entre os 5 conjuntos de componentes $a_2, ..., a_5$ o cálculo da fórmula de acordo com o modelo 2 será:

$$\textbf{Modelo 2} \Rightarrow$$

$$Z = 1 - \left(\frac{4\left(\frac{i_{2,3,4,5}}{a_t}\right)+3\left(\frac{i_{2,3,4}}{a_t}+\frac{i_{2,3,5}}{a_t}+\frac{i_{2,4,5}}{a_t}+\frac{i_{3,4,5}}{a_t}\right)+2\left(\frac{i_{2,3}}{a_t}+\frac{i_{2,4}}{a_t}+\frac{i_{2,5}}{a_t}+\frac{i_{3,4}}{a_t}+\frac{i_{3,5}}{a_t}+\frac{i_{4,5}}{a_t}\right)+\left(\frac{a_2}{a_t}+\frac{a_3}{a_t}+\frac{a_4}{a_t}+\frac{a_5}{a_t}\right)}{32}\right)$$

$$F_6 = \frac{p\frac{a_1}{a_{t1}} + Z}{2}$$

Métrica 7 - Disponibilidade e confiabilidade dos servidores

- **Objetivo:** Aumentar a disponibilidade e confiabilidade dos servidores. Diminuição do impacto em eventuais "quedas" de serviços disponibilizados por tais servidores.
- **Métrica:** Taxa dos servidores provedores de serviços que possuem algum tipo de redundância e avaliação do impacto da indisponibilidade de algum desses serviços.
- **Medidas:** i) Quantidade de servidores provedores de serviço, ii) Quantidade de servidores que possuem algum tipo de redundância, iii) Quantidade de servidores que estão no programa de backup, iv) Quantidade de servidores que possuem backup em locais fisicamente distantes , v) Serviços que possuem maior taxa de indisponibilidade, vi) porcentagem de *uptime* (tempo que o computador está no ar) de cada servidor e vii) porcentagem de *downtime* (tempo que o computador está fora do ar) de cada servidor.
- **Origem dos dados:** Auditoria nos servidores.
- **Freqüência:** Trimestral ou semestral.
- **Classificação da métrica:** Serviços.

[1]Trata-se do ato de buscar por redes sem fio deslocando-se dentro de um veículo (daí o "driving"). Além do automóvel, o procedimento envolve também, evidentemente, um computador equipado com Wi-Fi, como um notebook ou um PDA para detectar as redes.

- **Fórmula:** Seja a_{t1} = número total de servidores, a_{t2} = número total de horas , a_1 = número de servidores que possuem redundância, a_2 = número de servidores que estão no programa de backup, a_3 = número de servidores que possuem backup em locais fisicamente distantes, a_4 = média aritmética de *uptime* dos servidores e $i_{1,2}$ = número de servidores com redundância e que estão no programa de backup. A análise dos componentes mostra que: a_1 = componente seguro, pois quanto maior a quantidade de servidores com serviços de redundância, maior a segurança do sistema, a_2 = componente seguro, pois quanto maior a quantidade de servidores no programa de backup, maior a segurança do sistema, a_3 = componente seguro, pois quanto maior a quantidade de servidores com cópias de segurança em locais fisicamente distantes, maior a segurança do sistema e a_4 = componente seguro, pois quanto maior o tempo que o servidor fica no ar, maior a robustez e segurança do sistema. Assim:

$$\textbf{Modelo 1} \Rightarrow F_7 = \overline{X} \text{ com } X = \left\{ \frac{a_1}{a_{t1}}, \frac{a_2}{a_{t1}}, \frac{a_3}{a_{t1}}, \frac{a_4}{a_{t2}} \right\}$$

$$\textbf{Modelo 2} \Rightarrow F_7 = \left(\frac{\left(\frac{2\left(\frac{i_{1,2}}{a_{t1}}\right)+\left(\frac{a_1}{a_{t1}}\right)+\left(\frac{a_2}{a_{t1}}\right)}{(2+1+1)} \right) + \left(\frac{a_3}{a_2}\right)+\left(\frac{a_4}{a_{t2}}\right)}{3} \right)$$

Métrica 8 - Utilização e dimensionamento do link de Internet

- **Objetivo:** Dimensionar a utilização da Internet. Criação de *baseline* para análise de gargalos, uso abusivo, capacidade do link, *outliers* e etc.
- **Métrica:** Taxa de utilização da banda de Internet da MBAN e taxa de computadores que utilizam outros links de Internet.
- **Medidas:** i) Número de prédios da MBAN que possuem acesso à Internet, ii) Tamanho da banda contratada de Internet, iii) Porcentagem de utilização da banda de Internet por prédio (ou por VLAN), iv) Número de computadores que estão conectados à Internet não distribuída pela Infovia.
- **Origem dos dados:** Utilizar ferramentas de análise de tráfego e banda de Internet, além de auditoria com a gerência de rede.
- **Freqüência:** Mensal.
- **Classificação da métrica:** Estrutura de rede e serviços.
- **Fórmula:** Seja a_{t1} = tamanho total da banda alocada para Internet, a_{t2} = número de computadores que possuem acesso à Internet, a_1 = banda média de Internet utilizada e a_2 = número de computadores que estão conectados à internet não distribuída pela Infovia. O componente a_1 é inseguro, pois o alto uso da banda de Internet pode levar a congestionamentos e queda da

disponibilidade de serviços ou mostrar um uso abusivo dos usuários. A utilização de outras fontes de conexão à Internet externas à Rede Municipal pode trazer problemas de segurança, já que a fonte externa pode não estar obedecendo as políticas de acesso definidas no perímetro da MBAN. Um exemplo típico é o acesso não autorizado através de conexões discadas. Portanto, o componente a_2 também é classificado como inseguro. Então:

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_8 = \left(1 - \overline{Y}\right) \text{ com } Y = \left\{\frac{a_1}{a_{t1}}, \frac{a_2}{at2}\right\}$$

Métrica 9 - Aplicação de *patchs* no centro de interconexão

- **Objetivo:** Analisar a eficiência do programa de aplicação de *patch* nos servidores do centro de interconexão.
- **Métrica:** Criticidade das vulnerabilidades detectadas por servidor. A criticidade será medida utilizando o CVSS - Common Vulnerability Score System[2][59].
- **Medidas:** i) Número de servidores, ii) Número de vulnerabilidades detectadas, iii) Pontuação do CVSS para cada vulnerabilidade, iv) Relação pontuação CVSS por servidor.
- **Origem dos dados:** Ferramenta de detecção de vulnerabilidades. Exemplo de ferramentas: Shavlik NetChk Protect [60], GFI LANguard N.S.S [61] e Nessus Vulnerability Scanner [62]. As vulnerabilidades e respectivos índices de CVSS podem ser encontradas nas base de dados do NIST [10] e CERT [8].
- **Freqüência:** Mensal ou bimestral.
- **Classificação da métrica:** Tipos de pontos.
- **Fórmula:** Seja a_{t1} = número de servidores, a_1 = soma das médias dos índices, a_2 = média. Note que a_1 é um componente inseguro pois o CVSS gera valores entre 0 e 10, quanto mais alto o valor maior a severidade da vulnerabilidade. A fórmula será dada através do cálculo da média entre as índices CVSS encontrados pelo número de servidores. Como os índices são números entre 0 e 10, para adequar a escala definida neste trabalho, o índice CVSS será dividido por 10.

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_9 = 1 - \left(\frac{a_1}{a_{t1}}\right)$$

Métrica 10 - Complexidade de senhas

[2]Metodologia que propõe um sistema padronizado de pontuação para vulnerabilidades de segurança desenvolvida por Peter Mell, Karen Scarfone e Sasha Romanosky.

- **Objetivo:** Analisar e aumentar a complexidade das senhas de servidores, roteadores e pontos de acesso da Infovia Municipal.
- **Métrica:** Mensurar o nível de complexidade de senhas de servidores, roteadores e pontos de acesso da Infovia.
- **Medidas:** i) Número de servidores, roteadores e pontos de acesso da Infovia, ii) Número de servidores, roteadores e pontos de acesso que não necessitam de senha para autenticação, iii) Utilizando uma ferramenta de quebra de senha fazer o teste nos equipamentos da rede. Porcentagem de senhas com complexidade baixa, ou seja, senhas baseadas em informações pessoais, com poucos dígitos, nomes próprios e que estejam fora dos padrões definidos nas políticas de segurança. iv) Listar os servidores, roteadores e pontos de acesso de acordo com a baixa complexidade das senhas.
- **Origem dos dados:** Ferramentas de quebra de senha, ou de análise de complexidade de senhas, como Password Strength Meter [63].
- **Freqüência:** Semestral.
- **Classificação da métrica:** Tipos de pontos.
- **Fórmula:** Seja a_{t1} número de servidores, a_{t2} = número de roteadores, a_{t3} número de pontos de acesso, a_1 = média dos índices de segurança (calculados com o uso do Password Strength Meter) das senhas dos servidores, a_2 = média dos índices de segurança das senhas dos roteadores a_3 = média dos índices de segurança das senhas dos pontos de acesso.

  Os componentes a_1, a_2 e a_3 são seguros, já que o Password Strength Meter utiliza a escala $0 =$ baixa complexidade e $1 =$alta complexidade. As fórmulas para o modelo 1 e o modelo 2 são iguais, pois não existe intersecção entre os componentes.

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_{10} = \left(\frac{a_1+a_2+a_3}{3}\right).$$

Métrica 11 - Classificação do tráfego de email

- **Objetivo:** Analisar e classificar o tráfego de e-mail dentro da Infovia. Criação de um indicador do uso do e-mail interno.
- **Métrica:** Classificar o tráfego de e-mail legítimo e não-legítimo no servidor de e-mail da rede municipal.

- **Medidas:** i) Quantidade de e-mails enviados durante determinado período de tempo, ii) Quantidade de e-mails recebidos durante determinado período de tempo, iii) Quantidade de e-mails enviados e recebidos por prédio da Infovia, iv) Tamanho dos emails enviados e recebidos. Dividi-los em três categorias: até 100KB, de 100KB - 1MB e maior que 1MB, v) Quantidade de vírus e spams detectados, dividí-los em categorias: enviados, recebidos e por prédio da rede municipal. vi) Quantidade de spams detectados, dividi-los em categorias: spams enviados, recebidos e por prédio da rede municipal.
- **Origem dos dados:** Auditoria no servidor de e-mail.
- **Freqüência:** Mensal ou trimestral.
- **Classificação da métrica:** Serviços.
- **Fórmula:** Seja a_{t1} = número total de e-mails enviados, a_{t2} = número total de e-mails recebidos, a_1 = número de spams enviados, a_2 = número de spams recebidos, a_3 = número de vírus enviados, a_4 = número de vírus recebidos e a_5 = número de e-mails enviados que possuem mais de 1 mega byte. Os componentes a_1, a_2, a_3 e a_4 tratam da quantidade de spams e vírus detectado nos e-mails do domínio da Rede Municipal. É sabido que o aumento do número de vírus e *spams* detectado causa aumento nos problemas de segurança, portanto tais componentes são classificados como inseguros. Analogamente, e-mails com mais de 1 mega byte dificilmente são considerados como válidos e freqüêntemente vêm acompanhado por pragas virtuais como vírus e cavalos de tróia, ou seja, um tráfego alto de emails com esse tamanho pode significar muitos riscos de segurança. Assim, o componente a_5 também é classificado como inseguro. As fórmulas para o modelo 1 e o modelo 2 são iguais, pois não existe intersecção entre os componentes. Então:

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_{11} = \left(1 - \overline{Y}\right) \text{ com } Y = \left\{ \frac{a_1}{a_{t1}}, \frac{a_2}{a_{t2}}, \frac{a_3}{a_{t1}}, \frac{a_4}{a_{t2}}, \frac{a_5}{a_{t1}}, \frac{a_6}{a_{t2}} \right\}$$

Métrica 12 - Segmentação da rede metropolitana de acesso aberto

- **Objetivo:** Medir o nível de segmentação da rede metropolitana de acesso aberto. Pontos que não possuem o mesmo domínio de interesse devem ser segregados logicamente através de tecnologias como VLANs e firewalls.
- **Métrica:** Taxa de pontos com o mesmo domínio de broadcast que são separados logicamente.
- **Medidas:** i) Número de computadores, ii) Número de domínios ou sub-redes da rede municipal, iii) Número de VLANs (ou outra forma de segregação de rede), iv) Número de domínios (sub-redes) que acessam outros domínios não definidos pela política de segurança.
- **Origem dos dados:** Entrevistas com administradores de rede, testes de penetração com o objetivo de reconhecer e mapear a rede, ferramentas de *ping* múltiplos e similares para requisitar acessso a diferentes domínios de rede.

- **Freqüência:** Semestral.
- **Classificação da métrica:** Estrutura de rede.
- **Fórmula:** Seja a_t o número total de sub-redes, $a_1 =$ número de domínios que acessam outros domínios de sub-rede não definidos pela política de segurança interna. O componente a_1 é inseguro pois uma sub-rede só pode acessar os domínios que lhe são pertinentes.

$$\textbf{Modelo 1 = Modelo 2} \Rightarrow F_{12} = \left(1 - \overline{Y}\right) \text{ com } Y = \left\{\frac{a_1}{a_{t1}}\right\}$$

Capítulo 5

Aplicação das métricas na análise de segurança em Redes Metropolitanas de Acesso Aberto

A complexidade de uma rede metropolitana de acesso aberto exige que os requisitos para a coleta de dados sejam bem-definidos. Requisitos como escolha de ferramentas, definição das métricas que se adequam ao ambiente e reconhecimento da rede são fundamentais para que a coleta dos dados seja bem-sucedida. Após a coleta, as métricas são calculadas e os dados brutos são transformados em dados passíveis de serem analisados.

Este capítulo tem como objetivo apresentar a metodologia para a coleta e análise dos dados das métricas de segurança. A metodologia será descrita no formato de "etapas a cumprir". Essa construção gradual, a partir de passos pré-definidos, contribui para uma melhor visualização e organização dos dados e também para o desenvolvimento de ferramentas de automação. As sete etapas que compõem o *framework* serão explicadas com base em um exemplo fictício.

5.1 Metodologia para coleta e análise de dados

Considere o exemplo descrito na Tabela 5.1 em que 12 métricas foram coletadas. A Tabela 5.1 mostra o resultado de cada uma delas em que a coluna **Métrica** corresponde as mesmas métricas propostas na seção anterior:

Tab. 5.1: Métricas coletadas

Métrica	Fórmula
1) Segurança entre os prédios da MBAN	0,574
2) Requisitos de segurança da rede VoIP	0,351
3) Gerenciamento das contas de usuários	0,258
4) Contaminação por vírus	0,665
5) Tentativas de invasões	0,506
6) Configurações de segurança da rede sem fio	0,940
7) Disponibilidade e confiabilidade dos servidores	0,127
8) Utilização e dimensionamento do link de Internet	0,712
9) Aplicação de *patchs* no centro de interconexão	0,369
10) Complexidade de senhas	0,709
11) Tráfego de email	0,683
12) Segmentação da rede metropolitana de acesso aberto	0,250

As sete etapas que definem a metodologia proposta de análise e coleta de dados das métricas de segurança para MBANs são:

1. Preparar o ambiente para a coleta dos dados;
2. Automatizar as ferramentas de coleta de dados;
3. Coleta dos dados;
4. Cálculo das fórmulas de cada métrica;
5. Organizar as métricas em ordem decrescente de acordo com o resultado da fórmula;
6. Agrupar os resultados de cada métrica de acordo com sua classificação;
7. Análise dos dados coletados em cada métrica;

A seguir cada uma das etapas será explicada.

Preparar o ambiente para a coleta dos dados

A adequação do ambiente para a coleta dos dados começa com o reconhecimento da Rede Municipal. Diagramas com informações acerca da topologia da rede devem ser disponibilizados assim como outras informações técnicas como faixas de endereço IP, quantidade aproximada de máquinas, tecnologias empregadas na interconexão da rede, acessos remoto, distribuição de *switches* e roteadores e etc. Assim, o dimensionamento do esforço necessário na coleta e análise das métricas se torna possível.

O ambiente porém ainda não está totalmente preparado. Sistemas operacionais utilizados em desktops e servidores e especificações técnicas de hardware e software em desktops e servidores são informações que ajudam a completar a preparação do ambiente para a coleta dos dados.

Automatizar as ferramentas de coleta de dados

A definição das ferramentas que serão utilizadas na coleta dos dados deve respeitar um importante critério: seu nível de automação. A tarefa de medir segurança utilizando métricas é custosa. Portanto, é essencial que as ferramentas que auxiliam nesse processo sejam escolhidas levando-se em conta a automação. Por exemplo, considere a métrica 4 em que uma da medidas é o número de computadores que possuem anti-vírus instalado. Em uma Rede Municipal com 150 computadores é completamente inviável o administrador de rede se deslocar de máquina em máquina e verificar se existe anti-vírus instalado. Este tipo de medida deve ser realizada com a ajuda de uma ferramenta que remotamente faça auditoria nos computadores da rede mostrando os softwares instalados e salvando os resultados obtidos em relatórios.

A coleta automatizada dos dados ajuda na padronização dos métodos de coleta, aumenta a precisão e confiança das medições, aumenta a freqüência com que os dados são coletados e, dependendo do formato em que os relatórios são gerados, podem servir como dados de entrada para a criação de uma ferramenta integrada de coleta de dados, englobando diversas origens de dados [38] e [37].

Coleta dos dados

Após as duas primeiras etapas os dados já podem ser coletados. Existem basicamente quatro formas de realizar tal coleta: através de ferramentas de auditoria específicas, análise de logs, relatórios técnicos e entrevistas. O processo de coleta dos dados deve ser não-intrusivo de modo que os recursos alocados para a coleta não interfiram no andamento de todo o sistema [38].

Os dados coletados devem ser armazenados de forma a constituir um banco de dados com todas essas informações. Esse repositório é importante para a realizar comparações entre diferentes medições, também conhecido como "*before-and-after*" [37] e [64]. Ele aprimora o conhecimento da rede e de seus problemas e facilita a criação de relatórios informativos para os gestores da MBAN com o intuito de alertar sobre os problemas de segurança.

Os dados podem ser armazenados em bancos de dados como Oracle [65], SQL Server [66] e PostgreSQL [67] e também em *spreadsheets* ou planilhas de cálculo tais como Microsoft Excel e Minitab [68].

Cálculo das fórmulas de cada métrica

O resultado de cada métrica é expresso por uma fórmula. Esse resultado pode ser compreendido como uma espécie de indicador da métrica o qual varia entre 0 e 1, com 0 representando o valor mínimo e 1 o valor máximo. Ou seja, uma métrica com valores próximos de zero devem indicar que algo de errado está acontecendo e que os controles de segurança para tal métrica devem ser investigados e revisados imediatamente. Já valores próximos de 1 mostram que os objetivos da métrica estão sendo cumpridos com um bom nível de confiança. Por exemplo: Uma métrica que possui $0,2524$ como

valor deverá ser analisada com cuidado pois é um baixo valor, já uma métrica com valor de 0.885 pode ser considerado um bom resultado mas também pode melhorar.

Organizar as métricas em ordem decrescente de acordo com o resultado da fórmula

Uma abordagem simples para estabelecer as prioridades com relação a implementação dos controles de segurança é organizar as métricas em ordem decrescente de acordo com o resultado da fórmula. Assim, as métricas que obtiveram os piores resultados de acordo com a fórmula podem ser investigadas primeiramente facilitando a detecção de falhas primárias nos controles de segurança ou então erros no processo de coleta dos dados.

A Tabela 5.2 apresenta os resultados ordenados decrescentemente. Com os dados organizados, a visualização fica facilitada principalmente se o trabalho envolver muitas métricas para analisar. A Tabela 5.2 mostra a fragilidade dos serviços de disponibilidade e confiabilidade, que podem representar a baixa utilização de sistemas de *backups* e redundâncias críticos para o bom funcionamento da Rede Municipal. Nota-se também pelo valor da métrica o uso adequado dos controles de segurança para redes sem fio.

Tab. 5.2: Métricas ordenadas

Métrica	Fórmula
7) Disponibilidade e confiabilidade dos servidores	0,127
12) Segmentação da rede metropolitana de acesso aberto	0,250
3) Gerenciamento das contas de usuários	0,258
2) Requisitos de segurança da rede VoIP	0,351
9) Aplicação de patches no centro de interconexão	0,369
5) Tentativas de invasões	0,506
1) Segurança entre os prédios da MBAN	0,574
4) Contaminação por vírus	0.665
11) Tráfego de email	0,683
10) Complexidade de senhas	0,709
8) Utilização de Internet	0,712
6) Configurações de segurança da rede sem fio	0.940

Agrupar os resultados de cada métrica de acordo com sua classificação

Um dos atributos de uma métrica de segurança para Redes Municipais é a sua classificação. A classificação da métrica está relacionada aos componenentes da Rede Metropolitana de Acesso Aberto: estrutura de rede, pontos de interconexão e serviço. Propor uma reorganização dos resultados levando em consideração sua classificação, proporciona uma visão abragente sobre a localização dos problemas de segurança. A Tabela 5.3 que mostra a organização das métricas a partir das camadas de classificação da Infovia.

Tab. 5.3: Métricas - Camadas da MBAN

Serviço	Estrutura de rede	Tipo de ponto
0,351	0,574	0,258
0,127	0,506	0,665
0,712	0,250	0,506
0,683	0,940	0,250
	0,712	0,369
		0,709

Análise dos dados coletados

De posse das informações obtidas nos passos anteriores as análises dos resultados podem ser realizadas. O objetivo da análise dos dados é identificar a distância entre a atual e a desejada performance dos controles de segurança e descobrir as áreas da Rede Municipal que necessitam de melhorias. Dois aspectos serão abordados: a análise dos resultados das fórmulas, chamada de *análise global das métricas* e a análise dos componentes de cada métrica chamada de *análise individual das métricas*. O fluxo geral da análise dos dados coletados é representado pela Figura 5.1:

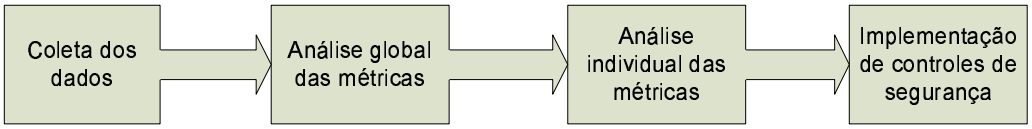

Fig. 5.1: Fluxo da análise das métricas

Jaquith [37] discute algumas técnicas comumente utilizadas para a análise de dados de segurança, dentre as quais: média aritmética, mediana, desvio padrão, agrupamento e agregação, análise de série temporal e análise transversal.

A média aritmética, mediana e desvio padrão são conhecidas medidas estatísticas; A média aritmética e a mediana são medidas de tendência central e o desvio padrão é uma medida de dispersão. Para a análise dos dados de segurança a média e a mediana são importantes pois mostram o valor representativo em torno do qual os dados tendem a agrupar-se, com maior ou menor freqüência. Já o desvio padrão mostra o grau de dispersão dos valores observados em relação à média.

O agrupamento consiste em colocar todos os registros juntos dentro de um escopo particular de análise, como, por exemplo, foi feito no item “Agrupar os resultados de cada métrica de acordo com sua classificação”. Nesse caso, os dados foram agrupados de acordo com as camadas da Rede Municipal e também com as áreas de concentração da métrica. A agregação implica em calcular estatísticas no conjunto de dados agrupado.

A análise de série temporal é feita dispondo registros através do tempo e analisando como é o comportamento dos mesmos no período observado. Já a análise transversal consiste em utilizar me-

didas estatísticas para acentuar semelhanças e diferenças entre os diversos grupos de dados. Exemplo: calcular a média aritmética, mediana e desvio padrão dos registros dispostos na Tabela 5.3.

Na subseções a seguir, serão discutidas com detalhes a análise global e a análise individual das métricas.

5.1.1 Análise global

A análise global das métricas tem como principal objetivo a criação de indicadores de segurança para facilitar a visualização das áreas problemáticas da Rede Municipal. Serão definidos dois indicadores: um geral para todas as métricas e um para as classificações da métrica.

Os indicadores serão compostos de dois números M e V e calculados a partir da fórmula de cada métrica. O indicador M será dado pela média aritmética entre cada um dos resultados das fórmulas do conjunto de métricas selecionado e V será obtido pelo cálculo do coeficiente de variação (quociente entre o desvio padrão e a média aritmética) dos resultados das fórmulas do conjunto de métricas. Como as fórmulas das métricas variam entre 0 e 1 então $0 \leq M \leq 1$. Da definição de coeficiente de variação, V é dado em forma de porcentagem [69].

Analogamente à fórmula das métricas, M representa o indicador de segurança do conjunto de métricas analisado. Quanto maior o valor de M, maior segurança representa o indicador. O coeficiente de variação V é utilizado para auxiliar a detecção de *outliers*[1] e também para comparar diferentes indicadores. Considere o exemplo apresentado na Tabela 5.4. As quantidades A_1, A_2 e A_3 representam o mesmo conjunto de métricas, porém medidos em tempos distintos.

Tab. 5.4: Exemplo - Coeficiente de Variação

Conjunto de métricas	Média	Coeficiente de variação
A_1	$0,602$	10%
A_2	$0,618$	38%
A_3	$0,598$	$0,7\%$

Note que as médias estão próximas do valor $0,6$ o que representaria aproximadamente o mesmo indicador de segurança para A_1, A_2 e A_3. Porém, o alto coeficiente de variação mostra que os dados do indicador A_2 são mais dispersos, ou seja, existem *outliers* que influenciaram o resultado do cálculo da média. O baixo coeficiente de variação de A_3 mostra que os valores se acumulam próximos a média. Em termos de segurança é desejável que uma análise cuidadosa seja realizada nos conjuntos de métrica em que o coeficiente de variação é alto e assim tentar descobrir de que forma os *outliers* estão influenciando a segurança do sistema.

Voltemos a Tabela 5.2 gerada pela ordenação decrescente das métricas. Este será o ponto inicial para a discussão dos resultados. Primeiramente, os dados da Tabela 5.2 serão agregados utilizando as seguintes medidas estatísticas: média aritmética, mediana e desvio padrão. Considere então a nova Tabela 5.5:

[1] Em estatística, um outlier é uma observação que é numericamente distante dos outros dados.

Tab. 5.5: Indicadores - Métricas ordenadas

Métrica	**Fórmula**
7) Disponibilidade e confiabilidade dos servidores	0,127
12) Segmentação da rede metropolitana de acesso aberto	0,250
3) Gerenciamento das contas de usuários	0,258
2) Requisitos de segurança da rede VoIP	0,351
9) Aplicação de patches no centro de interconexão	0,369
5) Tentativas de invasões	0,506
1) Segurança entre os prédios da Infovia	0,574
4) Contaminação por vírus	0,665
11) Tráfego de email	0,683
10) Complexidade de senhas	0,709
8) Utilização de Internet	0,712
6) Configurações de segurança da rede sem fio	0,940
$M =$ Média aritmética	0,5120
$V =$ Coeficiente de variação	47,34
Mediana	0,5400

Apesar do valor da média M estar próximo do valor da mediana $(0,5120 \approx 0,5400)$, o coeficiente de variação $V = 47,34$ indica que o conjunto de dados é disperso. Dessa forma, nosso conjunto de dados possui valores muito distantes da média, sejam eles mais altos ou mais baixos. Para a segurança da informação, este tipo de resultado mostra que os controles de segurança são eficientes para determinados objetivos e ineficientes para outros. Ou seja, controles bem sucedidos em somente um ponto do sistema podem não ser expressivos em termos da segurança global se a existência de brechas em outros pontos expuser o sistema. Por exemplo, considere uma arquitetura de rede composta pelos componentes descritos na Figura 5.2. O objetivo deste modelo é proteger a rede interna.

Basicamente os pontos de ataque são quatro: Firewall 1, Firewall 2, Servidor Web e Servidor de E-mail. Todos devem estar protegidos e vulnerabilidades em pontos prejudicam a segurança de todo o sistema.

A primeira vista, dedicar maior atenção ao Firewall 1 parece ser uma opção interessante. Porém, vulnerabilidades no Servidor Web ou no Servidor de E-mail podem encaminhar um atacante ao Firewall 2 e conseqüêntemente a rede interna. Analogamente, a aplicação de controles somente ao Firewall 2 pode custar a perda do Firewall 1 que gerencia o acesso a Internet, tornando os "desktops" da rede interna que acessam a Internet novamente vulneráveis a ataques.

Portanto, para o cálculo do indicador é esperado que os *outliers* possam interferir no resultado final. Dessa forma, a média aritmética é a medida de tendência central utilizada para a realização do cálculo do indicador global de segurança das métricas.

Os indicadores globais para cada uma das classificações da métrica serão obtidos calculando a média aritmética e o coeficiente de variação de cada coluna da Tabela 5.3.

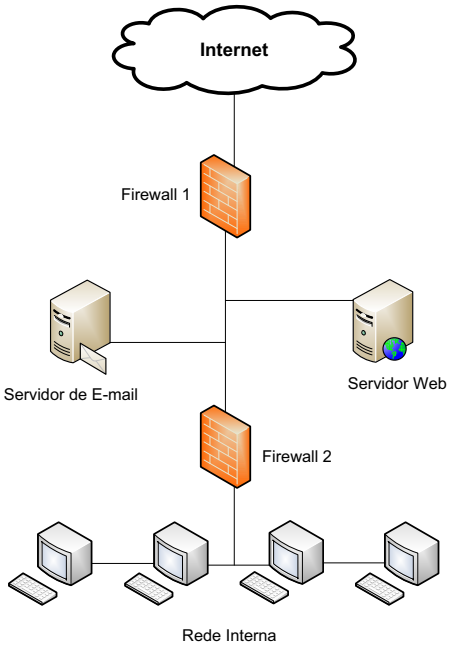

Fig. 5.2: Exemplo

Analisando a Tabela 5.6 nota-se que a camada de estrutura de rede é a que obteve o melhor indicador de segurança. As camadas de serviço e tipos de ponto possuem indicadores com valores próximos. Já a camada que possui o maior indíce de variação é a de serviço. Em termos de segurança esses resultados mostram que a estrutura de rede está mais "segura" que as outras camadas, porém seu respectivo indicador $I_1 = 0,5964$ pode ser melhorarado principalmente se controles de segurança forem aplicados para melhorar o resultado da métrica 12 cujo resultado da fórmula é $0,250$.

A análise global fornece a primeira impressão dos resultados das métricas. Ela facilita a visualização das áreas que obtiveram resultados ruins e satisfatórios, prioriza o tratamento das métricas e possibilita a análise temporal de um mesmo conjunto de dados.

Tab. 5.6: Indicadores - Camadas da MBAN

Serviço	**Estrutura de rede**	**Tipo de ponto**
0,351	0,574	0,258
0,127	0,506	0,665
0,712	0,250	0,506
0,683	0,940	0,369
	0,712	0,709
$M = 0,4682$	$M = 0,5964$	$M = 0,5014$
$V = 59,86$	$V = 42,76$	$V = 38,19$

5.1.2 Análise individual

A ordenação, agrupação e agregação dos resultados, como mostrado anteriormente nas Tabelas 5.5 e 5.6 possibilita a criação de um "*ranking*" de prioridades de segurança. Em nosso modelo a análise individual das métricas é feita obedecendo esse "*ranking*" começando pela métrica que obteve o resultado mais baixo. A justificativa é simples: se uma métrica obteve um resultado muito baixo, as chances de se encontrar problemas de segurança críticos aumenta.

Para auxiliar a análise individual das métricas, será definido um modelo formado pelas seguintes etapas:

1. Agrupar as medidas de acordo com algum atributo em comum. Por exemplo: agrupar os dados por prédio, VLan, servidor e etc. Aqui, mais de um agrupamento pode ser realizado, dependendo do tipo da métrica a ser analizada.

2. Agregar os dados já agrupados aplicando as seguintes medidas estatísticas: média aritmética, mediana, desvio padrão e coeficiente de variação.

3. Quando possível, analisar o comportamento dos dados de acordo com o tempo. A análise temporal é possível se dados de coletas anteriores estiverem disponíveis.

4. A partir dos resultados da análise, propor ou alterar políticas e controles de segurança.

A Figura 5.3 ilustra o modelo para análise individual das métricas de segurança para MBANs.

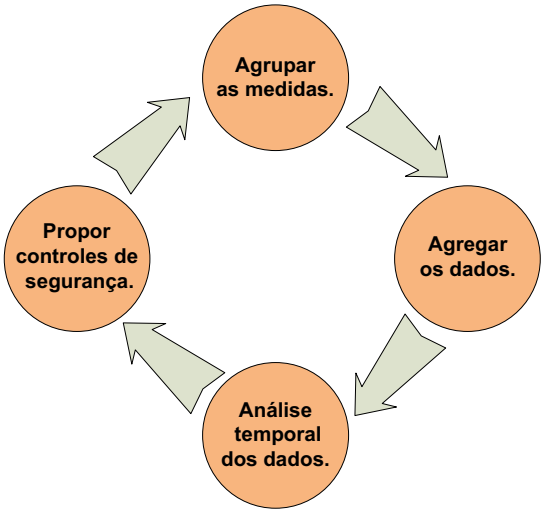

Fig. 5.3: Modelo para análise individual de métricas de segurança

Assim, com o uso de métodos quantitativos sobre os dados da Rede Municipal, a visualização de possíveis problemas em diferentes áreas da rede fica facilitada. O exemplo a seguir mostra a análise individual da métrica que trata da segurança das senhas dos equipamentos de rede da Infovia Municipal. Considere a Tabela 5.7 onde estão dispostos os dados da métrica já agrupados e agregados.

De acordo com o modelo proposto o primeiro passo é agrupar as medidas. Em nosso caso, as medidas foram agrupadas de acordo com o tipo de equipamento (servidores, roteadores e pontos

Tab. 5.7: Exemplo - Análise Individual

	Servidores	**Roteadores**	**Pontos de acesso**
Quantidade	11	4	13
Sem senha	3	3	5
Baixa complexidade	7	2	7
Média - Sem senha	0,2727	0,75	0,3846
Média - Baixa complexidade	0,6363	0,5	0,5384
Média geral	0,4545	0,625	0,4615

de acesso). O agrupamento facilita a análise do tratamento da segurança em cada equipamento. A seguir, os dados devem ser agrupados. Como o conjunto de dados é pequeno somente a média entre os grupos foi calculada.

Analisando a Tabela 5.7, pode-se notar que o problema da baixa complexidade de senhas é freqüênte em todos os equipamentos, em especial entre os servidores, com uma alta taxa de $0,6363$. Esses dados podem sugerir que a política de senhas não está sendo cumprida ou foi mal projetada.

Entre os equipamentos que não necessitam de senha para autenticação o resultado é um pouco melhor, com $0,2727$ para os servidores e $0,3846$ para os pontos de acesso. Porém o resultado dos roteadores mostra que somente 1 dos 4 roteadores faz uso de senha para autenticação. Fica claro neste exemplo que a administração dos roteadores não está sendo feita de maneira adequada e que os controles de segurança deveriam ser aplicados em caráter emergencial nesses equipamentos.

Nesse caso alguns dos controles de segurança possíveis são: revisão da política interna de senhas, troca de todas as senhas administrativas de servidores, roteadores e pontos de acesso além da conscientização e educação dos administradores da MBAN para o uso de senhas “fortes”.

A Figura 5.4 sintetiza todo o processo de análise dos dados coletados. O fluxo 1 representa a análise global das métricas. Já o fluxo 2 representa a análise individual das métricas. Após a obtenção dos dados e dos cálculos das fórmulas de cada métrica, os resultados da fórmula passam por um processo de ordenação e agrupamento e através de medidas estatísticas os indicadores de segurança são gerados. A partir desses indicadores, a pré-visualizaçãodas áreas problemáticas para a segurança da Rede Municipal é facilitada e o fluxo 1 é finalizado. O fluxo 2 inicia-se com a ordenação das métricas a partir de seu resultado e com a escolha da métrica com o valor mais baixo. O próximo passo é agrupar e agregar as medidas da métrica gerando um novo conjunto de dados o qual será analisado e a partir desta propor ou alterar os controles de segurança. O fluxo 2 continua até o término da análise das métricas ordenadas.

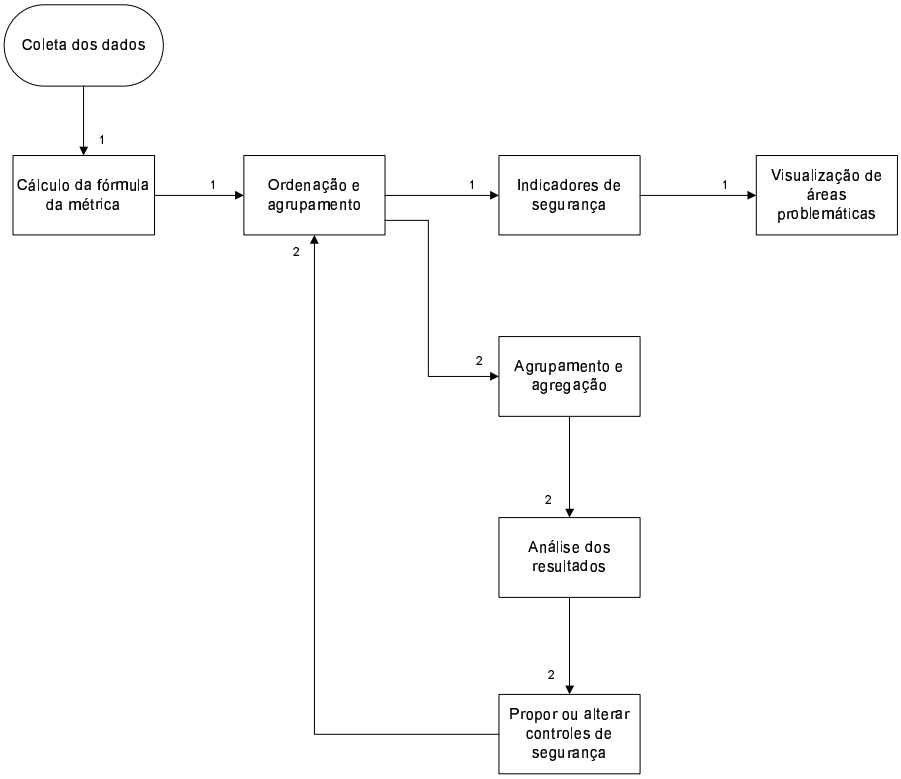

Fig. 5.4: Processo de análise dos dados coletados

Capítulo 6

Estudo de caso: Rede Metropolitana de Acesso aberto - Pedreira, SP

A presente seção tem como objetivo apresentar o estudo de caso envolvendo a aplicação de métricas de segurança na rede metropolitana de acesso aberto da cidade de Pedreira, localizada no interior do estado de São Paulo.

A Rede Metropolitana de Acesso Aberto de Pedreira é um projeto entre o LaRCom-Unicamp (Laboratório de Redes de Comunicação da Unicamp) e a prefeitura da cidade. Os estudos para a implantação da rede começaram em 2005 e sua inauguração se deu em junho de 2007. Atualmente, a infra-estrutura de rede da Infovia de Pedreira é híbrida, formada por um backbone óptico que interliga diversos pontos no centro da cidade e também por pontos de rádio espalhados pelo município. Alguns destes pontos de rádio são utilizados para oferecer Internet de graça a população. É esperado que até o mês de dezembro de 2008 aproximadamente 100% da população esteja apta a se conectar a tais pontos de rádio.

Além das residências, os principais prédios públicos da cidade de Pedreira estão conectados a MBAN. A Figura 6.1 mostra a disposição dos prédios públicos e a respectiva tecnologia de interconexão de rede.

Os serviços atualmente disponibilizados e que trafegam sobre a Infovia são: distribuição de Internet, Voz sobre IP (VoIP), E-mail e Câmeras IP para a segurança pública. Maiores detalhes sobre a rede de Pedreira serão apresentados na próxima seção que trata da aplicação das métricas de segurança.

6.1 Aplicação das métricas de segurança

A necessidade de detectar vulnerabilidades de segurança na rede de Pedreira e a iminente inserção da população no contexto da Infovia foram os fatores motivadores para o desenvolvimento de métricas específicas que pudessem quantificar a grande massa de dados gerada por relatórios, tabelas e softwares de gerenciamento. Além da quantificação de dados, as métricas possibilitam a criação de uma base de dados que é importante para analisar o retorno de investimento em segurança e também a segurança dos components através do tempo [64].

A aplicação das métricas aconteceu no período entre agosto de 2007 e julho de 2008. As métricas escolhidas para o estudo de caso foram as seguintes:

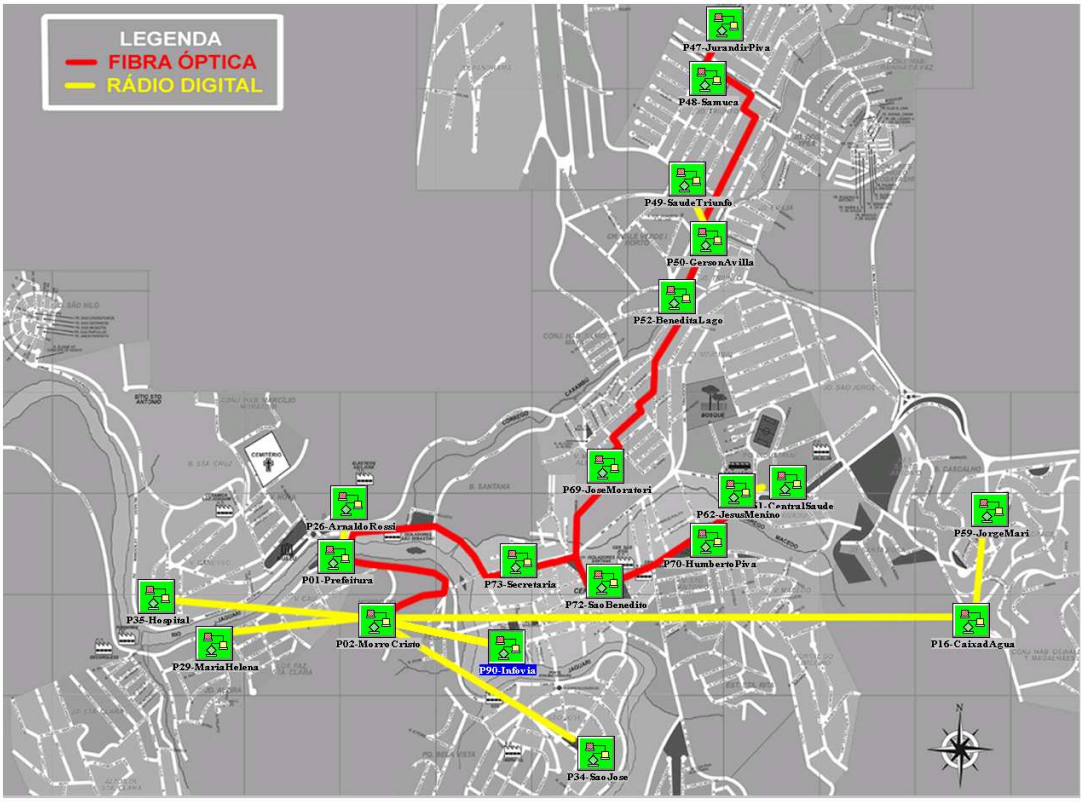

Fig. 6.1: Prédios públicos - Pedreira

- Métrica 1 - Segurança entre os prédios da MBAN;
- Métrica 2 - Requisitos de segurança da rede VoIP;
- Métrica 3 - Gerenciamento das contas de usuários;
- Métrica 6 - Configurações de segurança da rede sem fio;
- Métrica 7 - Disponibilidade e confiabilidade dos servidores;
- Métrica 8 - Utilização e dimensionamento do link de Internet;
- Métrica 9 - Aplicação de *patchs* no centro de interconexão;
- Métrica 10 - Complexidade de senhas;
- Métrica 12 - Segmentação da rede metropolitana de acesso aberto.

As métricas foram escolhidas em conjunto com a gerência da MBAN de Pedreira. Os fatores decisivos para a definição das métricas foram: possibilidade de impactos negativos no desempenho da rede, usabilidade de softwares já instalados e preferência por métricas com dados passíveis de serem coletados remotamente.

Métrica 1 - Segurança entre os prédios da MBAN

A métrica 1, definida no capítulo 4 trata da segurança das conexões entre os prédios da Rede Metropolitana de Acesso Aberto. Abaixo os dados coletados:

$a_{t1} = 17$ prédios.

$a_1 = 17$ prédios possuem recursos de firewall ou controles de acesso lógico entre as conexões. No caso da rede de Pedreira, todos os prédios possuem ACL's (*Access Controls Lists*) atreladas aos *switches* responsáveis pela interconexão dos prédios. As access lists estão configuradas para impedir o acesso de uma rede para a outra, a não ser que o acesso esteja dentro da política de acesso definida.

$a_2 = 7$ prédios possuem criptografia entre as conexões. Os 7 prédios interligados pela rede sem fio são os únicos que possuem recursos de criptografia entre as conexões. O protocolo criptográfico utilizado é o WEP. Neste caso, a tabela de pesos para tamanho de chave não se aplica. O peso será o mesmo definido na métrica 6, ou seja, $0,2$. Portanto, $7(0,2) = 1,4$.

$i_{1,2} = 7$ prédios que possuem recursos de firewall e criptografia entre as conexões. Esses prédios são justamente os 7 prédios interconectados pela rede sem fio.

Cálculo do indicador:

$$\text{Modelo 1} \Rightarrow F_1 = \frac{\frac{17}{17} + \frac{7(0,2)}{17}}{2} = 0,5411$$

$$\text{Modelo 2} \Rightarrow F_1 = \frac{2(0,0823)+1+0,0823}{4} = 0,3117$$

O resultado dos indicadores $0,5411$ e $0,3117$ mostram que existem problemas no tratamento da segurança entre as conexões dos prédios da Rede Metropolitana de Acesso Aberto de Pedreira. A seguir será feita a análise dos resultados obtidos pela métrica.

Vamos utilizar o modelo proposto na seção 5.1.2 para a análise dos dados. O primeiro passo é agrupar as medidas. As medidas foram agrupadas na Tabela 6.1 de acordo com a tecnologia de interconexão, fibra óptica ou rede sem fio, e com a classificação funcional do prédio - saúde, educação ou prefeitura.

Tab. 6.1: Dados agrupados - Métrica 1

	Saúde	Educação	Prefeitura
Número de prédios	3	12	2
Prédios com ACLs	3	12	2
Prédios com Criptografia	3	4	0
Fibra Óptica	0	8	2
Sem fio	3	4	0
Taxa de prédios com criptografia	100%	$0,3333\%$	0%

A Figura 6.2 ilustra a distribuição dos prédios descrita na Tabela 6.1.

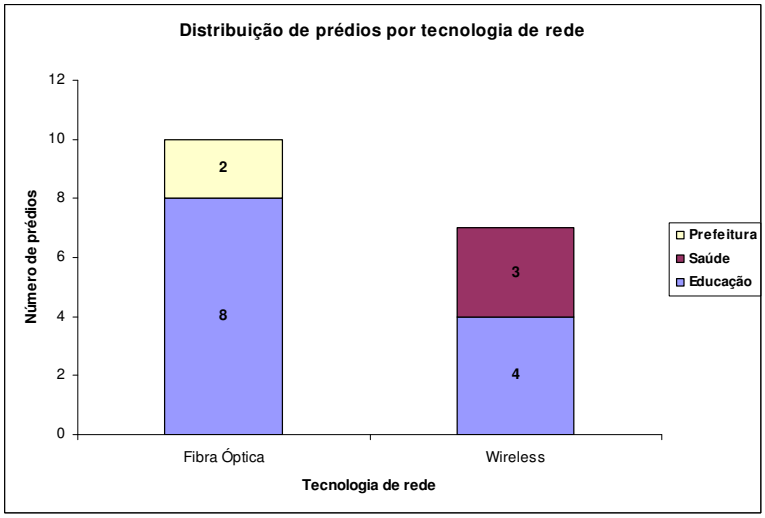

Fig. 6.2: Distribuição de prédios por tecnologia de rede

A análise da Tabela 6.1 nos fornece um dado interessante. Apesar de os prédios da Prefeitura estarem todos conectados através de fibra óptica - uma tecnologia conhecida pela dificuldade de grampo e com alta confiabilidade [70], [71] - as conexões não são cifradas. Estes prédios são considerados críticos, já que toda a infraestrutura computacional da Infovia está alocada fisicamente na prefeitura. Apesar da Access List bloquear o acesso de sub-redes diferentes à Prefeitura, um possível cenário de ataque seria a utilização de sniffers [16] de rede dentro da própria prefeitura. Como os dados estão sendo transmitidos em claro, existem softwares que são capazes de capturar e até manipular tais dados. Uma outra vulnerabilidade crítica encontrada é com relação aos prédios da saúde. O protocolo criptográfico utilizado é o inseguro WEP. Fazendo uso de técnicas bem documentadas [58], [72], [73], o WEP pode ser facilmente quebrado e informações confidenciais de prontuários médicos, por exemplo, são passíveis de serem capturadas.

A troca do protocolo criptográfico WEP pelo WPA, por exemplo, seria o início da solução destes problemas. Além disso, para proteger seus dados a prefeitura poderia implementar soluções de criptografia utilizando túneis VPN. Existem tecnologias de implementação livre como o OpenVPN [74] desenvolvido por James Yonan e publicado sob licença livre GNU/GPL. Neste caso, os pontos críticos devem ser previamente definidos e a partir deles iniciar o desenvolvimento do túnel seguro.

Outro controle sugerido foi o desenvolvimento de um conjunto de testes para as *Access Lists*. Em redes da proporção de uma MBAN, sub-redes são freqüêntente criadas, desktops inseridos no domínio além do acesso de notebooks. Usar uma ferramenta automatizada com determinada periodicidade a fim de certificar que as *Access Lists* estão funcionando corretamente ajudaria a aumentar a eficiência do controle de acesso da Infovia Municipal.

Métrica 2 - Requisitos de segurança da rede VoIP

A métrica 2 trata dos requisitos de segurança da rede VoIP da rede metropolitana de acesso aberto. Em Pedreira, o serviço de VoIP está disponível somente para os prédios públicos, a população não

possui tal acesso. Juntamente com a distribuição de Internet, foi o primeiro serviço a ser disponibilizado para a Infovia Municipal. Os dados da métrica são os seguintes:

$a_{t1} = 60$ ramais VoIP.

$a_{t2} = 2$ trimestres. O primeiro trimestre corresponde aos meses de agosto, setembro e outrubro de 2007. Neste período o número de ligações foi de 1050. Já o segundo trimestre corresponde aos meses de novembro e dezembro de 2007 e janeiro de 2008. O número de ligações neste período foi de 5497.

$a_1 = 0$. Nenhum ramal VoIP é cifrado.

$a_2 = 60$. Todos os ramais VoIP da rede de Pedreira estão segregados da rede de dados. Foram criadas VLANs específicas com essa finalidade.

$a_3 =$ No primeiro trimestre, o número de ligações não concluídas foi de 110. Já no segundo trimestre o número de ligações não concluídas foi de 224.

$i_{1,2} = 0$, pois nenhum ramal VoIP é cifrado.

Durante as medições entre os trimestres, o único componente que se alterou foi o número de ligações. Os componentes a_1 e a_2 se mantiveram constantes. O cálculo do indicador de segurança foi dividido por trimestre.

Primeiro trimestre:
Modelo 1 $\Rightarrow F_2 = \frac{F_{seg}+F_{ins}}{2} = \frac{0{,}5+0{,}8953}{2} = 0,6976$

Com $F_{seg} = \frac{0+1}{2} = 0,5$ e $F_{ins} = 1 - \left(\frac{110}{1050}\right) = 0,8953$

Modelo 2 $\Rightarrow F_2 = \left(\frac{\left(\frac{2(\frac{0}{60})+\frac{0}{60}+1}{4}\right)+\left(1-\left(\frac{110}{1050}\right)\right)}{2} \right) = 0,5726$

Segundo trimestre:
Modelo 1 $\Rightarrow F_2 = \frac{F_{seg}+F_{ins}}{2} = \frac{0{,}5+0{,}9593}{2} = 0,7296$

Com $F_{seg} = \frac{0+1}{2} = 0,5$ e $F_{ins} = 1 - \left(\frac{224}{5497}\right) = 0,9593$

Modelo 2 $\Rightarrow F_2 = \left(\frac{\left(\frac{2(\frac{0}{60})+\frac{0}{60}+1}{4}\right)+\left(1-\left(\frac{224}{5497}\right)\right)}{2} \right) = 0,6046$

Apesar de todos os ramais VoIP estarem separados da rede de dados, nenhum ramal é protegido com criptografia. Pesquisas estão sendo atualmente desenvolvidas para utilizar criptografia nos ramais VoIP da MBAN de Pedreira. A tecnologia implementada envolve o uso do PABX livre Asterisk [75]. Existem diversos problemas no uso conjunto do Asterisk com diversos protocolos de criptografia, como o IPSec [14] e também com o protocolo NAT [17]. Os indicadores de segurança dos dois trimestres, mostram que a métrica obteve bons resultados, e assim que os trabalhos envolvendo a cifragem dos ramais forem concluídos, os indicadores provavelmente irão melhorar.

Como a métrica foi coletada duas vezes em tempos diferentes, podemos aplicar a análise temporal nos dados. Considere a Tabela 6.2:

Comparando o primeiro e o segundo trimestre o número de ligações teve um aumento de aproximadamente 500% no segundo trimestre. Esse fato ocorreu pois os dois primeiros meses do primeiro

Tab. 6.2: Análise temporal - Métrica 2

	1° trimestre	2° trimestre
Número de ligações	1050	5497
Número de ligações não completadas	110	224
Taxa de ligações não completadas	10,47%	4,07%

trimestre ficaram marcados por testes na rede VoIP. Com a situação normalizada o número de ligações aumentou.

A taxa de ligações não completadas é um importante indicador de disponibilidade do sistema. Um alto índice pode ser sinal de que o sistema está sobrecarregado ou ainda representar um mal funcionamento. No primeiro trimestre esta taxa foi de 10,47%, um valor consideravelmente alto mas que pode ser explicado pela fase de testes que o sistema VoIP estava passando em tal período. Já no segundo trimestre, com o sistema estabilizado, a taxa caiu para 4,07%, o que representa uma queda de aproximadamente 157%.

Métrica 3 - Gerenciamento das contas de usuários

Todos as estações de trabalho dos prédios públicos da MBAN de Pedreira utilizam sistemas operacionais Windows, versões 98 e XP. Esse fato reforça a importância da métrica que estuda os problemas de segurança pertinentes a gerência das contas dos usuários dos prédios públicos em uma rede municipal, pois, problemas de segurança em contas de usuários representam uma grande parcela das vulnerabilidades do Windows [76].

Como os prédios públicos da rede de Pedreira não possuem controladores de domínio, a auditoria das máquinas foi realizada com o auxílio de um software chamado *Network Management Suite* [77]. Devido a complexidade da coleta dos dados, foram auditadas 94 máquinas de um total de 214. Foram escolhidos prédios chave, dentre eles o Paço Municipal. Abaixo os dados coletados:

$a_{t1} = 131$ contas de usuário. Os usuários "HelpAssistant" e "SUPPORT_388945a0" não entraram no cálculo. O Windows cria automaticamente tais contas para auxiliar em processos de administração remota e as permissões são extremamente restritas além de não incluir o logon no computador [78]. A conta de "Convidado" ou "Guest" também não consta nos cálculos.

$a_{t2} = 66$ computadores. Somente os computadores com Windows XP fazem parte do cálculo. Computadores com Windows 98 não pertencentes a um domínio não necessitam de contas de usuários para efetuar o logon.

$a_1 = 120$ usuários com permissão de administrador. Deve-se notar que o cálculo considera o usuário "Administrador", criado pelo Windows.

$a_2 = 23$ computadores fazem logon no sistema utilizando somente a conta de "Administrador".

Modelo 1 = Modelo 2 $\Rightarrow F_3 = 1 - \left(\frac{\frac{120}{131}+\frac{23}{66}}{2}\right) = 1 - \frac{0{,}9160+0{,}3484}{2} = 0,3678$

A auditoria foi feita em 3 VLan's da rede municipal de Pedreira. Cada uma das VLan's corresponde ao seguinte conjunto de prédios: escolas, secretária da educação e prefeitura. A Tabela 6.3 agrupa os dados de acordo com os prédios.

Tab. 6.3: Dados agrupados - Métrica 3

	Escolas	Secretaria	Prefeitura
Número de contas de usuários	30	12	89
Número de computadores	30	9	37
Contas com privilégio de administrador	26	11	83
Computadores com a conta de Administrador como conta de trabalho	16	6	1
Taxa de contas com privilégio de administrador	76,92%	91,67%	93,25%
Taxa de computadores com Administrador como conta de trabalho	80%	66,67%	0,027%

Com o agrupamento dos dados é possível visualizar as áreas problemáticas do escopo da métrica. O baixo indicador $0,3678$ foi o primeiro sinal de que existem problemas no gerenciamento de usuários na MBAN de Pedreira. Seja nas Escolas, Prefeitura ou Secretaria, as taxas de usuários com privilégios de administrador são muito altas e fica claro a necessidade de um controlador de domínio para gerenciar com eficiência as permissões dos usuários.

Com relação aos computadores que utilizam somente a conta nativa de Administrador do Windows para efetuar logon, o resultado foi de certa maneira surpreendente. Apenas 0,027% dos computadores da prefeitura são utilizados desta forma, ou seja, existe uma pré-política que incentiva os usuários a criarem contas diferentes para trabalharem. Porém, tais contas não necessitam ter sempre altos privilégios. Já as Escolas obtiveram a alta e preocupante taxa de 80%, indicando que sequer foram executados procedimentos iniciais de segurança nos computadores.

A Figura 6.3 ilustra os resultados obtidos pela métrica 3.

Métrica 6 - Configurações de segurança da rede sem fio

A MBAN de Pedreira possui atualmente 5 pontos de acesso distribuídos pela cidade. Como teoricamente qualquer usuário dispondo de um notebook é um atacante em potencial a tais dispositivos, os cuidados com a segurança devem ser redobrados. A métrica 6 coleta informações sobre as configurações da rede, hardware e software dos pontos de acesso, possibilitando a realização de uma análise de segurança com maior eficiência.

Os softwares *NetStumbler* e *AirSnort* auxiliaram no coleta dos dados. As informações coletadas sobre os APs de Pedreira foram as seguintes:

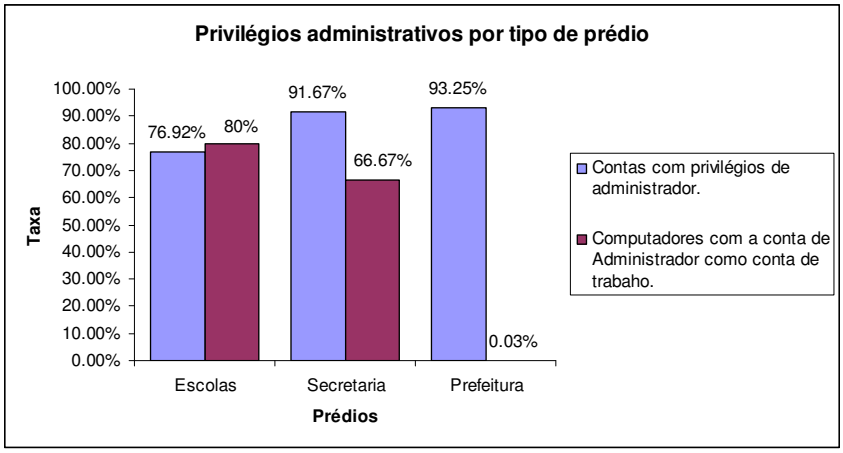

Fig. 6.3: Privilégios administrativos por prédio público

$a_t = 5$ pontos de acesso.

$a_1 = 5$*(0,2) = 1. Em todos os pontos de acesso o protocolo WEP está habilitado.

$a_2 = a_3 = a_4 = a_5 = 0$. Ou seja, nenhum Acess Point possui SSID de fábrica, senha padrão, versões desatualizadas de firmware e software e autenticação aberta.

Modelo 1 = Modelo 2 $\Rightarrow F_6 = \left(\frac{(1-(0))+\left(\frac{1}{5}\right)}{2} \right) = 0,6$

Os resultados da métrica mostraram a existência de políticas de segurança na configuração dos pontos de acesso da MBAN de Pedreira, pois, os *APs* não possuiam SSID de fábrica, senha padrão, versões desatualizadas de firmware e software e autenticação aberta. Além destes requisitos, o protocolo de segurança também estava habilitado, no caso, o WEP. Dos componentes analisados, a única vulnerabilidade detectada foi o uso do protocolo WEP.

Métrica 7 - Disponibilidade e confiabilidade dos servidores

O objetivo da métrica 7 é analisar a disponibilidade e confiabilidade dos servidores da rede metropolitana de acesso aberto. Programas de backup, redundâncias e *uptime* (tempo no qual um serviço está operacional) são os componentes desta métrica. Até o período analisado, a Infovia de Pedreira contava com três servidores: um para o Firewall, um para o VoIP e outro para o E-mail. Atualmente, mais dois servidores estão em fase de implementação: *Traffic Shapper* e *Radius*. Ambos os servidores fazem parte do projeto de inserção da população na MBAN de Pedreira. O *Traffic Shapper*, ou balanceador de tráfego, tem como principal funcionalidade controlar a banda de Internet disponível para a população. Já o *Radius* [79] é o servidor responsável pela autenticação dos usuários. Os dados foram coletados entre abril e julho de 2008.

$a_{t1} = 3$ servidores.

$a_{t2} = 128$ dias ou 3072 horas.

$a_1 = 1$. Somente o servidor de E-mail possui redundância. A técnica de redundância utilizada é o espelhamento de discos rígidos via RAID.

$a_2 = 3$.

$a_3 = 2$. Os servidores VoIP e Firewall possuem backups fisicamente distantes.
$i_{1,2} = 1$. No caso, o servidor de E-mail.
$a_4 =$ 3067,84. Abaixo, os servidores e respectivos valores de uptime, em horas:
Firewall = $3064,5$
VoIP = $3068,52$
E-mail = $3070,5$

Portanto, o cálculo da fórmula será o seguinte:

$$\text{Modelo 1} \Rightarrow F_7 = \frac{\frac{1}{3}+\frac{3}{3}+\frac{2}{3}+\frac{3067,84}{3072}}{4} = 0,7496$$

$$\text{Modelo 2} \Rightarrow F_7 = \frac{\left(\frac{2\frac{1}{3}+\frac{1}{3}+\frac{3}{3}}{4}\right)+\frac{2}{3}+\frac{3067,84}{3072}}{3} = 0,7217$$

O resultado obtido foi muito bom, afinal 100% dos computadores estão no programa de backup e 66,67% possuem backups em locais fisicamente distantes. É importante que os outros servidores, além do E-mail, implementem funções de redundância. Vimos na métrica 2, o aumento do uso do VoIP, ou seja, uma queda neste servidor significa indisponibilidade de serviço para todos os usuários do VoIP representando um sério problema de segurança. O mesmo ocorre para o Firewall que é a primeira linha de defesa da rede. Uma solução interessante para a redundância de servidores Linux é o *HeartBeat* [80]. O *HeartBeat* é um dos componentes principais do projeto Linux-HA (High-Availability Linux). Suas principais funcionalidades são a detecção de queda de um nó da rede e gerenciamento da comunicação entre clusters. O *HeartBeat* também pode ser configurado entre dois servidores, se um deles "cair" o outro automaticamente assume o seu lugar.

Com relação ao uptime dos servidores, os resultados foram muito bons. A média de tempo no ar dos três servidores foi de $\frac{3067,84}{3072} = 99,86\%$. Ou seja, os três servidores obtiveram excelentes resultados. O período medido foi de 128 dias = 3072 horas ou ainda 184320 minutos. A Figura 6.4 mostra o tempo que cada servidor ficou "fora do ar" (downtime) durante o período total medido:

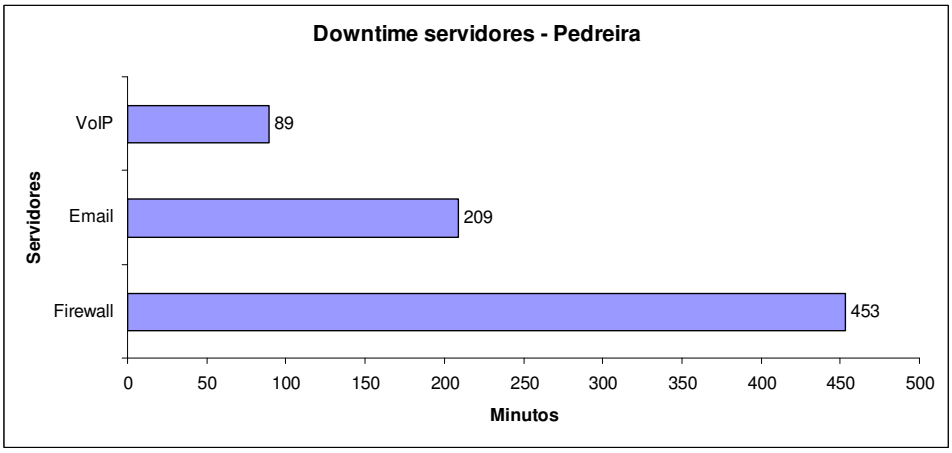

Fig. 6.4: Downtime dos servidores

A Figura 6.5 mostra a distribuição das quedas durante o período medido. Em nenhum momento,

os servidores VoIP e de E-mail caíram mais de uma vez no dia. Isso evidencia a eficiência no tratamento dos problemas em tais servidores. Já o Firewall chegou a cair 5 vezes em um só dia. A principal causa deste fenômeno foi a inserção da população no contexto da Infovia. O hardware do Firewall não era robusto o suficiente para atender toda a demanda de conexões. Em agosto de 2008, o Firewall foi trocado por outro mais robusto e com alta capacidade de tratamento de conexões diminuindo a incidência de quedas.

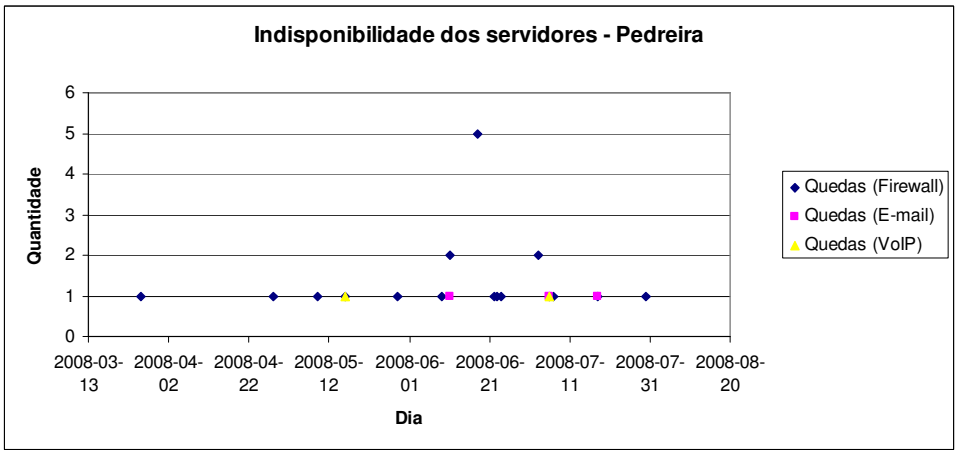

Fig. 6.5: Número de "quedas" dos servidores

Métrica 8 - Utilização e dimensionamento do link de Internet

A análise da utilização do link de Internet em uma MBAN possui grande importância para a segurança da informação pois permite a detecção de uso abusivo e de congestionamentos da rede contribuindo para o aumento da disponibilidade do serviço. A métrica 8 é responsável por tal tarefa. As medições foram realizadas no período entre abril e julho de 2008. A monitoração do link foi realizada com a ajuda do software MRTG - *Multi Router Traffic Grapher* [81].

$a_{t1} = 8$ mbits/s.

$a_{t2} = 214$ computadores acessam Internet através do link disponibilizado pela Infovia Municipal de Pedreira. Neste número ainda não estão inclusos os computadores das residências.

$a_1 =$ a banda média de download medida durante o período foi de $6,1731$ mbits/s e a de upload foi de $2,1222$ mbits/s.

$a_2 = 6$

Modelo 1 = Modelo 2 $\Rightarrow F_8 = 1 - \left(\frac{\frac{6,1731}{8} + \frac{2,1222}{8} + \frac{6}{214}}{3} \right) = 0,8756$

O software MRTG gera dois tipos de dados em suas medições diárias: o valor máximo e o valor médio. O cálculo do componente a_1 foi feito com base nos valores médios diários calculados pelo MRTG. Porém, a análise dos picos se torna interessante especialmente por tratarmos dos dados relativos a um link de Internet. Ter sempre picos perto do valor total pode significar congestionamento em determinados períodos do dia.

A Tabela 6.4 apresenta os valores médios e máximos de download e upload do link de Internet da MBAN de Pedreira.

Tab. 6.4: Dados agrupados - Métrica 8

	Download(Max)	Download(Médio)	Upload(Max)	Upload(Médio)
Média	6,1731 mbits/s	2,1222 mbits/s	2,4902 mbits/s	0,645 mbits/s
Taxa	77,164%	26,5285%	31,1278%	8,0633%
Coeficiente de variação	0,2510	0,4986	0,5113	0,5315

Apesar da média diária do uso da banda de download representar 26,5285% do link, os picos diários representam 77,164% da banda de download. Esses picos são atingidos principalmente nos períodos entre às 8:00 - 10:00 da manhã e entre 14:00 - 17:00 da tarde. Analisar os valores máximos também é útil na detecção de anomalias. Valores máximos em horários não convencionais, como a madrugada, podem indicar uso abusivo do link ou ainda execução de processos em máquinas "zumbi" [1] [82].

A análise do coeficiente de variação indica que o conjunto de dados mais homogêneo é o de Download(Max), mais uma evidência da existência de períodos constantes de alto uso do link. Para os outros conjuntos de dados o coeficiente de variação foi alto, revelando a falta de um padrão de uso do link, principalmente de Upload.

As Figuras 6.6 e 6.7 exibem o uso do link de download e upload respectivamente.

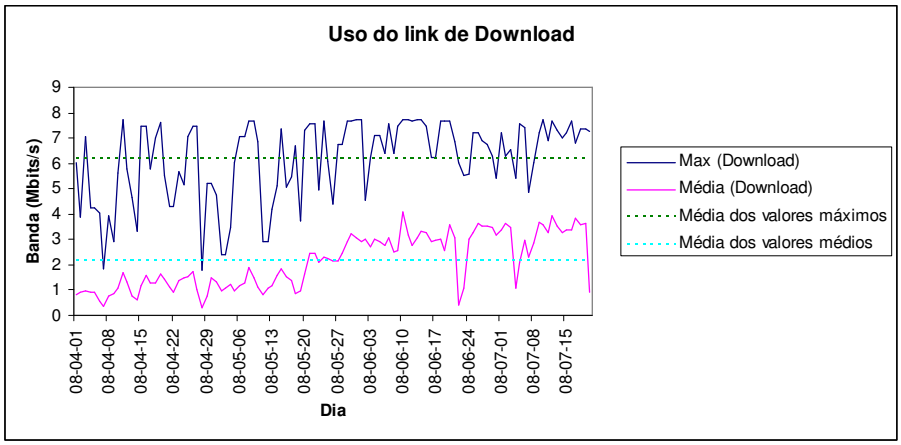

Fig. 6.6: Uso do link de Download

Métrica 9 - Aplicação de *patchs* no centro de interconexão

[1] É o nome que se dá aos computadores com acesso à Internet invadidos e controlados a distância por criminosos e atacantes em geral

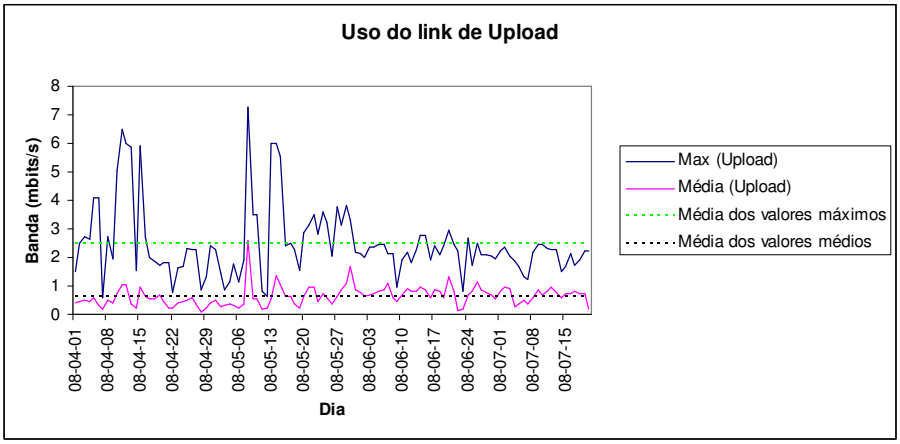

Fig. 6.7: Uso do link de Upload

Os três servidores: VoIP, Email e Firewall, foram submetidos a testes com a ferramenta *Tenable Nessus Network Security*. O software gera um relatório com as vulnerabilidades de segurança encontradas, suas descrições, os sistemas afetados, severidade e os respectivos links para a NVD - *National Vulnerability Database* mantida pelo NIST.

Na página do NIST, são expostos os índices CVSS das vulnerabilidades e os respectivos patches de segurança que devem ser executados.

Os dados de entrada para o cálculo do indicador de segurança da métrica são, $a_{t1} = 3$ servidores e $a_1 = 1.8399$ que corresponde a soma das médias dos índices de CVSS dos três servidores. Então,

Modelo 1 = Modelo 2 $\Rightarrow F_9 = 1 - \left(\frac{a_1}{a_{t1}}\right) = \frac{1.8399}{3} = 0,389$

Os dados coletados foram dispostos na Tabela 6.5:

Tab. 6.5: Vulnerabilidades de segurança por servidor

	Firewall	VoIP	Email
Número de vulnerabilidades	136	13	75
Média do CVSS	0,5877	0,6841	0,5681
Desvio padrão CVSS	0,2091	0,2233	0,2057
Mediana CVSS	0,5	0,69	0,5
Coeficiente de variação CVSS	0,3559	0,3262	0,3669

Apesar do alto número de vulnerabilidades encontrada no Firewall, em média as vulnerabilidades do servidor VoIP são de criticidade mais alta. Analisando somente a severidade das vulnerabilidades detectadas, o servidor que obteve os melhores resultados foi o de E-mail, com uma média de 0,5681 aliado também ao desvio padrão - o mais baixo entre os três servidores - o que caracteriza um conjunto

de dados pouco disperso da média. A Figura 6.8 mostra o nível de criticidade, definido pelo CVSS, das vulnerabilidades detectadas em cada servidor.

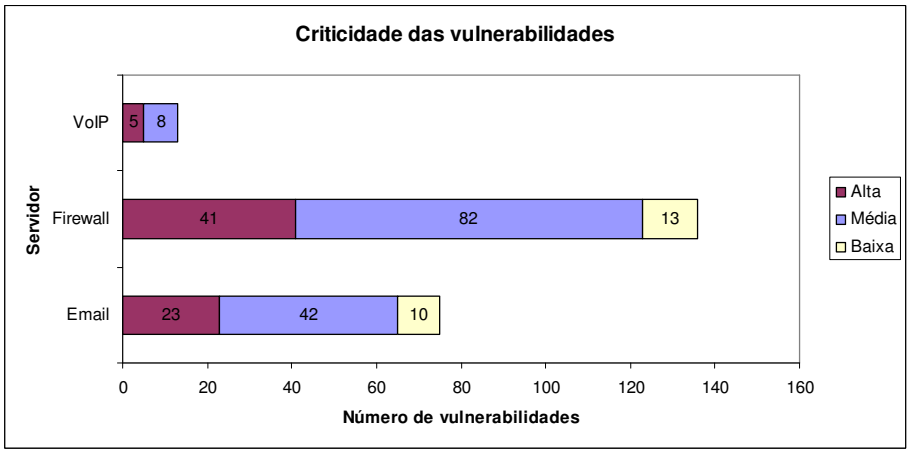

Fig. 6.8: Nível de criticidade das vulnerabilidades

Não devemos porém deixar de lado o fato de que sozinha, as vulnerabilidades do Firewall representam mais 60% do total de vulnerabilidades encontradas nos três servidores. Por ser o servidor com a maior carga de dados para analisar e que também serve como primeira linha de defesa da rede, os resultados deveriam ser melhores. A Figura 6.9 exibe a contribuição dos servidores para o total de vulnerabilidades encontradas.

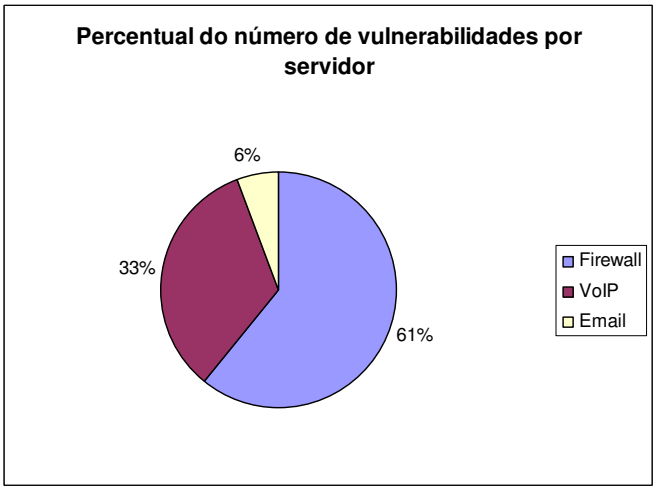

Fig. 6.9: Taxa de vulnerabilidades por servidor

Métrica 10 - Complexidade de senhas

A métrica 10 é responsável pela análise da complexidade das senhas de equipamentos e computadores da rede metropolitana de acesso aberto. Foram auditados servidores, *switches*, roteadores e rádios. Abaixo, os dados obtidos:

$a_{t1} = 5$ servidores. Nesta métrica os servidores de *Traffic Shaper* e *Radius* fazem parte do cálculo.
$a_{t2} = 2$ roteadores e 19 *switches*.
$a_{t3} = 13$ rádios.
$a_1 = 0{,}71$.
$a_2 = 0{,}8$.
$a_3 = 0{,}79$.

Modelo 1 = Modelo 2 $\Rightarrow F_{10} = \frac{0{,}71+0{,}8+0{,}79}{3} = 0,76666$.

Os resultados da análise do *Password Strength Meter* são retornados de duas formas: quantitativa e qualitativa. Utilizaremos o resultado quantitativo para o cálculo do indicador de segurança da métrica. O retorno em formato qualitativo, ajuda a compreender os números obtidos. O *Password Strength Meter* utiliza a seguinte regra para gerar as saídas do programa: seja s o resultado da análise, então se:

$s < 0,2 \Rightarrow$ senha é muito fraca.
$0,2 \leq s < 0,4 \Rightarrow$ senha é fraca.
$0,4 \leq s < 0,6 \Rightarrow$ senha é média.
$0,6 \leq s < 0,8 \Rightarrow$ senha é forte.
$0,8 \leq s \leq 1$ senha é muito forte.

O resultado da métrica indica que as senhas dos servidores, *switches*, roteadores e rádios foram classificadas como fortes. Esse resultado é muito animador pois indica que os administradores e gerentes da Infovia de Pedreira se preocuparam em construir senhas fortes para seus sistemas. A única senha que ficou distante do resultado da fórmula foi uma com índice 0,38 foi encontrada nos servidores de VoIP, E-mail e Firewall. Note que uma senha com tal pontuação é considerada fraca. O primeiro controle de segurança para a métrica é o aumento da complexidade desta senha. Um segundo controle é a padronização da política de senhas em todos equipamentos da Infovia.

Métrica 12 - Segmentação da rede metropolitana de acesso aberto

A rede metropolitana de acesso aberto de Pedreira é dividida em 14 sub-redes ou domínios. O desenvolvimento de sub-redes foi necessário a fim de segregar o tráfego entre os diferentes tipos de prédios da Infovia. As sub-redes foram implementadas com o auxílio de VLANs criadas nos *switches* e roteadores da rede. Cada VLAN possui características próprias que vão desde a definição do número IP, da máscara de rede, do gateway e de protocolos de rede a serem utilizados até a configuração dos controles de acesso. Os *switches* e roteadores possuem regras para o controle de acesso no formato de Access Lists impedindo ou permitindo o tráfego de pacotes.

Para cada domínio de interesse da rede foi criada uma VLAN. Existem VLANs para escolas, hospitais, VoIP, prefeitura, postos de saúde e para o acesso da população. As Access Lists podem ser aplicadas em números IPs específicos ou nos domínios de interesse.

A estratégia escolhida para a coleta dos dados foi a execução de uma espécie de teste de penetração. Munido de um *notebook* e a lista com as faixas de IP das VLANs, o administrador da rede

inseria o *notebook* em cada uma das VLANs. A partir de uma VLAN x, eram disparadas requisições de acessos as outras VLANs. O teste foi repetido para todas as VLANs. Abaixo, os dados coletados:

$a_t = 14$.

$a_1 = 1$. Somente à partir de uma VLAN foi possível o acesso a VLANs fora da política de acesso.

Modelo 1 = Modelo 2 $\Rightarrow F_{12} = \left(1 - \left(\frac{1}{14}\right)\right) = 0,9285$

A única VLAN que possuia acessos não permitidos era a da população. Detectado este fato, foram sugeridos controles de acesso específicos à partir da VLAN da população. Tal VLAN deve ter acesso somente a Internet distribuída e a eventuais aplicações que futuramente serão disponibilizadas. Todo acesso oriundo da VLAN da população com destino as outras VLANs da MBAN de Pedreira deve ser bloqueado.

6.2 Análise dos resultados

Esta seção tem como objetivo realizar a análise dos dados obtidos com a aplicação das métricas e mostrar os benefícios de sua utilização nas redes metropolitanas de acesso aberto, em especial na rede de Pedreira.

A Tabela 6.6 apresenta o resultado do cálculo dos indicadores de segurança para os modelos 1 e 2.

Tab. 6.6: Resultados das métricas - Modelos 1 e 2

Métrica	Modelo 1	Modelo 2
1 - Segurança entre os prédios da MBAN	0,5411	0,3117
2 - Requisitos de segurança da rede VoIP	0,7296	0,6046
3 - Gerenciamento das contas de usuários	0,3678	0,3678
6 - Configurações de segurança da rede sem fio	0,6	0,6
7 - Disponibilidade e confiabilidade dos servidores	0,7496	0,7217
8 - Utilização e dimensionamento do link de Internet	0,8756	0,8756
9 - Aplicação de *patchs* no centro de interconexão	0,389	0,389
10 - Complexidade de senhas	0,7666	0,7666
12 - Segmentação da rede metropolitana de acesso aberto	0,9285	0,9285
Média	$M_1 = 0,6608$	$M_2 = 0,6183$
Mediana	0,7296	0,6046
Desvio padrão	0,1998	0,2249
Coeficiente de variação (%)	$V_1 = 30,23$	$V_2 = 36,38$

Onde M_1, V_1, M_2 e V_2 denotam os indicadores globais do modelo 1 e do modelo 2, respectivamente.

Os indicadores globais de 0,6608 e 0,6183 aliados à baixa dispersão dos conjuntos de dados podem ser considerados resultados muito bons, ou seja, o comprometimento com a segurança da informação existe e não representa um fato isolado. Aliado ao fato de que este foi o primeiro teste de segurança aplicado à rede municipal de Pedreira, concluímos que os resultados foram satisfatórios.

Além disso, os bons resultados são também reforçados pela distribuição do conjunto de dados. A Figura 6.10 mostra a distribuição dos conjunto dos dados relativos aos resultados das métricas. Os pontos vermelhos indicam os valores das métricas e os pontos azuis as médias. Note que em ambos os modelos, somente duas métricas no modelo 1 e três no modelo 2 ficaram abaixo da média, representando um percentual de $0,22$ e $0,33$ respectivamente. Estes valores representam um indicador positivo para a segurança da rede. Ainda no modelo 1, os valores estão mais agrupados ao redor da média do que no modelo 2, representando uma maior variação no conjunto de dados do modelo 2. Isto pode ser justificado pela maior rigidez do modelo 2 quando comparado com o modelo 1, fato demonstrado no capítulo 4.

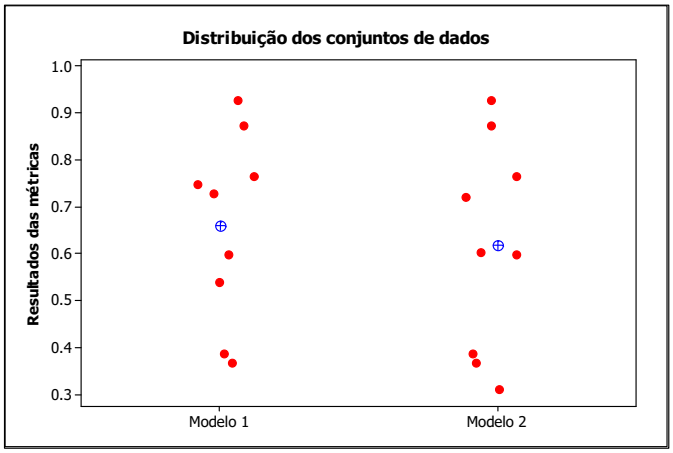

Fig. 6.10: Distribução dos conjuntos de dados

Analisando os dados, podemos afirmar que os modelos obtiveram resultados semelhantes, já que somente 3 das 8 métricas calculadas não tiveram o mesmo desempenho. A maior diferença ficou por conta do coeficiente de variação. Isto ocorreu, principalmente pela grande diferença entre os resultados das métricas número 1 e 2 para os dois modelos. A métrica 1, que mede a segurança entre os prédios da MBAN, quando comparada entre os modelos 1 e 2, variou de $0,5411$ para $0,3117$, uma queda de 42%. Já a métrica 2, que mede os requisitos de segurança da rede VoIP, variou de $0,7296$ para $0,6046$ representando uma queda de aproximadamente 17%.

As Figuras 6.11 e 6.12 representam a distribuição das métricas pela classificação da MBAN. Os resultados das métricas foram agrupados de acordo com sua classificação e agregados utilizando a média.

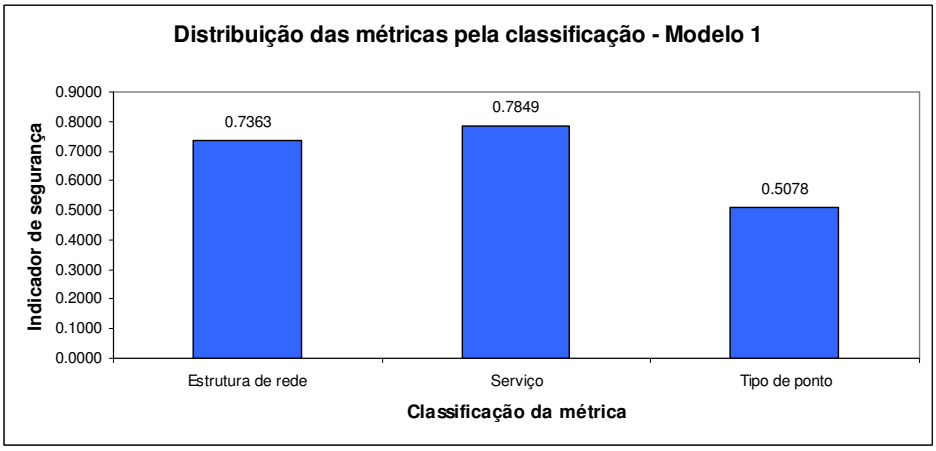

Fig. 6.11: Distribuição das métricas de acordo com a classificação da MBAN - Modelo 1

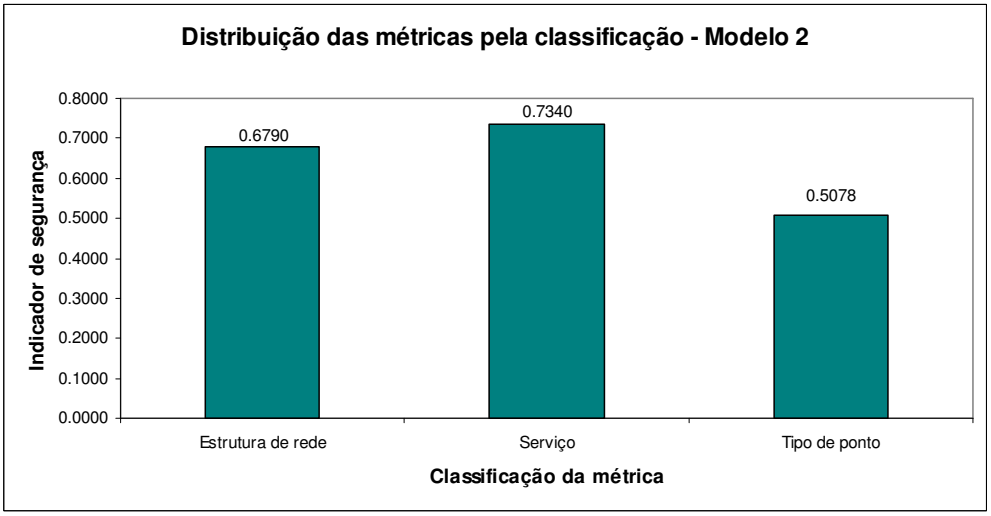

Fig. 6.12: Distribuição das métricas de acordo com a classificação da MBAN - Modelo 2

Com relação a segurança das camadas da rede metropolitana de acesso aberto, os dois modelos geraram resultados idênticos. As métricas de serviços foram as que obtiveram melhores resultados, seguidos pela estrutura de rede e por último a camada dos pontos de interconexão, também chamada de tipos de pontos. Esse resultado é importante para os administradores da rede metropolitana de acesso aberto visualizarem quais áreas obtiveram os piores e melhores resultados.

A primeira fase da construção da rede metropolitana de acesso aberto de Pedreira consistiu no planejamento e implantação da estrutura física e lógica da rede. A segunda fase é destinada a disponibilização dos serviços que trafegarão sobre a Infovia. Atualmente, o projeto está na segunda fase, ou seja, os investimentos aplicados na estrutura da rede e serviços podem explicar os resultados favoráveis das métricas de tais áreas, quando comparadas com os pontos de interconexão.

Toda a estrutura de informática como computadores e recursos humanos dos prédios públicos é legado da Prefeitura e até o momento não fez parte do projeto da Infovia Municipal. A falta de recursos, investimentos e definição de uma política de segurança, foi determinante para que as métricas de

pontos de interconexão 3 e 9 que tratam do gerenciamento das contas de usuários e da aplicação de *patchs* no centro de interconexão e que são estritamente ligadas a área de informática da Prefeitura, obtivessem resultados abaixo da média.

A última análise a ser realizada será sobre o desempenho dos servidores. Organizando os dados obtidos de três métricas relacionadas aos servidores, métricas 7, 9 e 10, a Tabela 6.7 pode ser construída. Este tipo de análise é conhecida como análise transversal [37].

Tab. 6.7: Análise transversal - Servidores

Componentes	Firewall	VoIP	Email
Backups fisicamente distantes	Sim	Sim	Não
Média Uptime	3064,5	3068,52	3070,5
Número de vulnerabilidades	136	13	75
Média CVSS	0,5877	0,6841	0,5681
Média Complexidade da senhas	0,69	0,69	0,66

Os servidores da Infovia Municipal de Pedreira obtiveram resultados semelhantes com relação à segurança da informação. As diferenças entre os componentes são pequenas, como por exemplo a média de uptime, onde a maior diferença é de 6 minutos de um servidor para o outro. Com relação a complexidade das senhas, apesar de ligeiramente melhor, os resultados do Firewall e VoIP estão muito perto do E-mail (0,03).

A maior disparidade é encontrada no número de vulnerabilidades de segurança, quesito em que o servidor VoIP leva grande vantagem apesar da média de pontuação CVSS ser maior que dos outros servidores, ou seja, apesar do baixo número de vulnerabilidades elas possuem em média maior criticidade. Analogamente, o servidor de E-mail, que mesmo com a melhor média de Uptime e de CVSS, não possui backups fisicamente distantes e conta com um alto número de vulnerabilidades detectadas, 75.

Apesar dos resultados semelhantes, o servidor VoIP leva uma pequena vantagem em relação aos outros. Além de ter backups fisicamente distantes, tem baixo número de vulnerabilidades, a segunda maior média de uptime e juntamente com o Firewall, a maior média com relação a complexidade das senhas.

A aplicação das métricas de segurança propostas neste trabalho proporcionaram diversos benefícios imediatos à rede metropolitana de acesso aberto de Pedreira. Dentre eles, podemos citar:

- Início das pesquisas para a aplicação de soluções criptográficas nos ramais VoIP.
- Proposta de integração dos computadores dos prédios públicos de Pedreira em um domínio de rede.
- Implantação de backups fisicamente distantes no servidor de E-mail.
- Aumento do link de Internet. Atualmente, a rede de Pedreira dispõe de dois links full-duplex de 8 mbits/s.

- Revisão da política de acesso e implementação das *Access Control Lists* nos *switches* e roteadores.
- Limitação da banda de download/upload destinada a população.
- Conscientização de gerentes e executores sobre os riscos de segurança em redes metropolitanas de acesso aberto. Motivação para a disponibilização de recursos financeiros na área de segurança da informação.

Capítulo 7

Conclusões e trabalhos futuros

O sucesso na implantação de redes metropolitanas de acesso aberto depende da confiabilidade dos sistemas que a constituem. A garantia desta confiabilidade pode ser obtida através da gestão criteriosa das questões ligadas à segurança da informação. As métricas de segurança são ferramentas que podem cumprir tais objetivos quando desenvolvidas e aplicadas adequadamente. Este trabalho propôs um modelo que apóia as tarefas de definir e aplicar as métricas.

Antes da definição das métricas, foi proposto um modelo com os atributos considerados indispensáveis para a formação das mesmas. O modelo das métricas de segurança para redes metropolitanas de acesso aberto foi construído com os seguintes atributos: objetivo, métrica, medida, origem dos dados, freqüência, classificação e fórmula. Cada um deles possui sua devida importância e freqüêntemente o termo "métrica" em nosso trabalho remete a este conjunto de componentes.

Um componente foi tratado de maneira especial. A fórmula de uma métrica foi alvo de esforços para que seu papel de indicador de segurança fosse cumprido de forma clara e genérica. A padronização da nomenclatura matemática e sugestão de dois modelos para o cálculo da fórmula foram contribuições não só para o desenvolvimento deste trabalho, mas também para a área de métricas de segurança em geral. Toda a base construída para os modelos: componentização(seguros e inseguros), escala, definição de termos e as formulações, podem ser reutilizadas em outros modelos de métricas de segurança.

Com o modelo pronto, o próximo passo foi o desenvolvimento do conjunto de métricas de segurança para redes metropolitanas de acesso aberto. Consideramos este o ponto chave do trabalho. A análise correta dos problemas de segurança de uma rede depende, principalmente, de um conjunto de métricas consistente. Quando se trata de uma rede metropolitana de acesso aberto, este conjunto de métricas deve ser capaz de medir com igual eficiência os problemas estruturais da rede, as vulnerabilidades dos serviços e as particularidades de cada um dos prédios a qual é formada.

Foi proposta uma metodologia para facilitar a análise dos dados obtidos com a aplicação das métricas. A metodologia consiste nos seguintes passos: preparo do ambiente para a coleta dos dados, automatização das ferramentas de coleta de dados, coleta dos dados, cálculo das fórmulas de cada métrica, organização das métricas de acordo com o resultado da fórmula, agrupamento dos resultados de cada métrica de acordo com sua classificação e, por fim, a análise individual dos dados coletados em cada métrica. Algumas ferramentas estatísticas foram usadas para apoiar a análise dos dados e também deram origem a dois importantes indicadores M e V que suportam o estudo da segurança em redes metropolitanas de acesso aberto: M, dado pela média aritmética entre cada um dos resultados

das fórmulas do conjunto de métricas selecionado e V, obtido pelo cálculo do coeficiente de variação.

Para mostrar os benefícios da utilização de métodos quantitativos na análise de segurança, nove métricas propostas neste trabalho foram aplicadas na rede metropolitana de acesso aberto de Pedreira, SP. O estudo de caso revelou dados interessantes como o acesso indevido de uma determinada sub-rede à outras sub-redes, a alta complexidade das senhas de servidores e equipamentos de rede, a evolução da rede VoIP, o alto índice de usuários das estações de trabalho com permissões de administrador, a latência na disponibilização de *patches* de segurança para os servidores entre outros. No final, a análise dos dados mostrou que a rede de Pedreira está com um nível de segurança considerado bom, já que em uma escala de 0 a 1 os resultados foram de 0,6608 para um modelo e 0,6183 para o outro modelo. Além da importância pelos resultados obtidos, o estudo de caso mostrou ser uma experiência de campo riquíssima devido a grande interação com diversas tecnologias e também pela diversidade de problemas reais enfrentados.

Apesar dos benefícios, algumas deficiências foram encontradas no uso de métricas para a análise de segurança em rede metropolitanas de acesso aberto. Uma delas, é a exigência de muitos dados de entrada, que podem transformar a aplicação de métricas de segurança em um grande problema para gestores de MBANs. Para uma análise coerente e precisa, um grande conjunto de métricas deve ser aplicado, o que consequêntemente implica em "garimpar" muitos dados. A extração dos dados, que vão alimentar as métricas, depende muitas vezes de softwares adequados, maquinário atualizado, estrutura computacional bem-definida e administradores de rede competentes, fatores que em um primeiro momento podem significar aos gestores grande prejuízo financeiro. Este é um grande problema da aplicação das métricas, sua alta dependência tecnológica e organizacional.

Outro grande problema, é a ausência de documentação com dados relacionados à segurança da informação de MBANs. Pois, uma maneira de refinar o modelo proposto, é aplicá-lo em outras MBANs ou então compará-lo com trabalhos existentes. Por fim, uma outra dificuldade que deve ser citada é a ausência de ferramentas específicas para o tratamento dos dados coletados. No decorrer do trabalho foram utilizadas várias ferramentas, desde o Microsoft Excel, Minitab e até "shell scripts" próprios. Um exemplo de ferramenta típica para a aplicação de métricas de segurança poderia ser desenvolvida utilizando o fluxo: automatização na coleta de determinados dados, gravação em base de dados, análise estatística. O desenvolvimento de uma ferramenta deste tipo poderia contribuir para o desenvolvimento das métricas de segurança, principalmente para a sua adesão em diversos setores, seja nas próprias MBANs ou em empresas e universidades.

Os estudos apresentados neste trabalho também abriram possibilidades para trabalhos futuros, dentre os quais:

- Desenvolvimento de novas métricas de segurança para redes metropolitanas de acesso aberto que contemplem as diversas áreas de concentração aqui propostas;
- Aplicar os modelos aqui propostos em outras redes metropolitanas de acesso aberto e assim iniciar a criação de uma base de dados com informações de segurança de diversas MBANs;
- Desenvolvimento de software para o armazenamento eficiente dos dados coletados, permitindo consultas de histórico, análises de regressão e simulações;
- Estudo do grau de dependência entre as métricas de segurança. Como um determinado resultado em uma métrica pode influenciar o resultado de uma ou mais métricas? Este tópico é

importante pois é sabido que a segurança da informação está relacionada com diversos componentes. Descobrir relações entre métricas e possíveis problemas de segurança pode diminuir o custo do trabalho em recuperação de incidentes de segurança. Por exemplo, “Em 77% dos casos estudados, se o problema de segurança causado pela métrica x for evitado, as métricas y e z também não vão apresentar problemas”.

- Aplicar os modelos de cálculo das fórmulas em métricas já existentes e comparar os resultados obtidos, na tentativa de descobrir padrões e boas práticas;

As métricas mostraram ser uma ferramenta de grande importância para o tratamento das questões relacionadas à segurança da informação. Principalmente no que diz respeito as seguintes áreas:

- Visualização de áreas problemáticas;
- Verificação da eficiência dos controles de segurança implementados;
- Proposta de melhorias e correções nos controles de segurança;
- Criação de base de dados sobre segurança, auxiliando as tomadas de decisão e compreensão dos problemas.

Referências Bibliográficas

[1] Incidentes reportados ao CAIS: por ano. http://www.rnp.br/cais/estatisticas/index.php.

[2] Estatísticas dos Incidentes Reportados ao CERT.br. http://www.cert.br/stats/incidentes/.

[3] Anni Sademies. *Process Approach to Information Security Metrics in Finnish Industry and State Institutions*. PhD thesis, University of Oulu, 2004.

[4] Securitymetrics.org. http://www.securitymetrics.org. Acessado em 30/09/2008.

[5] Cryptographic Key Length Recomendation. http://www.keylength.com/. Acessado em 08/09/2008.

[6] Leonardo de Souza Mendes. *Infovia Municipal - Um novo Paradigma em Comunicações*. Universidade Estadual de Campinas, 2006.

[7] Leonardo de Souza Mendes. Colocando as comunicações para impulsionar o desenvolvimento comunitário. *O Espaço Funcamp de Políticas Públicas: Um Exemplo de Interação Universidade-Sociedade*, 1:77–94, 2004.

[8] CERT. http://www.cert.org/.

[9] SANS. http://www.sans.org/.

[10] NIST. http://www.nist.gov/.

[11] Potential vulnerabilities in municipal communications network. Technical report, National Cyber Security Division Control Systems Security Program - US CERT, May 2006.

[12] Mercado de segurança de rede na América Latina movimentará 598.4 milhões de dólares em 2013. http://www.frost.com/prod/servlet/press-release.pag?docid=128005764. Acessado em 30/09/2008.

[13] Tecnologia da informação - código de prática para a gestão da segurança da informação. Technical report, NBR ISO-IEC 17799, 2001.

[14] Mark Stamp. *Information Security Principles and Practice*. Wiley Publishing, Inc., 2006.

[15] P. Geus and E. Nakamura. *Segurança de Redes em Ambientes Cooperativos*. Editora Berkeley, 2001.

[16] John E. Canavan. *Fundamentals of Network Security*. Artech House, 2001.

[17] Andrew S. Tanenbaum. *Computer Networks (International Edition)*. Prentice Hall, fourth edition, August 2002.

[18] Jonathan Davidson, James Peters, Manoj Bathia, and Satish Kalidindi. *Fundamentos de Voip*. CISCO, 2008.

[19] Telefonia Voip: Aprenda sobre Voip e saiba como economizar na conta de telefone. http://www.igf.com.br/aprende/dicas/dicasResp.aspx?dica_Id=5466. Acessado em 30/09/08.

[20] J. Bauer, Gai P., J. Kim, A. T. Muth, and Steven S. Wildman. Broadband: Benefits and policy challenges. Technical report, Michigan State University, 2002.

[21] FMEA. The case for municipal broadband in florida. Technical report, FMEA (Florida Municipal Electric Association), 2005.

[22] Harold Feld, Gregory Rose, Mark Cooper, and Ben Scott. *Connecting the Public: The Truth About Municipal Broadband*. Media Access Project, Abril 2005.

[23] Terrence McGarty and Ravi Bhagavan. Municipal broadband networks: A revised paradigm of ownership. Technical report, MIT ITC - Internet and Telephony Consortium, 2002.

[24] R. D. J. Kramer, A. Lopez, and A. M. J. Koonen. Municipal broadband access networks in the netherlands - three successful cases, and how new europe may benefit. In *AcessNets '06: Proceedings of the 1st international conference on Access networks*, page 12, New York, NY, USA, 2006. ACM Press.

[25] A. Alexiou, C. Bouras, V. Igglesis, V. Kapoulas, M. Paraskeuas, I. Scopoulis, and J. Papagiannopoulos. Deployment of broadband infrastructure in the region of western greece. In *Broadband Networks, 2005 2nd International Conference on*, pages 1510–1515Vol.2, 3-7 Oct. 2005.

[26] Y. Shim, H. Lee, and K. Yun. The growth of broadband internet in sweden: contributing factors. *Int. J. Advanced Media and Communication*, 1(2):122–138, 2006.

[27] China Stakes. http://www.chinastakes.com/story.aspx?id=246. Acessado em 30/09/2008.

[28] CityLink. http://www.citylink.co.nz/. Acessado em 30/09/2008.

[29] Elaine Lawrence, Mary Bina, Gordana Culjak, and Tarek El-Kiki. Wireless community networks: Public assets for 21st century society. In *Information Technology, 2007. ITNG '07. Fourth International Conference on*, pages 166–174, 2-4 April 2007.

[30] Eric Cole, Ronald Krutz, and James W. Conley. *Network Security Bible*. Wiley Publishing, Inc., 2005.

[31] John Vacca. *Guide to Wireless Network Security*. Springer, 2006.

[32] A. C. Middleton. Understanding the benefits of broadband: Insights for a broadband enabled ontario. Technical report, Ryerson University, 2007.

[33] Joel Rosenblatt. Security metrics: A solution in search of a problem. *EDUCAUSE Quarterly*, 3:8–11, 2008.

[34] Steffen Weiss, Oliver Weissmann, and Falko Dressler. A comprehensive and comparative metric for information security. In *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)*, pages 1–10, nov 2005.

[35] Shirley C. Payne. A guide to security metrics. SANS Security Essentials GSEC Practical Assignment Version 1.2e, June 2006.

[36] Paul W. Lowans. Implementing a network security metrics program. Technical report, SANS, 2002.

[37] Andrew Jaquith. *Security Metrics - Replacing Fear, Uncertainty and Doubt*. Addison-Wesley, 2007.

[38] M. Swanson, N. Bartol, J. Sabato, J. Hash, and Laurie Graffo. Security metrics guide for information technology systems. Technical report, NIST Special Publication 800-55, 2003.

[39] Gerald Kovacich. Information system security metrics management. *Computers & Security*, 16(7):610–618, 1997.

[40] S. Katzke. Security metrics. In *Proceedings of the Workshop on Information Security System Scoring and Ranking*, 2001.

[41] R. Henning. Information system security attribute quantification or ordering (commonly but improperly known as security metrics). In *Workshop on Information Security Scoring and Ranking*. Applied Computer Security Associates, 2001.

[42] Common Criteria. http://www.commoncriteriaportal.org/. Acessado em 11/11/2008.

[43] SSE-CMM (Systems Security Engineering Capability Maturity Model). http://www.sse-cmm.org/index.html. Acessado em 11/11/2008.

[44] INFOSEC Assurance Training and Rating Program. http://www.iatrp.com/iacmm.php. Acessado em 15/03/2009.

[45] COBIT. http://www.isaca.org/cobit/. Acessado em 30/09/2008.

[46] Maximilian Immo Orm Gorissen. Política de segurança da informação: A norma iso 17799. http://www.compustream.com.br/imagens/down/Artigo0- Acessado em 15/09/2008.

[47] Ricardo Mansur. Governança de tecnologia: Itil. http://www.profissionaisdetecnologia.com.br/artigos/arquivos/itil.pdf. Acessado em 10/09/2008.

[48] Gary Hinson. Seven myths about information security metrics. *ISSA (Information Systems Security Association) Journal*, July 2006:2–10, 2006.

[49] R. Savola. Towards a security metrics taxonomy for the information and communication technology industry. In *Software Engineering Advances, 2007. ICSEA 2007. International Conference on*, pages 60–60, 25-31 Aug. 2007.

[50] Metrics Center. http://www.metricscenter.org/index.php/plexlogicmetricviewer. Acessado em 10/09/2008.

[51] Scott Berinato. A few good information security metrics. http://www.csoonline.com/article/print/220462, 07 2005. Acessado em 30/09/2008.

[52] Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini. Analysis of iso/iec 17799: 2000 to be used in security metrics. In Hamid R. Arabnia, Selim Aissi, and Youngsong Mun, editors, *Security and Management*, pages 109–117. CSREA Press, 2004.

[53] Rodrigo S. Miani, Bruno B. Zarpelão, Leonardo de Souza Mendes, and Mario L. Proença Jr. Metrics application in metropolitan broadband access network security analysis. In *SECRYPT 2008 - International Conference on Security and Cryptography*, pages 473–476, 2008.

[54] Ecrypt. http://www.ecrypt.eu.org/. Acessado em 30/09/2008.

[55] WinAudit. http://www.pxserver.com/WinAudit.htm. Acessado em 15/03/2009.

[56] Admin PC Tools. http://www.adminpctools.com/asset-tracker/. Acessado em 15/03/2009.

[57] Portal do Software Público Brasileiro CACIC. http://www.softwarepublico.gov.br/. Acessado em 15/03/2009.

[58] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. *IACR Eprint Server, http://eprint.iacr.org/*, 2007/120, 2007.

[59] Common Vulnerability Scoring System (CVSS-SIG). http://www.first.org/cvss/. Acessado em 30/09/2008.

[60] Shavlik NetChk Protect. http://www.shavlik.com/. Acessado em 29/11/08.

[61] GFI LANguard. http://www.gfi.com/lannetscan/. Acessado em 29/11/08.

[62] NESSUS Network Vulnerability Scanner. http://www.nessus.org/nessus/. Acessado em 29/11/08.

[63] Password Strength Meter. http://www.passwordmeter.com/. Acessado em 15/03/2009.

[64] John R. Hauser and Gerald M. Katz. Metrics: You are what you measure! *European Management Journal*, 16(5):516–528, 1998.

[65] Oracle. www.oracle.com. Acessado em 11/09/2008.

[66] SQL Server. http://www.microsoft.com/brasil/servidores/sql/default.mspx. Acessado em 24/09/2008.

[67] Postgre Sql. http://www.postgresql.org/. Acessado em 30/09/2008.

[68] Minitab. http://www.minitab.com/.

[69] Murray R. Spiegel. *Probabilidade e Estatística*. Makron Books, 1978.

[70] K. Witcher. Fiber optics and its security vulnerabilities. Technical report, University Mary Washington - GIAC Security Essentials Certification (GSEC) Practical Assignment, 2005.

[71] Fiber optic intrusion detection systems. Technical report, Marketing Group of Network Integrity Systems, 2005.

[72] How to Break WEP Encryption. http://www.wikihow.com/Break-WEP-Encryption. Acessado em 30/09/2008.

[73] A step by step guide to breaking WEP. http://www.wirelessdefence.org/Contents /stepbystepWEP.htm. Acessado em 30/09/2008.

[74] Open VPN. http://openvpn.net/. Acessado em 28/09/2008.

[75] Asterisk. http://www.asterisk.org/.

[76] SANS Top-20 2007 Security Risks. http://www.sans.org/top20/. Acessado em 29/11/2008.

[77] Network Management Suite. www.mishelpers.com/network_management/index.html. Acessado em 30/09/2008.

[78] Contas de usuário e de computador. http://technet2.microsoft.com/windowsserver/pt-br/library/91a98c38-38c5-49dc-83bf-e69d8e1dbbfa1046.mspx?mfr=true. Acessado em 30/09/2008.

[79] Radius. http://freeradius.org/. Acessado em 19/09/2008.

[80] The High Availability Linux Project. http://www.linux-ha.org/. Acessado em 30/09/2008.

[81] MRTG The Multi Router Traffic Grapher. http://oss.oetiker.ch/mrtg/. Acessado em 29/11/2008.

[82] Zombie Machine. http://www.mysecurecyberspace.com/encyclopedia/index/zombie-machine.html. Acessado em 17/09/2008.