UNIVERSIDADE FEDERAL DO PAMPA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

TIAGO BELMONTE NASCIMENTO

UMA PROPOSTA DE DESENVOLVIMENTO DE MÉTRICAS PARA A REDE DA UNIPAMPA

DISSERTAÇÃO DE MESTRADO

Alegrete
2013

TIAGO BELMONTE NASCIMENTO

UMA PROPOSTA DE DESENVOLVIMENTO DE MÉTRICAS PARA A REDE DA UNIPAMPA

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Engenharia Elétrica da Universidade Federal do Pampa como requisito parcial para obtenção do titulo de Mestre em Engenharia Elétrica.

Orientador: Dr. Jorge Pedraza Arpasi

Alegrete

2013

N395p Nascimento, Tiago Belmonte
Uma proposta de desenvolvimento de métricas para a rede da Unipampa / Tiago Belmonte Nascimento – 2013.
97 p. ; 30 cm

Dissertação (Mestrado) – Universidade Federal do Pampa, Campus Alegrete, 2013.
“Orientação: Prof. Dr. Jorge Pedraza Arpazi”.

1. Métricas de segurança. 2. Redes de computadores. 3. Segurança de redes. 4. Probabilidade. I. Título.

Catalogação na Fonte: Cátia Rosana Lemos de Araújo – CRB 10/1451

TIAGO BELMONTE NASCIMENTO

UMA PROPOSTA DE DESENVOLVIMENTO DE MÉTRICAS PARA A REDE DA UNIPAMPA

Dissertação apresentada ao Programa de Pós-graduação Stricto Sensu em Engenharia Elétrica da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Mestre em Engenharia Elétrica.

Área de concentração: Sistemas de Energia

Dissertação defendida e aprovada em: 25 de julho de 2013.
Banca examinadora:

Prof. Dr. Jorge Pedraza Arpasi
Orientador
UNIPAMPA

Prof. Dr. Vinicius Jacques Garcia
UFSM

Prof. Dr. Jumar Luis Russi
UNIPAMPA

Dedico

A minha mãe Zulmira por sempre nos incentivar a estudar e a concluir os projetos que iniciamos.

A minha esposa Vaneisa e meu filho Augusto pelo apoio nos bons e maus momentos.

AGRADECIMENTOS

Ao professor Dr. Jorge Arpasi pela orientação e pelo apoio para que eu realizasse o curso de mestrado.

Ao professor Diego Kreutz, ao analista Ricardo Lazzari e a toda a equipe do NTIC pela colaboração no desenvolvimento deste trabalho.

Aos professores doutores do PPGEE, Jumar Russi, Alessandro Girardi, Daniel Bernardon e Márcio Stefanello minha gratidão pelas contribuições e pela forma de conduzir o curso em todas as etapas.

A todos os colegas de curso pelo convívio e pelos momentos de amizade.

Ao meu amigo Antonio Dalmolin, ex-colega de graduação e de trabalho, pela ajuda e companheirismo no Alegrete.

A minha mãe Zulmira e minha família pelo incentivo e carinho.

Ao meu amigo professor Dr. Eduardo Terrazzan pela oportunidade de aprender a ensinar algo além da física.

Ao professor Henrique Schetinger Filho pela amizade e pela ajuda à ingressar no curso.

Ao professor Nestor Santini pela confiança e incentivo a trabalhar nos atuais Institutos Federais.

Aos colegas técnicos de laboratório do IFRS pelo apoio em todos os momentos.

RESUMO

Um dos maiores desafios da implantação da Universidade Federal do Pampa como uma instituição pública de ensino superior no interior do Rio Grande do Sul é a estruturação de sua rede de dados. Devido às suas peculiaridades a rede de computadores da UNIPAMPA necessita de controles eficientes para garantir sua operação com estabilidade e segurança. Dessa forma, torna-se imprescindível o uso de sistemas confiáveis de comunicação que interliguem todas estas unidades descentralizadas. Em geral, a confiabilidade dos sistemas de comunicação pode ser melhorada em três grandes frentes de ação. 1) manipulação e codificação da informação, 2) melhoria de recursos como potência e banda nos canais de comunicação físicos 3) levantamento de métricas nos pontos de transmissão e recepção. A fim de colaborar neste processo, nosso trabalho consistiu na elaboração de uma proposta do uso de métricas na política de segurança desta rede, tornando mais eficiente a detecção de vulnerabilidades e a orientação de novas políticas de segurança e investimentos. As 10 métricas apresentadas e o método que foi utilizado para gerá-las podem ser aplicados em qualquer rede com características similares à rede da Unipampa.

Palavras-chave: Métricas de segurança. Redes de computadores. Segurança de redes.

ABSTRACT

One of the biggest challenges in the implementation of the University of Pampa as a public university in the countryside of the state of Rio Grande do Sul is the structure of its data network. Due to its peculiarities, the Unipampa's computer network needs efficient controls to ensure operations with stability and safety. Thus, it becomes essential to use reliable communication systems that interconnect all these decentralized units. In general, the reliability of communication systems can be improved in three major areas of action. 1) manipulation and encoding of information, 2) improving resources such as power and bandwidth in communication physical channels 3) survey metrics at points of transmission and reception. Aiming to contribute in this process, our research consisted in elaborating a proposal of metric use in the security policy of this network, making the vulnerability detection more efficient as well as the orientation of new policies of safety and investment. The 10 metrics and presented method was used to generate them may be applied in any network with similar characteristics to the network of Unipampa.

Keywords: Security Metrics. Computer Networks. Network Security.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Assim como a evolução tecnológica, mudanças significativas ocorreram nas estruturas da administração pública. A descentralização física e lógica da administração criou novas demandas, como por exemplo, a necessidade de uma intercomunicação veloz e estável, entre diferentes setores de uma instituição como laboratórios, secretarias, campus e reitoria.

Dessa forma, torna-se imprescindível o uso de sistemas confiáveis de comunicação que interliguem todas estas unidades descentralizadas. Em geral, a confiabilidade dos sistemas de comunicação pode ser melhorada em três grandes frentes de ação. 1)manipulação e codificação da informação, 2)melhoria de recursos como potência e banda nos canais de comunicação físicos 3)levantamento de métricas nos pontos de transmissão e recepção. Existe uma abundante literatura e métodos a respeito do campo 1) que é a codificação da informação, por exemplo em Arpasi (2011) foi apresentado um método de codificação baseado na teoria dos grupos algébricos. Esta dissertação aborda a frente de ação 3).

No caso da Universidade Federal do Pampa (UNIPAMPA), devido ao caráter descentralizado e geograficamente distribuído, os serviços básicos como links de dados, VoIP, videoconferência, conferência web, serviços de telefonia convencional (fixa e móvel), redes de dados móveis (3G ou similares) e infraestrutura de portais/sites Web, são essenciais para o bom funcionamento da instituição.

A interconexão de nossa instituição com a rede mundial de computadores foi viabilizada através de contatos com a RNP e o MEC. O primeiro link com a RNP (SLDD de 34 Mbps entre o Núcleo de Tecnologia da Informação e Comunicação - NTIC e o PoP-RS, via fibra óptica) foi entregue no final de 2009.

A escolha do tema desta proposta se deu pelo desafio proporcionado pelas características da rede da UNIPAMPA como dimensões, multisserviços, estabilidade, segurança e pelo pioneirismo. Até o inicio deste trabalho as informações e dados coletados não eram analisados de modo conjunto e sistematizado.

1.1 A Rede RNP[1]

Primeira rede de acesso à Internet no Brasil, a Rede Nacional de Ensino e Pesquisa (RNP) integra mais de 800 instituições de ensino e pesquisa no país, beneficiando a mais de três milhões de usuários. Esta rede foi criada em 1989 pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infraestrutura de rede Internet nacional para a comunidade acadêmica. A rede começou a ser montada em 1991. Em 94, já atingia todas as regiões do país. Entre 2000 e 2001, a rede foi totalmente atualizada para oferecer suporte a aplicações avançadas. Desde então, o backbone RNP possui pontos de presença em todos os estados brasileiros. Em 2005, a tecnologia do backbone é novamente atualizada com links ópticos operando a múltiplos gigabits por segundo.

A RNP oferece conexão gratuita à Internet para instituições federais de ensino superior ligadas ao Ministério da Educação (MEC), unidades de pesquisa federais ligadas ao MCT, agências de ambos os ministérios e outras instituições de ensino e de pesquisa públicas e privadas. Além da integração do território brasileiro, a rede RNP oferece conexões internacionais para os Estados Unidos. Um universo estimado em mais de um milhão de usuários da comunidade acadêmica brasileira se beneficia dessa infraestrutura que estimula o progresso da ciência e da educação superior no país.

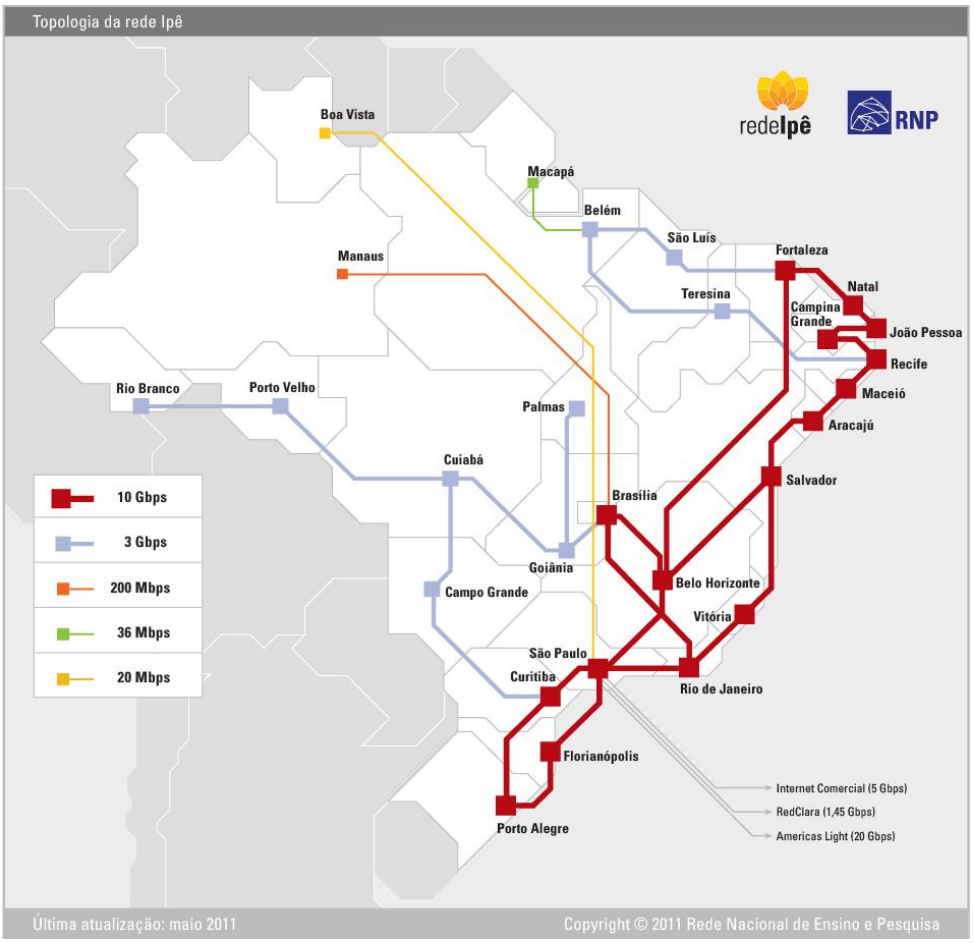
1.2 A rede Ipê

A rede Ipê é uma infraestrutura de rede Internet voltada para a comunidade brasileira de ensino e pesquisa. Nela conectam-se as principais universidades e institutos de pesquisa do país, beneficiando-se de um canal de comunicação rápido e com suporte a serviços e aplicações avançadas.

Baseada em tecnologia de transmissão óptica, a rede Ipê está entre as mais avançadas do mundo e possui conexão com redes acadêmicas estrangeiras, tais como Clara (América Latina), Internet2 (Estados Unidos) e Géant (Europa).

[1] Fonte: http://www.rnp.br/rnp/

Figura 1 – Mapa do Backbone RNP



Fonte: RNP (2013)

1.3 Sobre o CAIS

O CAIS – Centro de Atendimento a Incidentes de Segurança, atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

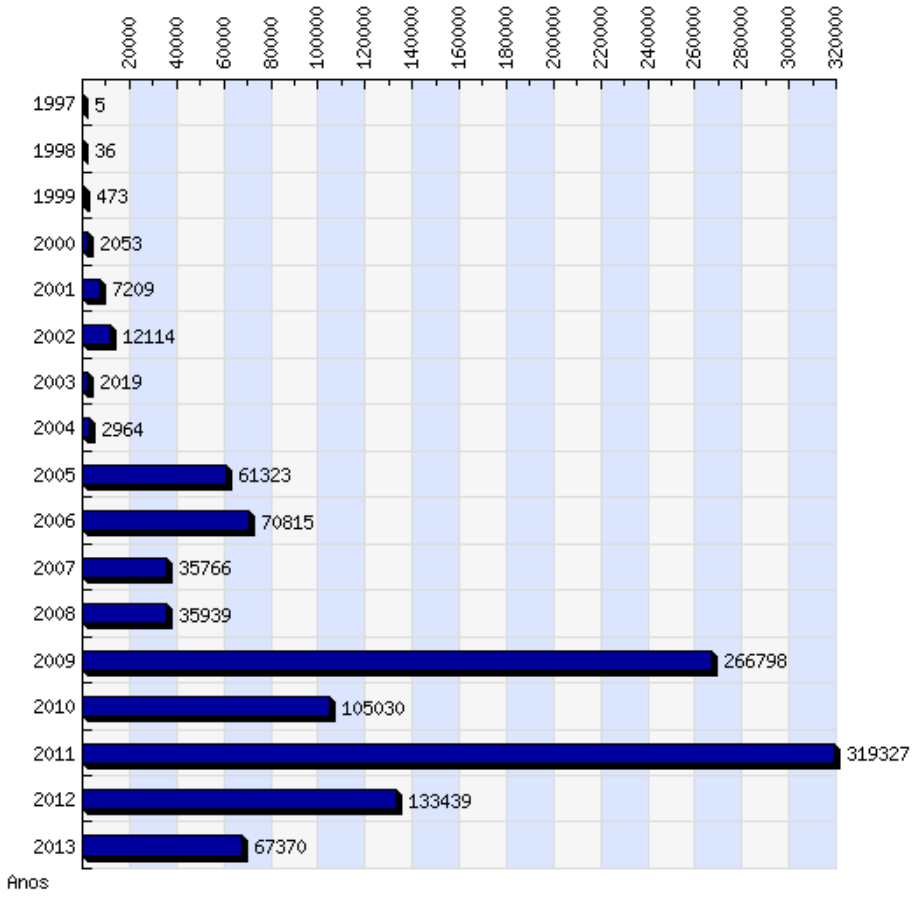
Atividades do CAIS:

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

- Recomendação de políticas para os PoPs.
- Recomendação de políticas para o backbone da RNP.

Estatísticas de Incidentes reportados ao CAIS por ano:

Figura 1 - Incidentes reportados ao CAIS por ano



Fonte: CAIS (2013)

1.4 Sobre o CERT.br

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. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil.

Estas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

As atividades conduzidas pelo CERT.br fazem parte das atribuições do CGI.br[2] de:

- Estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
- Promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem como para a sua crescente e adequada utilização pela sociedade;
- Representação nos fóruns técnicos nacionais e internacionais relativos à Internet;

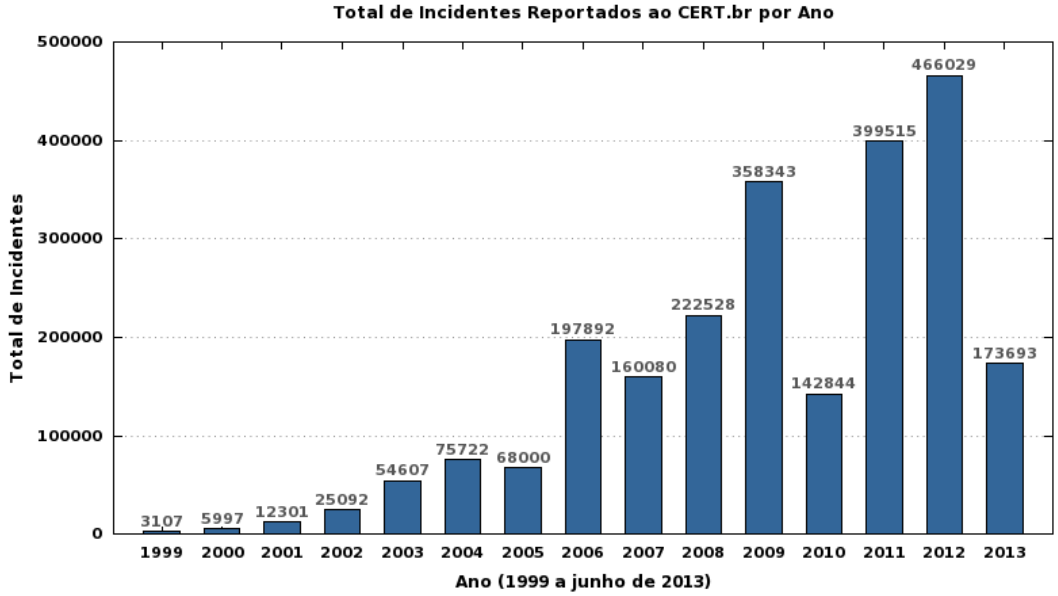
Bem como dos objetivos do NIC.br[3], conforme seu Estatuto4:

- Atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis;
- Promover ou colaborar na realização de cursos, simpósios, seminários, conferências, feiras e congressos, visando contribuir para o desenvolvimento e aperfeiçoamento do ensino e dos conhecimentos nas áreas de suas especialidades.

[2] Comitê Gestor da Internet no Brasil. As atribuições estão disponíveis em http://www.cgi.br/regulamentacao/decr4829.htm

[3] Núcleo de Informação e Coordenação do Ponto BR. O estatuto está disponível em http://www.nic.br/estatuto/

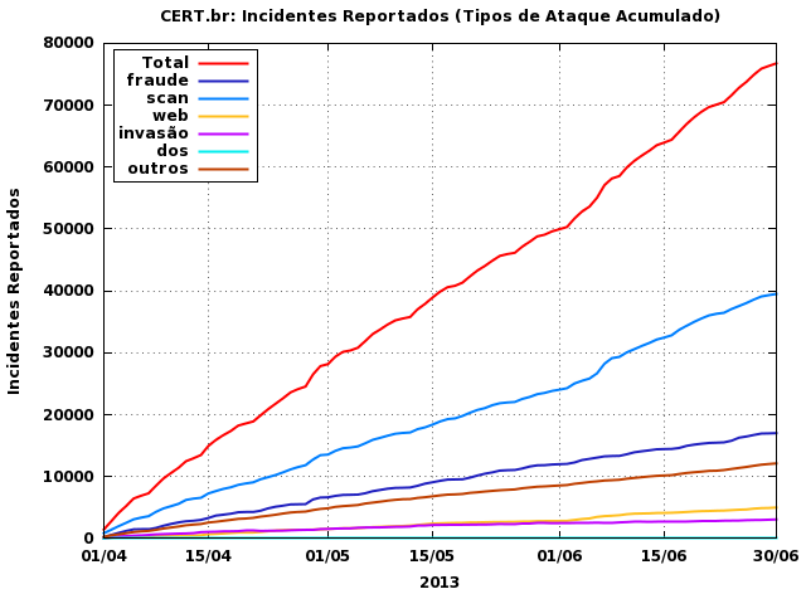
Figura 3 – Gráfico do total de incidentes reportados ao CERT.br



Fonte: CERT.br (2012)

Os dados na figura 4 representam os incidentes de segurança envolvendo redes conectadas à Internet em todo Brasil.

Figura 4 – Gráfico de incidentes por tipo de ataque



Fonte: CERT.br (2012)

Os dados de ambos os gráficos mostram que os incidentes de segurança continuam crescendo de forma assustadora. A revolução digital e o crescimento das vendas de computadores, aliada a falta de informação e a falta de capacitação são alguns dos fatores que podem explicar este crescimento. Em 2007 esse número diminuiu e as expectativas para 2008 também indicavam que os valores alcançados até o ano 2006 dificilmente se repetiriam. Acreditava-se que Isto se devia, a quatro fatores:

- Maior capacidade de identificação dos sistemas comprometidos e a consequente 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;
- Aumento na disseminação da informação sobre segurança digital
- O aumento de investimentos em soluções de segurança.

Mas, infelizmente, o tempo revelou o contrário.

1.5 Contribuições da dissertação

Neste trabalho pretende-se contribuir para:

- Dar subsídios para a escolha do melhor método de cálculo e as melhores métricas de segurança a serem utilizadas na rede da Universidade Federal do Pampa (UNIPAMPA);
- Enumerar um conjunto de métricas mais importantes para o caso estudado;
- Criar novas métricas para rede da UNIPAMPA, em função de suas características;
- Contribuir para uma política de segurança mais eficaz nesta instituição.

1.6 Estrutura da dissertação

No capítulo 1 é apresentada uma introdução básica a redes de computadores.

No capítulo 2 tem-se o desenvolvimento do conceito de métrica e seu cálculo, e a metodologia aplicada para coleta e análise de dados.

No capítulo 3 são apresentadas as métricas escolhidas pela equipe para serem aplicadas ao caso em estudo; a estrutura básica da rede da Unipampa; os resultados obtidos e sua análise.

No capítulo 4 tem-se as conclusões.

1.7 Redes de computadores

Algumas das principais conquistas tecnológicas dos últimos séculos foram no campo da aquisição, processamento e distribuição de informações. Pode-se destacar o desenvolvimento das redes de telegrafo, rádio, telefone, televisão e atualmente as redes de computadores.

Com a rapidez com que se dá este desenvolvimento, com uma acentuada convergência ocorrendo principalmente neste novo século, tem-se cada vez mais uma diminuição entre o tempo de coleta, transporte, armazenamento e processamento de informações. Instituições em qualquer parte do mundo podem acessar suas unidades remotas ou publicar resultados de pesquisas com um simples apertar de botão. À medida que a velocidade de coleta, processamento e distribuição de informações cresce, a demanda por essas informações e a necessidade de sofisticação destes processos também vai crescendo (TANENBAUM, 2003).

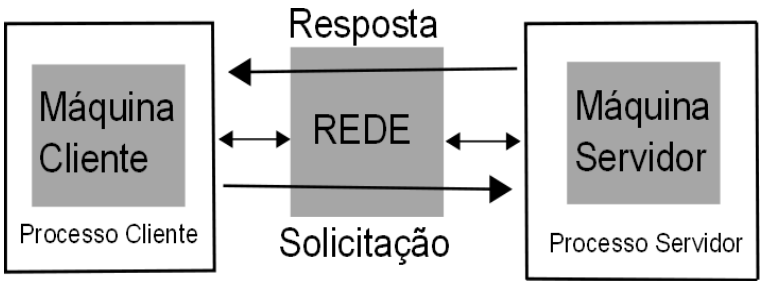
Inicialmente os sistemas computacionais eram altamente centralizados. Apenas grandes empresas e instituições contavam com algumas dezenas de computadores. A ideia de miniaturização destes grandes computadores era apenas ficção cientifica na época.

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais eram organizados. O conceito de “centro de computação” como uma sala com um grande computador ao qual os usuários levam seu trabalho para processamento agora está totalmente obsoleto. O Método de um único computador robusto atendendo a todas as necessidades de uma instituição foi superado substituindo-o pelas redes de computadores, onde as necessidades são atendidas por um grande número de computadores interconectados.

Uma rede de computadores é constituída por um conjunto de computadores e /ou dispositivos pessoais autônomos interconectados por meio de tecnologias de comunicação compatíveis.

Dois computadores estão interconectados quando podem trocar informações entre si. Esta conexão pode ser realizada via cabo ou por ondas eletromagnéticas.

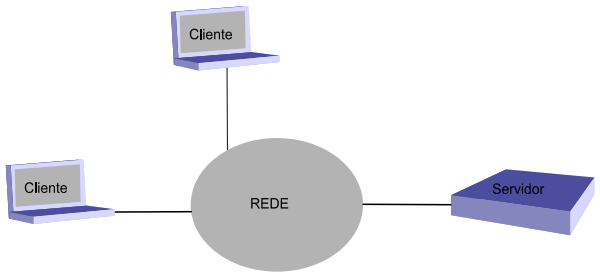
Figura 5 – Método de rede cliente/servidor



Fonte: Nascimento (2013)

Existem redes de vários tamanhos, métodos e formas e embora pareça estranho a internet não é uma única rede, mas uma rede de várias redes, e a World Wide Web (WWW) é um sistema distribuído que funciona na internet. A principal diferença é que em um sistema distribuído, o usuário percebe um conjunto de computadores independentes como um único sistema coerente. Em geral ele tem um único Método ou paradigma que apresenta aos usuários. Frequentemente uma camada de software sobre o sistema operacional, chamada middleware, é responsável pela implementação deste Método. No caso da WWW tudo tem aparência de uma página web para o usuário. Estes elementos estão ausentes numa rede de computadores. Nela os usuários percebem as máquinas na rede e suas características particulares como hardware e sistema operacional.

Figura 6 – Uma rede formada de um servidor e dois clientes



Fonte: Nascimento (2013)

1.7.1 Hardware de rede

Um projeto de redes de computadores pode ser classificado principalmente quanto à tecnologia de transmissão e a escala.

Os dois tipos de tecnologia de transmissão mais utilizados atualmente são os Links de difusão e Links ponto a ponto (TANENBAUM, 2003).

As redes de difusão tem apenas um canal de comunicação, compartilhados por todas as máquinas da rede. Os pacotes enviados por qualquer máquina são recebidos por todas as máquinas. No momento em que o pacote é recebido a máquina lê o campo de endereço do pacote para saber qual o destinatário. Caso o pacote se destine à máquina receptora ela o processará caso contrário o pacote será simplesmente ignorado.

As redes ponto a ponto consistem em muitas conexões entre pares de máquinas individuais. Para um pacote ir da origem ao destino podem haver muitas rotas com diferentes tamanhos. Cabe a ele encontrar a melhor rota.

No caso da escala podemos classificar sistemas de vários processadores organizados por seu tamanho físico (TANENBAUM, 2003).

A) Temos as redes domésticas de um único usuário conectado a periféricos chamada Rede Pessoal onde a distância entre processadores é de 1m e os processadores estão localizados no mesmo metro quadrado; por exemplo um notebook conectado a um sistema de áudio por Wireless.

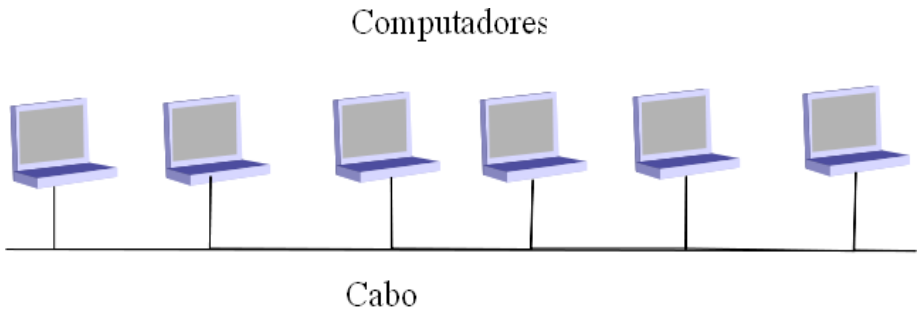
B) Temos redes mais abrangentes como as Redes Locais também chamadas LANs, podem ser utilizadas em salas, edifícios, campus. Permitem a troca de

informações e o compartilhamento de recursos entre estações de trabalho e computadores pessoais em prédios e instituições.

As principais diferenças da rede LAN para as outras redes são: o tamanho restrito do projeto que é dimensionado a partir do limite de tempo de transmissão na rede; A tecnologia de transmissão que geralmente consiste na conexão de todas as máquinas por meio de cabo com uma velocidade nas linhas que pode ir de 10 Mbps a 10 Gbps de acordo com o projeto; e topologia.

Na topologia conhecida como rede de barramento, cada máquina poderia transmitir em um determinado momento e não simultaneamente. Para resolver os conflitos (quando duas máquinas querem transmitir simultaneamente) criou-se o mecanismo de arbitragem IEEE 802.3, conhecido como Ethernet. Nesta rede de difusão de barramento com controle descentralizado os computadores podem transmitir sempre que desejam, pois, quando ocorre uma colisão de pacotes cada máquina irá aguardar um tempo aleatório para realizar uma nova tentativa de transmissão. Esta rede pode operar de 10 Mbps a 10 Gbps.

Figura 7 – Rede de difusão de barramento

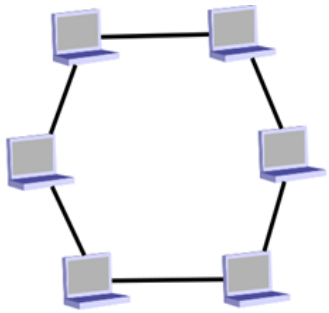


Rede de Difusão de Barramento

Fonte: Nascimento (2013)

Outro tipo de sistema de difusão é o anel. Nele cada bit propaga-se de modo independente. Cada bit percorre todo o anel antes mesmo de todo o pacote ser transmitido. Um exemplo de sistema de arbitragem para estas redes é o IEEE 802.5 (a rede Token Ring da IBM) é uma rede de difusão em anel que pode operar a 4 Mbps e 16 Mbps.

Figura 8 – Rede de difusão em anel



Fonte: Nascimento (2013)

Ainda pode-se dividir as redes de difusão de acordo com o modo em que o canal é alocado.

Elas podem ser estáticas, onde o tempo seria dividido em intervalos discretos e seria utilizado um algoritmo de rodizio, assim, cada máquina transmite apenas no intervalo de tempo que dispõe. Esta alocação desperdiça a capacidade do canal quando uma máquina não tem nada a transmitir em seu intervalo de tempo (slot) alocado a ela.

A alocação dinâmica resolve este problema, pois à máquina é permitido transmitir na medida em que ela realiza a solicitação.

Os métodos de alocação dinâmica de um canal podem ser centralizados ou descentralizados. No método centralizado de alocação de canal apenas uma unidade de arbitragem é que define quem transmite num determinado momento, a partir de um algoritmo interno. No método descentralizado de alocação de canal ocorre o contrário, cada máquina é que decide se é momento de iniciar uma transmissão ou não.

C) As Redes Metropolitanas (MAN – Metropolitan Area Network) abrangem uma cidade. Um exemplo de MAN é uma rede de tv a cabo que abrange uma ou mais cidades. Ao longo do tempo com a popularização de internet os mesmos operadores de tv a cabo começaram a disponibilizar o serviço de internet no espectro não utilizado do cabo. Existem outros exemplos de MAN além da tv a cabo padronizados como IEEE 802.16.

D) As Redes Geograficamente Distribuídas (WAN – Wide Area Network) ou Remotas, estão localizados no mesmo país ou continente. Abrangem uma grande

área geográfica. Elas contem um conjunto de máquinas (hosts) para executar as aplicações dos usuários. Os hosts são os computadores pessoais (PC) dos usuários conectados por uma sub-rede cuja função é transferir dados entre os hosts.

A conexão de duas ou mais redes é chamada inter-rede. A internet é um exemplo de inter-rede.

1.7.2 O problema do congestionamento

O congestionamento ocorre quando o número de pacotes sendo transmitidos através de uma rede começa a se aproximar do limite da capacidade de manipulação de pacotes da rede. O objetivo do controle de congestionamento é manter a número de pacotes dentro da rede abaixo do nível em que o desempenho cai drasticamente.

A falta de mecanismos de controle de fluxo dificulta o controle de congestionamento. Uma variedade de técnicas foram desenvolvidas para lidar com os congestionamentos e para dar diferentes garantias de qualidade de serviço aos diferentes tipos de tráfego.

As redes estabelecem um contrato de tráfego com cada usuário que especifica as características do tráfego previsto e do tipo de serviço que a rede irá proporcionar. A rede implementa técnicas de controle de congestionamento, de tal forma a proteger a rede do congestionamento, enquanto encontra os contratos de tráfego.

Uma rede monitora o fluxo de células de cada fonte de entrada e pode descartar ou rotular para descartar possíveis células que excedem o contrato de tráfego acordado. Além disso, a rede pode moldar o tráfego proveniente de usuários, agrupando temporariamente as células para suavizar os fluxos de tráfego.

2 DESENVOLVIMENTO

Neste capítulo apresenta-se o conceito de métrica, suas características e propriedades, os métodos utilizados para o seu cálculo e a metodologia de aplicada.

2.1 Desenvolvimento de métricas

As métricas estão presentes em nosso dia a dia. Sem elas não teríamos como comparar ou avaliar algo. Desde a aparência de uma pessoa até o desempenho de um atleta.

Por exemplo, se tratando da aparência das pessoas elas podem ser avaliadas ou classificadas como pessoas feias ou pessoas bonitas, ou uma pessoa pode ser considerada interessante ou desprezível, mas tudo dependerá das métricas que foram utilizadas para chegar a esta classificação. Observa-se que estas métricas são de natureza qualitativa e o seu resultado pode mudar conforme a pessoa que as aplica.

No caso de um atleta podemos avaliar seu desempenho de modo quantitativo, medindo sua qualidade como competidor. Se ele for um jogador de basquete, por exemplo, uma métrica que pode ser utilizada para aferir boa ou má qualidade a ele, seria os pontos realizados por partida e isso seria medido pela divisão do número de pontos que ele realizou pelo número de partidas disputadas por ele.

No caso das métricas de segurança, elas nos possibilitam avaliar de modo quantitativo o quão seguro é um determinado local, uma organização, uma instituição ou o quão segura e estável é uma determinada rede de computadores.

Serão apresentados alguns dos diversos métodos presentes na literatura para o desenvolvimento de métricas de segurança para Redes de computadores. Os Métodos escolhidos também podem ser utilizados em qualquer métrica de segurança definida com base na literatura sobre métricas de segurança.

Para lidar com os problemas de segurança e vulnerabilidades de uma rede é necessário a implementação de controles e políticas de segurança Rosenblatt (2008). E o resultado destes controles devem nortear os investimentos em melhorias na estrutura de segurança de informação da instituição.

Grandes organizações da área de segurança da informação como CERT (Computer Emergency Response Team) e NIST (National Institute of Standards and Technology) recomendam a implementação de programas de métricas de segurança em corporações. Por exemplo, em Tarnes (2012) é apresentada uma pesquisa qualitativa sobre a aplicação de métricas de segurança em cinco instituições privadas e governamentais.

Através da combinação de objetivos definidos com a 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 instituição (PAYNE, 2006).

A definição de métricas passa por dois conceitos. Segundo autores da área existem duas abordagens:

- Para Lowans (2002), Sademies (2004) e Payne (2006) devemos definir o conceito de medida e a partir dele o de métrica.
- Por outro lado, Jaquith (2007) e Kovacich (1997) optam por não diferenciar os conceitos de métrica e de medida.

Para Kovacich (1997) Métrica é um padrão de medidas utilizando análises quantitativas, estatísticas ou matemáticas.

Para Lowans (2002) Métricas são um conjunto de medidas que geram uma abordagem quantitativa de algo, a respeito de uma rede, ao longo do tempo.

Para Swanson (2003). Métricas são ferramentas projetadas para facilitar a tomada de decisões e melhorar o desempenho e prestação de contas através da coleta, análise e divulgação de dados.

Para Payne (2006) medidas, como dados puros, são geradas através de contagem enquanto métricas, como interpretações, são geradas através de análises.

Para Jaquith (2007), qualquer quantificação de um problema e seus resultados em um valor numérico pode ser considerado uma métrica.

Neste trabalho, devido a frequentes confusões e diferentes abordagens presentes na literatura, optou-se por separar o conceito de métrica e o conceito de medida e defini-los da forma mais clara possível.

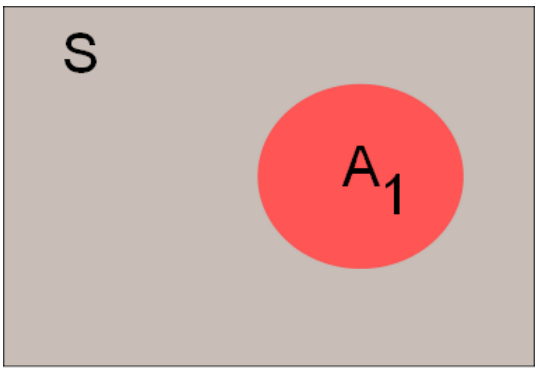
Seguindo orientações presentes na literatura Miani (2009) definiu Métrica de Segurança como a análise quantitativa de um conjunto específico de medidas ao longo de um período, dentro da finalidade da segurança da informação. A análise é quantitativa para evitar uma abordagem superficial, na qual detalhes importantes para a segurança permaneçam ocultos como poderia ocorrer numa abordagem

qualitativa. “O objetivo primário de uma métrica é transformar dados brutos em informações passíveis de análise.” (MIANI, 2009).

Neste trabalho optamos pela fundamentação na teoria de conjuntos e probabilidade para definir métrica como uma ação (um Controle) para análise ou proteção de uma rede ou conjuntos de computadores enquanto sua quantificação (medida) seria feita pelo estabelecimento de eventos relacionados a ela (as Ocorrências).

A medida da métrica $|A_1|$ seria constituída pelo conjunto afetado ou relacionado com o procedimento ou controle (S).

Figura 9 – Conjunto da métrica



Fonte: Nascimento (2013)

2.2 Atributos das métricas

As métricas também podem ser classificadas ou avaliadas como boas ou ruins. Tudo depende da utilidade de seus resultados ou da sua própria coerência.

Segundo Jaquit (2007) as métricas devem ser:

1. Definidas de maneira consistente, sem critérios subjetivos;

   Dar resultados equivalentes quando aplicadas ao mesmo conjunto de dados por diferentes pessoas. Devem ser calculadas de preferência por métodos computacionais para evitar falhas humanas.

2. Fáceis de coletar, de preferência de modo automatizado;

Métricas levam tempo para serem calculadas. Métodos ineficientes para coletar tais dados podem prejudicar o planejamento da instituição de acordo com tempo a ser utilizado para análise dos resultados obtidos.

3. Expressas em números cardinais ou porcentagem, não de maneira qualitativa com rótulos como ‘alto’, ‘médio’ e ‘baixo’.

Por exemplo, considere que foram abertos 10 chamados para uma determinada equipe de suporte e destes chamados foram atendidos 5 logo:

$(5/10) = 0{,}5$

ou seja,

$0{,}5 * 100 = 50\%$

Cinquenta por cento dos chamados foram atendidos, ou seja, a equipe esta trabalhando com uma eficiência de 50%.

4. Expressas utilizando ao menos uma unidade de medida como ‘chamados’, ‘infecções’ ou ‘Mbps’.

5. Minimamente relevantes a fim de que seus resultados possam fomentar a tomada de decisões.

Devem possuir um significado para as pessoas que as analisam para fomentar decisões, possibilitando a realização de medidas e melhoramentos na performance de qualquer processo.

2.3 Classificação das métricas

Segundo os trabalhos de Sademies (2004), Jaquith (2007) e Swanson (2003), as métricas podem ser classificadas pelos seguintes métodos:

Método 1 – Sademies

Estuda a aplicação das métricas em empresas finlandesas. Utiliza como referência os trabalhos realizados no Workshop on Information Security Scoring and Ranking (2001).

O método 1 deve ser constituído de três componentes

- O objeto a ser medido (um sistema ou produto).
- Os parâmetros de segurança que serão utilizados para comparação do objeto que está sendo medido.
- O método de medida: testes diretos, observações do sistema e avaliação de vulnerabilidades.

O Método de Katzke extraído de Sademies (2004) propõem uma divisão das métricas em quatro categorias: técnicas (logs de sistema por exemplo), organizacionais (eficiência de processos), operacionais, “brainstormers”, individuais (aptidão dos colaboradores) e de ambiente (aspectos relevantes ao ambiente organizacional).

Método 2 – Jaquith

Este Método propõe uma divisão das métricas em dois grandes grupos: métricas técnicas para identificação e diagnóstico de problemas e métricas de eficiência de programas de segurança.

Métricas técnicas para identificação e diagnóstico de problemas São caracterizadas pela tentativa de detecção de problemas de segurança em toda a infraestrutura (física e lógica) da organização.

Estas métricas podem ser classificadas em:

- Defesa do perímetro: Ajuda a compreender as ameaças externas a instituição. Medem a eficácia dos antivírus, firewalls e sistemas de detecção de invasão.
- Cobertura e controle: Estas métricas caracterizam o nível de sucesso das políticas de segurança. Tem-se como exemplos: estações de trabalho e servidores com antivírus instalado, número de patches de segurança aplicado por máquina, etc.
- Disponibilidade e confiabilidade: Incidentes de segurança frequentemente provocam quedas de sistemas e consequentemente aumentam o tempo que um sistema fica fora de operação (downtime). Aumentar o tempo de operação de um sistema (uptime) exige minimização das falhas de segurança relacionadas ao downtime.
- Riscos em aplicações: estas métricas registram o número de defeitos, complexidade e índices de riscos em aplicações personalizadas ou desenvolvidas diretamente pela instituição.

Métricas de eficiência de processos

O objetivo das métricas de eficiência de processos é medir a eficiência dos programas de segurança que firam implementados.

Programas ou políticas de segurança são elaborados baseados em normas, guias e práticas definidas em documentos propostos por grandes organizações de TI. Entre os mais citados temos:

Série ISO 27000: é uma compilação de varias recomendações para boas práticas de segurança, que podem ser aplicadas por empresas. A serie NBR ISO/IEC 27000 é uma tradução da que foi elaborada pelo Join Technical Committee Information Technology, subcommittee IT Security Techniques.

NIST série 800: 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. Propõem três tipos de métricas:

- Implementação,
- Eficiência/efetividade
- Impacto.

Control Objectives for Information Technology (COBIT) é um manual para a gestão de Tecnologia da Informação (TI) publicado pelo Information Systems Audit and Control Foundation (ISACA). Fornece diversos recursos como um sumário executivo, framework, controle de objetivos, mapas de auditoria, conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do COBIT ajudam a otimizar 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.

2.4 Definição do programa de métricas

O ideal para se promover a implantação de métricas de segurança é realizar esta implementação através de um projeto, um programa de métricas de segurança. Ou simplesmente programa de segurança.

Objetivos do programa de métricas:

Todas as métricas propostas neste trabalho foram desenvolvidas de acordo com o objetivo de Gerar métricas capazes de proporcionar uma análise eficientemente dos riscos de segurança e fomentar a escolha das respectivas medidas preventivas em uma rede, etc...

Dessa forma, os futuros investimentos na área de segurança podem ser dimensionados apropriadamente e as precauções tomadas com relação aos riscos

de segurança, possibilitando o desenvolvimento sustentável da rede. Como este objetivo é genérico, ele pode ser utilizado para a criação de outras métricas de segurança.

Além do objetivo primário, temos também os objetivos secundários. Eles consistem em um conjunto de ações que se executadas, podem levar ao cumprimento do objetivo primário.

2.5 Como criar métricas

Na literatura temos dois métodos:

No primeiro método (top-down) é a partir dos objetivos do programa de segurança que serão definidas as métricas que podem ajudar a determinar se tais objetivos estão sendo cumpridos e por último as medidas que vão gerar as métricas.

No segundo método (bottom-up) 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.

Ambos os métodos podem ser empregados para gerar métricas dependendo do objetivo de segurança ou da dificuldade de identificação do que será medido.

2.6 Calculando a qualidade dos indicadores de segurança da rede

A seguir, apresentam-se os métodos adotados para o cálculo da qualidade das métricas de segurança para Redes. Estes métodos são baseados nos trabalhos de Swanson (2003), Payne (2006) e Miani (2009). Procurou-se chegar a um método mais simples possível, para que este método possa facilitar a criação de novas métricas e também seja aplicado em qualquer métrica de segurança já existente.

As equações foram definidas utilizando basicamente os conceitos de Probabilidade, Teoria dos Conjuntos e Combinatória.

2.6.1 Estrutura das Métricas

Uma das dificuldades na implantação de métricas na segurança de redes é a compreensão do seu conceito, sua estrutura matemática. Entendemos que a melhor

forma de popularizar o uso de Métricas de Segurança em redes de computadores independente de sua dimensão e tecnologia é facilitar a compreensão do que seria uma Métrica de segurança do ponto de vista matemático. Para isso, a melhor forma é começar com um exemplo:

2.6.1.1 Exemplo de métrica 1

Dada uma Métrica: Controle de segurança dos pontos de acesso de uma rede Wi-Fi. A Métrica será definida como um Controle e terá um conjunto de resultados denominado Espaço Métrico que define-se como S análogo ao espaço amostral presente na Teoria de Probabilidade.

Este Espaço Métrico específico será $S = \{P_1, P_2 P_3 \dots P_n\}$ onde seus componentes serão: $P_1 = ponto\ de\ acesso\ 1$; $P_2 = ponto\ de\ acesso\ 2$; $P_3 = ponto\ de\ acesso\ 3$; e P_n é o enésimo ponto de acesso da rede com $P_n \in \mathbb{R} | P_n > 0$.

O subconjunto deste Espaço Métrico será definido como Ocorrência A. Sendo que $A \subset S$.

Seguindo no mesmo exemplo, uma Ocorrência para o Espaço Métrico S seria: A ={pontos de acesso que utilizam WAP}

Continuando a analogia, tem-se que a medida da Qualidade da Ocorrência A será dada por:

$$\mathrm{Q}(A) = \frac{|A|}{|S|}$$

Que é análogo a probabilidade de eventos de A. Com o intervalo de resultados $0 \leq \mathrm{Q}(A) \leq 1$.

Assim, o resultado desta equação é a medida de Qualidade da Ocorrência, com 0 representando o valor mínimo e 1 representando o valor máximo.

No caso de um conjunto vazio $\emptyset = \{\ \}$ claramente sua cardinalidade é $|\emptyset| = 0$.

Uma Ocorrência com Qualidade igual a 0 representa que esta Ocorrência não está presente ou não foi cumprida, analogamente uma Ocorrência com Qualidade igual a 1 representa que os requisitos de segurança da Ocorrência foram cumpridos em sua totalidade.

Conforme seu papel dentro do Espaço Métrico a Ocorrência pode ser classificada como positiva A ou negativa B.

As Ocorrências serão classificadas como positivas A quando o aumento da sua probabilidade implica em diminuição dos riscos e problemas de segurança. Ou seja, ela é positiva quando contribui para o aumento da segurança. As Ocorrências cujo aumento da sua probabilidade não colabora para o aumento da segurança são classificadas como Ocorrências negativas B. O cálculo da Qualidade destas ocorrências será mostrado no próximo exemplo.

Cada métrica será mensurada por um valor numérico chamado de Qualidade da Métrica $Q(M)$. Utilizam-se dois métodos para obter $Q(M)$ em função de suas Ocorrências. Quanto maior o número de Ocorrências maior será a fidelidade da Qualidade da Métrica.

Através do próximo exemplo vamos demonstrar a aplicação do primeiro método adotado para o cálculo da Qualidade de uma Métrica.

2.6.2 Método 1

Espaço Métrico sem interação.

2.6.2.1 Exemplo de métrica 2

Dada a Métrica M =.*{Controle de segurança interna de servidores}*

Para esta Métrica o Espaço Métrico será:

S =*{conjunto de servidores da rede}*

As Ocorrências serão:

Positivas:

A_1 =*{Servidores que executam backup local a cada 24h}*

A_2 =*{Servidores que executam backup remoto}*

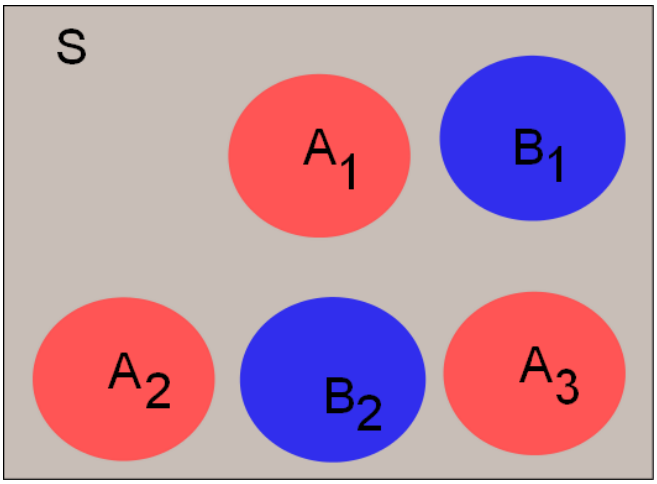
A_3 = *{servidores com acesso restrito. Somente administradores da rede têm acesso}*

Negativas:

B_1 =*{Servidores que não executam backup}*

B_2 =*{Servidores com firewall desatualizado}*

Figura 10 – Espaço métrico da métrica M



Fonte: Nascimento (2013)

Onde os valores do Espaço Métrico e das Ocorrências serão:

$|S| = 15$ *servidores.*

$|A_1| = 8$ *servidores.*

$|A_2| = 1$ *servidor.*

$|A_3| = 5$ *servidores.*

$|B_1| = 2$ *servidores.*

$|B_2| = 15$ *servidores.*

$\mathrm{Q(M)}$ será dada pela média aritmética da Qualidade das Ocorrências.

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Onde,

$Q(M)^+ =$ *Média da Qualidade dos componentes positivos.*

$$Q(M)^+ = \frac{Q(A_1) + Q(A_2) + Q(A_3)}{3}$$

Com:

$$Q(A_1) = \frac{|A_1|}{|S|} = \frac{8}{15} = 0{,}533$$

$$Q(A_2) = \frac{|A_2|}{|S|} = \frac{1}{15} = 0{,}066$$

$$Q(A_3) = \frac{|A_3|}{|S|} = \frac{5}{15} = 0{,}333$$

Assim, temos:

$$Q(M)^+ = \frac{Q(A_1) + Q(A_2) + Q(A_3)}{3} = \frac{0{,}533 + 0{,}066 + 0{,}333}{3} = 0{,}310$$

$Q(M)^- =$ *Média da Qualidade dos componentes negativos*

$$Q(M)^- = \frac{Q(B_1) + Q(B_2)}{2}$$

Como a Qualidade da Métrica indica de modo quantitativo o seu nível de segurança com valores entre 0 e 1, indicando respectivamente baixa e alta segurança, vamos acrescentar 1 complementar à equação da Qualidade da Ocorrência mantendo desta forma a coerência dos resultados da equação:

$$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right] = \left[1 - \frac{2}{15}\right] = [1 - 0{,}133] = 0{,}867$$

$$Q(B_2) = \left[1 - \frac{|B_2|}{|S|}\right] = \left[1 - \frac{15}{15}\right] = [1 - 1{,}000] = 0$$

Assim, temos:

$$Q(M)^- = \frac{Q(B_1) + Q(B_2)}{2} = \frac{0{,}867 + 0}{2} = 0{,}433$$

Portanto a Qualidade final da métrica será:

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2} = \frac{0{,}310 + 0{,}433}{2} = 0{,}3715$$

Logo, este valor para Qualidade da Métrica aponta que devem ser revistos os mecanismos de segurança. Deve-se buscar meios de aumentar o número de

servidores que executam backup local a cada 24h, que executam backup remoto e de servidores com acesso restrito. Pois a implementação de Ocorrências consideradas positivas deve ser expandida e as consideradas negativas minimizadas.

Salientamos que durante o desenvolvimento de uma métrica, quanto maior o número de Ocorrências que puderem ser medidas, melhor será a precisão no cálculo da Qualidade da Métrica.

No primeiro método utilizado para o cálculo da Qualidade de uma Métrica não foram consideradas as interações entre as Ocorrências do Espaço Métrico. Como a existência destas interações é muito provável numa situação real, utiliza-se nestes casos um outro método onde estas interações são consideradas. Estas interações colaboram para uma maior fidelidade nos resultados do mesmo modo que no aumento do número de Ocorrências no Espaço Métrico como já constatado no método 1.

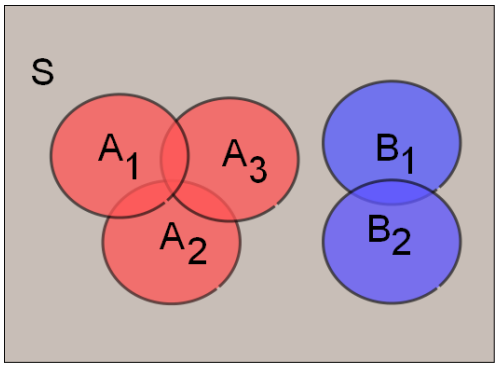
2.6.3 Método 2

Espaço Métrico com interação.

2.6.3.1 Exemplo de métrica 3

A seguir, retoma-se o Exemplo de métrica 2. Mas neste caso, consideram-se as seguintes interações entre as ocorrências do exemplo de métrica 2, conforme a figura 11.

Figura 11 – Métrica 2 com interação



Fonte: Nascimento (2013)

Novamente temos o caso de 03 Ocorrências positivas A_1, A_2, A_3 de um espaço métrico S. Para minimizar a carga nas expressões, consideram-se as cardinalidades $a_1 = |A_1|, a_2 = |A_2|, a_3 = |A_3|$,

Considerando as interações entre as ocorrências como:

$a_{12} = |A_1 \cap A_2|,\ a_{13} = |A_1 \cap A_3|,\ a_{23} = |A_2 \cap A_3|,\ a_{123} = |A_1 \cap A_2 \cap A_3|,$

e

$s = |S|$.

Então a equação para a medida de Qualidade das Ocorrências positivas $Q(M)^+$ é aprimorada com o acréscimo de pesos diferenciados para as interações entre ocorrências utilizando a média ponderada de acordo com o número de interações entre as ocorrências e o conceito de Combinação Simples da Teoria Combinatória. Para uma interação utiliza-se peso 1, para duas peso 2 e assim por diante. Aplicamos este mesmo princípio para as Ocorrências negativas.

$$Q(M)^+ = \frac{3a_{123} + 2a_{12} + 2a_{13} + 2a_{23} + a_1 + a_2 + a_3}{s\left(3C(3,3) + 2C(3,2) + C(3,1)\right)}$$

$$=$$

$$\frac{3a_{123} + 2a_{12} + 2a_{13} + 2a_{23} + a_1 + a_2 + a_3}{12s}$$

Considerando os dados vistos anteriormente para este exemplo e sendo definidos:

$a_{12} = 1$

$a_{13} = 2$

$a_{23} = 1$

$a_{123} = 0$

Substituindo os valores atribuídos teremos a Qualidade das Ocorrências positivas:

$$Q(M)^{+} = \frac{3 * 0 + 2 * 1 + 2 * 2 + 2 * 1 + 8 + 1 + 5}{12 * 15} = 0{,}122$$

Para o caso das duas ocorrências negativas B_1, B_2, com

$b_1 = |B_1|, b_2 = |B_2|, b_{12} = |B_1 \cap B_2|$

Com

$b_{12} = 2$

$$Q(M)^{-} = 1 - \frac{2b_{12} + b_1 + b_2}{s\left(2C(2,2) + C(2,1)\right)} = 1 - \frac{2b_{12} + b_1 + b_2}{4s}$$

$$Q(M)^{-} = 1 - \frac{2 * 2 + 2 + 15}{4 * 15} = 0{,}650$$

Portanto a medida da Qualidade da Métrica que têm 03 Ocorrências positivas e 02 Ocorrências negativas é dada por:

$$Q(M) = \frac{Q(M)^{+} + Q(M)^{-}}{2} = \frac{0{,}122 + 0{,}650}{2} = 0{,}386$$

Comparando os resultados fica evidente que o segundo método é mais rigoroso do que o primeiro.

Tabela 1 - Comparação entre os resultados da aplicação dos dois métodos

	Método 1	Método 2
$Q(M)^+$	0,310	0,122
$Q(M)^-$	0,433	0,650
$Q(M)$	0,371	0,386

Fonte: Nascimento (2013)

No método 1 o mesmo exemplo teve uma $Q(M)^+ = 0{,}31$ enquanto que no método, 2 $Q(M)^+ = 0{,}122$.

Pode-se dizer que o método 2 diminui a negatividade dos resultados para as Ocorrências negativas, portanto aumenta a positividade.

Pode-se explicar isso no exemplo:

$B_1 = 2, b_2 = 15, b_{12} = 2, s = 15$

A negatividade no método 1 é:

$\frac{b1 + b2}{2s} = 0{,}5666$

(mais negativo) enquanto que a negatividade pelo método 2 é:

$\frac{2 * b_{12} + b_1 + b_2}{4 * s} = 0{,}35$

(menos negativo). Portanto mais negativo implica menos positivo, assim:

$Q(M)^- = 1 - 0{,}5666 = 0{,}4334\ (método\ 1)$

$Q(M)^- = 1 - 0{,}35 = 0{,}65\ (método\ 2)$

Assim, conclui-se que o método 2 é mais rigoroso e portanto mais preciso em termos de medição de riscos do que o método 1.

Em uma situação real estes resultados podem indicar, a um administrador ou grupo de administradores de uma determinada rede, que a prioridade de melhorias não estaria sobre as Ocorrências negativas e sim em melhorar as Ocorrências positivas. Como, por exemplo, ampliar o número de Servidores que executam backup remoto e também o número de servidores que tem acesso restrito.

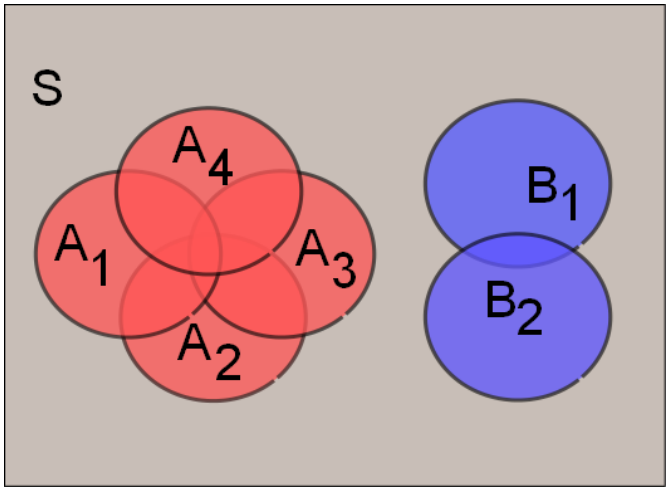
O objetivo da gestão desta rede através destes Controles deve ser sempre buscar e manter um valor que tenda a 1 para a Qualidade das Métricas.

No próximo exemplo, aplica-se este método em um espaço métrico diferente, constituído por 6 Ocorrências.

2.6.3.2 Exemplo de métrica 4

Dada a Métrica: Controle de acesso a informações confidenciais armazenadas em estações de trabalho. O Espaço Métrico S é definido como o número total de estações de trabalho que armazenam informação confidencial.

Figura 12 – Exemplo de métrica 4



Fonte: Nascimento (2013)

As Ocorrências serão classificadas da seguinte forma:

Ocorrências Positivas:

A_1 =*{Estações de trabalho que utilizam software de criptografia}*

A_2 =*{Estações de trabalho que utilizam autenticação de usuário}*

A_3 =*{Estações que executam backup diário}*

A_4 =*{Estações com CPU lacrado físicamente}*

Ocorrência negativa:

B_1 =*{Estações que armazenam informação confidencial e também são servidores web}*

B_2 ={*Estações de trabalho com antivírus freeware*[5]}

Onde os valores do Espaço Métrico e das Ocorrências serão:

$|S| = 20$ *Estações de trabalho.*

$|A_1| = 10$ *Estações de trabalho.*

$|A_2| = 18$ *Estações de trabalho.*

$|A_3| = 5$ *Estações de trabalho.*

$|A_4| = 8$ *Estações de trabalho.*

$|B_1| = 5$ *Estações de trabalho.*

$|B_2| = 3$ *Estações de trabalho.*

Para o caso de 04 ocorrências positivas A_1, A_2, A_3, A_4 de um espaço métrico S, consida-se:

$a_1 = |A_1|, a_2 = |A_2|, a_3 = |A_3|, a_4 = |A_4|,$

Com $a_{12} = |A_1 \cap A_2|, a_{13} = |A_1 \cap A_3|, a_{14} = |A_1 \cap A_4|, a_{23} = |A_2 \cap A_3|,$

$a_{24} = |A_2 \cap A_4|,$

$a_{34} = |A_3 \cap A_4|, a_{1234} = |A_1 \cap A_2 \cap A_3 \cap A_4|, a_{234} = |A_2 \cap A_3 \cap A_4|$

e $s = |S|$, então a medida de qualidade$M(Q)^+$ é dada por

$$Q(M)^+ = \frac{4a_{1234}+3a_{123}+3a_{234}+2a_{12}+2a_{13}+2a_{14}+2a_{23}+2a_{24}+2a_{34}+a_1+a_2+a_3+a_4}{s\left(4C(4,4)+3C(4,3)+2C(4,2)+C(4,1)\right)}$$

$$= \frac{4a_{1234}+3a_{123}+3a_{234}+2a_{12}+2a_{13}+2a_{14}+2a_{23}+2a_{24}+2a_{34}+a_1+a_2+a_3+a_4}{32s}$$

Substituindo os valores atribuídos:

$a_{12} = 8$ *Estações de trabalho*

$a_{13} = 4$ *Estações de trabalho*

$a_{14} = 7$ *Estações de trabalho*

$a_{23} = 4$ *Estações de trabalho*

$a_{24} = 6$ *Estações de trabalho*

$a_{34} = 3$ *Estações de trabalho*

$a_{123} = 4$ *Estações de trabalho*

[5] Programa de computador cuja utilização não implica o pagamento de licenças.

$a_{234} = 2$ *Estações de trabalho*

$a_{1234} = 3$ *Estações de trabalho*

A equação fica:

$$Q(M)^+ = \frac{4*3+3*4+3*2+2*8+2*4+2*7+2*4+2*6+2*3+10+18+5+8}{32*20}$$

$$=$$

$$Q(M)^+ = 0{,}210$$

Para o caso das duas ocorrências negativas B_1, B_2, com:

$b_1 = |B_1|$,

$b_2 = |B_2|$,

$b_{12} = |B_1 \cap B_2|$

Considerando:

$b_{12} = 2\ Estações\ de\ trabalho$

$$M(Q)^- = 1 - \frac{2b_{12}+b_1+b_2}{s\left(2C(2,2)+C(2,1)\right)} = 1 - \frac{2b_{12}+b_1+b_2}{s(4)}$$

$$M(Q)^- = 1 - \frac{2*2+5+3}{s*(4)} = 1 - \frac{12}{20*4} = 0{,}85$$

Portanto a medida da Qualidade da Métrica é dada por;

$$M(Q) = \frac{M(Q)^+ + M(Q)^-}{2}$$

$$M(Q) = \frac{0{,}232+0{,}85}{2} = 0{,}530$$

Observa-se que a Qualidade da Ocorrência negativa teve um valor significativamente alto, ou seja, representa que a segurança está em um nível que tende ao ideal, tende a 1. Isto se deve ao fato do número de ocorrências negativas

ser proporcionalmente menor. Já a Qualidade das Ocorrências positivas está relativamente baixa, pois está mais próxima de 0 do que de 1.

Generalizando:

Portanto, para o caso geral de uma métrica com n ocorrências positivas $A_1, A_2, \dots, A_n$ e m ocorrências negativas $B_1, B_2, \dots, B_m$ a Qualidade da Métrica é calculada por:

$$Q(M)^+ = \frac{na_{12\dots n}+(n-1)(a_{12\dots n-1}+\cdots+a_{23\dots n})+\cdots+2(a_{12}+\cdots+a_{n-1,n})+(a_1+a_2+\cdots+a_n)}{s[nC(n,n)+(n-1)C(n,n-1)+\cdots+2C(n,2)+C(n,1)]}$$

$$Q(M)^- = 1 - \frac{mb_{12\dots m}+(m-1)(b_{12\dots m-1}+\cdots+b_{23\dots m})+\cdots+2(b_{12}+\cdots+b_{m-1,m})+(b_1+b_2+\cdots+b_m)}{s[mC(m,m)+(m-1)C(m,m-1)+\cdots+2C(m,2)+C(m,1)]}$$

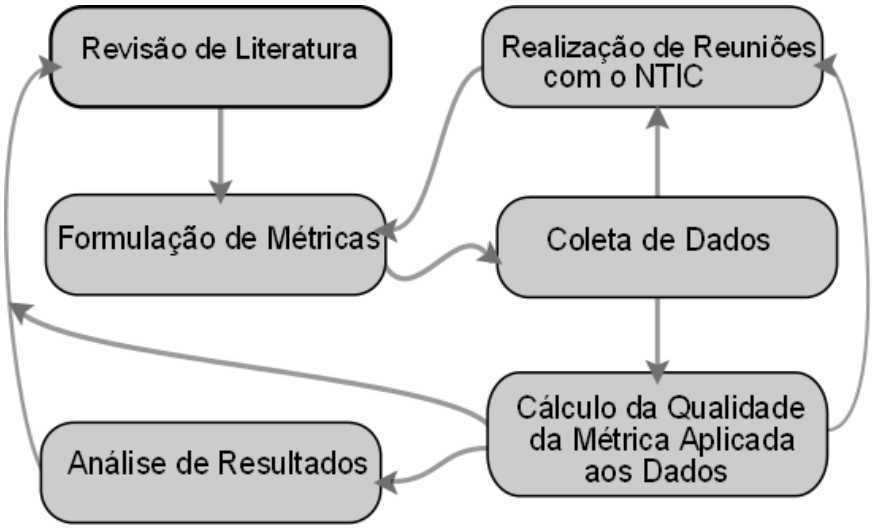
Com a Qualidade da Métrica sendo calculada pela equação:

$$Q(M) = \frac{M(Q)^+ + M(Q)^-}{2}$$

2.7 Metodologia

A metodologia consistiu na revisão de literatura da área para o levantamento de métricas adequadas para uma rede do porte da UNIPAMPA e do Método matemático para seu cálculo; na realização de reuniões presenciais e webconferências com a equipe do NTIC responsável pela rede da UNIPAMPA; na discussão da viabilidade de registro; na coleta de dados; na aplicação dos Métodos matemáticos escolhidos; na análise dos resultados; na apresentação das análises e conclusões; na proposição de ações futuras. A metodologia desenvolvida é apresentada detalhadamente a seguir.

Figura 13 – Metodologia



Fonte: Nascimento (2013)

2.7.1 Revisão de literatura

Realizou-se uma ampla revisão inicial da literatura existente ao respeito de métricas aplicadas a redes de computadores. Conforme a necessidade foram feitas novas consultas à literatura. Isto aconteceu depois do cálculo da qualidade das métricas ou da analise de resultados.

2.7.2 Realização de reuniões com o NTIC

Foram realizadas reuniões iniciais com os responsáveis pela rede da UNIPAMPA expondo a eles a relevância do estudo de caso e a necessidade de obtenção de alguns grupos de dados. Foi manifestado por parte deles, que alguns dados não poderiam estar disponíveis por serem de caráter sigiloso.

Conforme o andamento do processo foram realizadas outras reuniões, especialmente depois de algumas ações de coleta de dados e cálculo de qualidade das métricas. Estas reuniões posteriores foram realizadas com o intuito de melhoria da qualidade dos dados.

2.7.3 Formulação de métricas

Depois da revisão de literatura e realização de reuniões com o pessoal do NTIC, foi elaborada a proposta do conjunto de métricas que faz jus ao titulo desta dissertação. Esta proposta não foi caracterizada somente com a revisão de literatura e reuniões com o pessoal do NTIC. Esta proposta foi evoluindo conforme a dinâmica da coleta de dados, calculo de qualidade das métricas e analise de resultados. Inclusive consideramos que a forma inicial desta proposta deve evoluir, fato que chamamos de trabalhos futuros.

2.7.4 Cálculo da qualidade de métricas aplicada aos dados

Esta ação foi executada com softwares especializados, no caso planilha eletrônica. Nos casos em que os resultados destes cálculos estavam longe do esperado foram feitas revisões da formulação das métricas assim como na coleta de dados que implicou, em alguns casos, novas reuniões com o pessoal do NTIC.

2.7.5 Análise de resultados

Os valores dos resultados das Qualidades das Métricas devem estar compreendidos entre 0 e 1. Métricas com Qualidade tendendo a zero devem ser cuidadosamente estudadas, pois indicam a existência de falhas na segurança. Métricas com valores de Qualidade tendendo a 1 mostram que o controle está funcionando e cumprindo bem seus objetivos.

A partir da análise dos resultados pode-se detectar os problemas ou falhas de segurança em determinado serviço ou produto.

Neste momento, devem-se definir as prioridades nas ações para solucionar os problemas e melhorar a qualidade de determinada Métrica ou Ocorrência. Além da revisão da política interna de TI, pode ser necessário o desenvolvimento de novas Métricas ou Ocorrências ou até mesmo de um novo método.

3 ESTUDO DE CASO: A REDE DA UNIPAMPA

A Universidade Federal do Pampa (UNIPAMPA) foi criada pela Lei 11.640 de 11 de janeiro de 2008, como "Fundação Universidade Federal do Pampa", de natureza pública, com sede e foro na cidade de Bagé, no Estado do Rio Grande do Sul. É dotada de autonomia didático-científica, administrativa e de gestão financeira e patrimonial.

A UNIPAMPA é uma instituição federal de educação superior multicampi, com os campi localizados em Alegrete, Bagé, Caçapava do Sul, Dom Pedrito, Itaqui, Jaguarão, Santana do Livramento, São Borja, São Gabriel e Uruguaiana.

Figura 14 – Mapa de distribuição dos Campi da UNIPAMPA

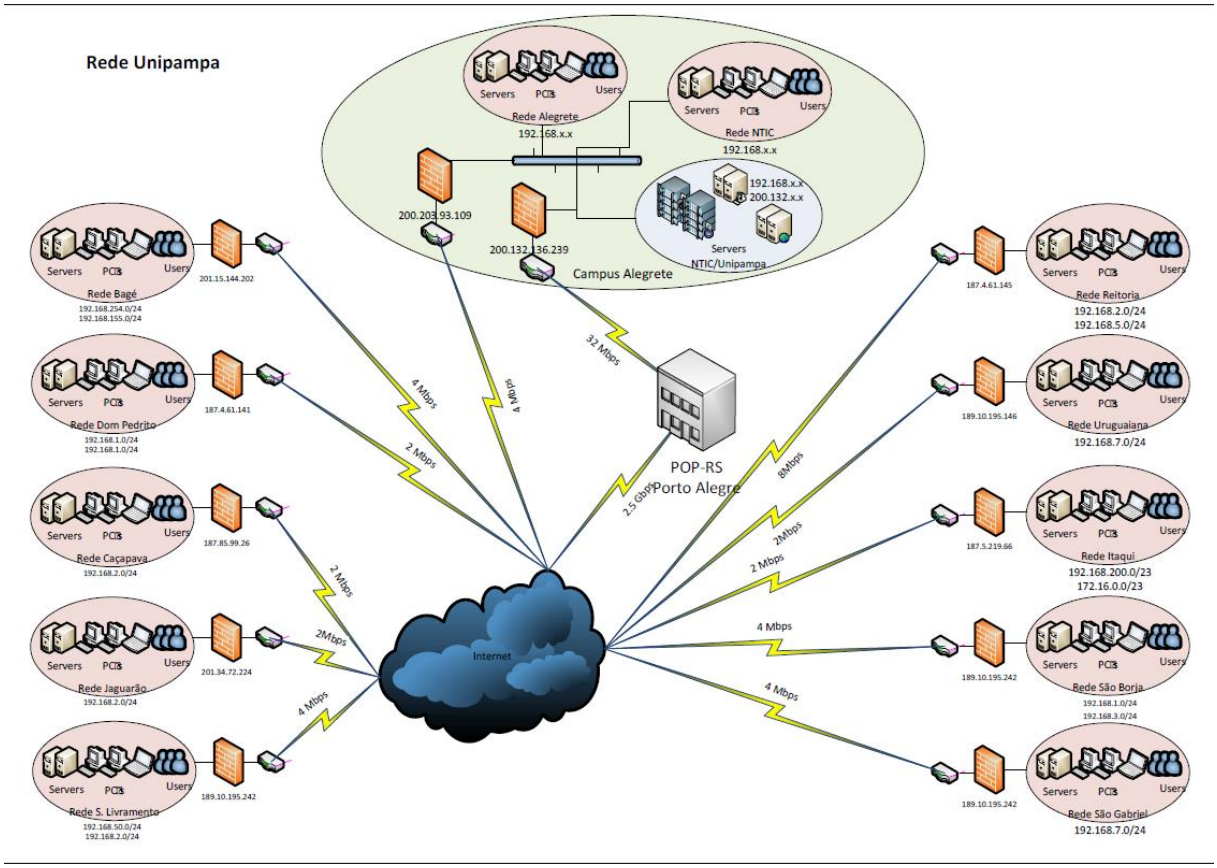
Fonte: Universidade Federal do Pampa

Por se tratar de uma única universidade, embora estruturada em vários espaços, não há, a rigor, uma ordem de importância para qualquer um dos campi.

Um fator que aumenta a dificuldade na administração, em especial da rede de computadores é o fato da universidade ser constituída por várias unidades com centenas de quilômetros de distância.

Cada unidade possui sua conexão independente para a internet, suas regras de firewall e administração local é realizada pelos técnicos de cada unidade. Também há falta de estatísticas sobre os incidentes já ocorridos, já que não havia (até 2010) uma administração comum, aplicação de regras globais e armazenamento de logs centralizados (DELLA FLORA, 2010).

Figura 15 – Rede da Unipampa em 2010



Fonte: Della Flora (2010)

3.1 Campus Alegrete

Este campus atualmente possui 7 cursos de graduação: Ciência Da Computação, Engenharia Agrícola, Engenharia Civil, Engenharia de Software, Engenharia de Telecomunicações, Engenharia Elétrica, Engenharia Mecânica e 5 cursos de Pós-Graduação: Especialização em Engenharia Econômica, Especialização em Praticas e Ensino de Física, Especialização em Tecnologia no Ensino da Matemática, Mestrado em Engenharia Elétrica, Mestrado em Engenharias.

A rede do campus Alegrete possui duas conexões para a internet, sendo um link de 34 Megabits que conecta a universidade à Rede IPÊ e outro de 4 Megabits contratado pela universidade (DELLA FLORA, 2010).

Apesar dos benefícios proporcionados, devemos ficar atentos aos problemas relacionados à segurança da informação neste tipo de rede. A instituição possui uma

quantidade elevada de usuários. O caráter multisserviço leva à manipulação de dados sigilosos da instituição e dos demais usuários.

São necessários, então, métodos específicos para o tratamento da segurança da informação nesta rede.

A UNIPAMPA possui o Núcleo de Tecnologia da Informação e Comunicação (NTIC), que é um órgão suplementar da Reitoria da Universidade Federal do Pampa, com estrutura prevista na Portaria UNIPAMPA nº 745 de 13 de abril de 2010. Tem por objetivo criar e manter as condições para o funcionamento sistêmico das atividades ligadas à tecnologia da informação e comunicação na Universidade, a fim de dar suporte ao desenvolvimento do ensino, pesquisa, extensão, gestão e serviços à comunidade, de acordo com as diretrizes da Universidade.

Tabela 2 - Mapeamento de serviços do NTIC

Serviço	Link de Acesso
Certificados Digitais (Tokens)	http://www.ntic.unipampa.edu.br/tokens
Gestão de Atas de Colação	http://www.unipampa.edu.br/sga
Gestão de Certificados Eletrônicos	http://www.ntic.unipampa.edu.br/sgce/
Inscrições em concursos	http://www.unipampa.edu.br/concursos
Licitações OnLine	http://www.unipampa.edu.br/licitacoes
Moodle	http://moodle.unipampa.edu.br
Painel de suporte	http://www.unipampa.edu.br/suporte
Pampatube	http://pampatube.unipampa.edu.br
SIE (Sistema de Informações de Ensino)	http://www.ntic.unipampa.edu.br/sie
SisRel	http://sisrel.unipampa.edu.br/academico/
Sistema de Chamados	http://chamados.unipampa.edu.br
Sistema de Serviços Gerais	http://ssg.unipampa.edu.br
Videoconferências	http://www.ntic.unipampa.edu.br/vconf
VoIP	http://www.ntic.unipampa.edu.br/voip
Webconferências	http://www.ntic.unipampa.edu.br/vconf

Fonte: Núcleo de Tecnologia da Informação e Comunicação (2013)

Dentre os serviços presentes na tabela 2 podemos destacar o SIE, Sistema de Informações para o Ensino, é um Projeto apoiado pela Secretaria de Ensino Superior (SESu) do Ministério da Educação (MEC). Trata-se de um software para gestão integrada no qual praticamente todas as atividades de uma Instituição de

Ensino Superior são desenvolvidas e acompanhadas por ele. O Sistema permite a gestão dos seguintes módulos integrados:

- Acadêmico (Graduação e Pós-Graduação)
- Recursos Humanos (Cadastro e Gestão)
- Orçamentários (Planejamento e Execução)
- Serviços Gerais (Frota, Espaço Físico, Almoxarifado, Patrimônio, Licitação e Compras)
- Biblioteca
- Legislação
- Processo Seletivo
- Central de Atendimento
- Protocolo e Módulos Administrativos

O SIE é acessível a partir de qualquer microcomputador instalado na rede da Universidade e possui um sistema de cadastro de usuários que fornece permissões de acesso aos módulos e funcionalidades customizadas.

3.2 Métricas adequadas para aplicação na rede da Unipampa

Abaixo apresentam-se as métricas de segurança escolhidas a partir das discussões conjuntas com a equipe do NTIC responsável pela segurança da rede da UNIPAMPA.

Lembra-se que a aplicação de métricas para a segurança da informação na rede da UNIPAMPA é um trabalho pioneiro, pois esta é uma instituição relativamente jovem, fundada em 2006. Até o início deste trabalho em 2011 as informações e dados coletados não eram analisados de modo conjunto e sistematizado como nessa proposta, sendo essa a motivação para o desenvolvimento deste trabalho.

Abaixo estão relacionadas as métricas escolhidas além das apresentadas inicialmente:

- Métrica M_1: “Controle das contas de usuários”;
- Métrica M_2: “Controle da proliferação de vírus”;
- Métrica M_3: “Controle de segurança dos pontos de acesso de uma rede Wi-Fi”;

- Métrica M_4: “Controle de utilização da banda de internet”;
- Métrica M_5: “Controle de segmentação da rede”;
- Métrica M_6: “Controle de segurança interna de servidores”;
- Métrica M_7: “Controle de acesso a informações confidenciais armazenadas em estações de trabalho”;
- Métrica M_8: “Controle de atendimento de chamados para o SIE”;
- Métrica M_9: “Controle de atendimentos do Suporte Técnico Alegrete”;
- Métrica M_{10}: “Controle da utilização do VoIP”.

Dentre outros critérios utilizados para a escolha das métricas, como por exemplo o seu impacto no desempenho da rede ou fatores econômicos, o mais determinante foi a viabilidade técnica para a realização das medidas, pois o NTIC não dispunha até o momento de muitos equipamentos e softwares para medida dos dados e a realização de algumas métricas. E também por questão de segurança algumas informações não podem ser disponibilizadas. Para o registro das ocorrências de cada espaço métrico foi adotada uma frequência mensal.

Desenvolveu-se uma tabela para facilitar a coleta dos dados necessários nas reuniões com a equipe do NTIC. A versão final da tabela está no Anexo A. Nesta tabela estão as respectivas medidas a serem coletadas para cada métrica, a fonte dos dados e o valor para cada mês monitorado. A seguir apresenta-se a tabela 3 como um pequeno extrato desta tabela.

Tabela 3 - Exemplo de tabela desenvolvida para a coleta dos dados.

Métrica	Medida	Software/Fonte dos dados	2012 Janeiro
Controle das contas de usuários	Número total de contas de usuários	RH e Secretaria	1200
	Número total de computadores (Desktops)	AD (Active Directory)	113
	Número total de computadores (Laboratórios)	AD (Active Directory)	125
	Número total de computadores (Notebooks)	AD (Active Directory)	3
	Número total de computadores (Servidores)	AD (Active Directory)	6
	Número de usuários com privilégios de administrador	AD (Active Directory)	247
	Número de computadores utilizando a conta de Administrador como conta de trabalho	AD (Active Directory)	247
Controle da proliferação de vírus	Controle da proliferação de vírus	SEP (Symantec Endpoint Protection)	103
	Número de computadores infectados	SEP (Symantec Endpoint Protection)	9
	Número de computadores com antivírus instalado	SEP (Symantec Endpoint Protection)	98
	Número de computadores com assinaturas de vírus desatualizadas	SEP (Symantec Endpoint Protection)	73
	Número de vírus com alta criticidade	SEP (Symantec Endpoint Protection)	0
	Número de computadores com antispyware instalado	SEP (Symantec Endpoint Protection)	67
	Número de computadores com antispyware com assinaturas atuais	SEP (Symantec Endpoint Protection)	65
	Número de computadores com antivírus e antispyware instalado	SEP (Symantec Endpoint Protection)	67

Fonte: Nascimento (2013)

A baixo apresentamos as Métricas e os procedimentos adotados para o cálculo da sua qualidade.

Métrica M_1: “Controle das contas dos usuários”

Para esta métrica temos o espaço métrico: $S = \{contas\ de\ usuários\ da\ rede\}$ e temos uma única ocorrência positiva:

$A_1 = \{contas\ de\ usuários\ com\ senhas\ boas\} \subset S.$

Ocorrências negativas:

B_1=*{contas de usuários que não acatam normas de segurança}*$\subset S$.

B_2=*{contas de usuários que têm privilégios de administrador e utilizam esta* conta como conta de trabalho}$\subset S$.

A qualidade das ocorrências pelo método 1:

$$Q(A_1) = \frac{|A_1|}{|s|}$$

$$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right]$$

$$Q(B_2) = \left[1 - \frac{|B_2|}{|S|}\right]$$

Qualidade das ocorrências negativas:

$$Q(M)^- = \frac{Q(B_1) + Q(B_2)}{2}$$

Enquanto que a qualidade das ocorrências positivas é:

$$Q(M)^+ = Q(A_1)$$

Portanto a qualidade da métrica será:

$$Q(M) = \left(\frac{Q(M)^- + Q(M)^+}{2}\right)$$

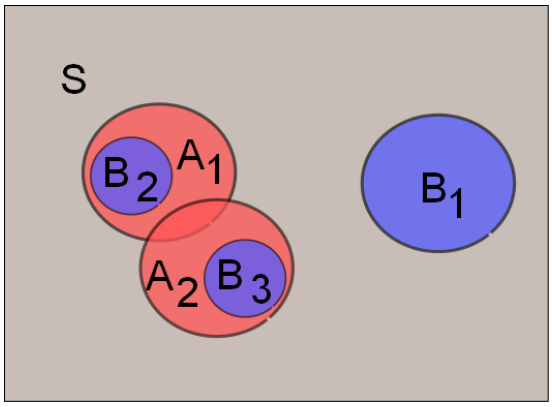
Métrica M_2: “Controle da proliferação de vírus”

Para esta métrica temos o espaço métrico: S={computadores da rede} e temos as seguintes ocorrências positivas:

A_1=*{Computadores com antivírus instalado}*

A_2=*{Computadores com antispyware instalado}*

Figura 16 – Métrica 2



Fonte: Nascimento (2013)

$A_1 \cap A_2$={*Computadores com antivírus e antispyware instalado*}

As Ocorrências negativas:

B_1={*Computadores infectados*}

B_2={*Computadores com antivírus desatualizado*};

B_3={*Computadores com antispyware desatualizado*};

$B_2 \cap B_3$={*Computadores com antivírus e antispyware desatualizados*};

A qualidade da métrica pelo método 1:

$Q(M)$ será dada pela média aritmética da Qualidade das Ocorrências.

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Onde a qualidade das ocorrências positivas é:

$$Q(M)^+ = \frac{Q(A_1) + Q(A_2)}{2}$$

Enquanto que a qualidade das ocorrências negativas é:

$$Q(M)^- = \frac{Q(B_1) + Q(B_2) + Q(B_3)}{3}$$

Onde

$$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right]$$

Como B_2 e B_3 são subconjuntos de A_1 e A_2 respectivamente então:

$$Q(B_2) = \left[1 - \frac{|B_2|}{|A_1|}\right]$$

,

$$Q(B_3) = \left[1 - \frac{|B_3|}{|A_2|}\right]$$

.

A qualidade da métrica pelo método 2:

A qualidade das ocorrências positivas será:

$$Q(M)^+ = \frac{2a_{12} + a_1 + a_2}{s\big(2C(2,2) + C(2,1)\big)} = \frac{2a_{12} + a_1 + a_2}{4s}$$

Enquanto que a qualidade das ocorrências negativas será:

$$Q(M)^- = \frac{\left(1 - \frac{b_1}{s}\right) + \left(1 - \frac{2b_{23} + b_3 + b_2}{s\big(2C(2,2) + C(2,1)\big)}\right)}{2} = \frac{\left(1 - \frac{b_1}{s}\right) + \left(1 - \frac{2b_{23} + b_2 + b_3}{4s}\right)}{2}$$

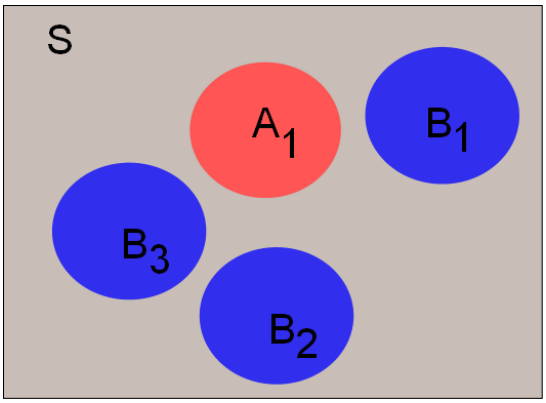
E portanto;

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Métrica M_3: “Controle de segurança dos pontos de acesso de uma rede Wi-Fi”

Para esta métrica temos o Espaço Métrico S={pontos de acesso Wi-Fi}

Figura 17 – Métrica 3



Fonte: Nascimento (2013)

As Ocorrências positivas:

A_1=*{Pontos de acesso com WAP2;}*

As Ocorrências negativas:

B_1=*{Pontos de acesso com o SSID padrão}*

B_2=*{Pontos de acesso com versões desatualizadas de firmware e software}*

B_3=*{Pontos de acesso com autenticação aberta}*

A Qualidade das Ocorrências positivas pelo método 1:

$Q(M)^+ = \frac{Q(A_1)}{s}$, onde $Q(A_1) = \frac{|A_1|}{|S|}$

A qualidade das ocorrências negativas:

$$Q(M)^- = \frac{Q(B_1) + Q(B_2) + Q(B_3)}{3}$$

, onde

$$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right]$$

$$, Q(B_2) = \left[1 - \frac{|B_2|}{|S|}\right], e\, Q(B_3) = \left[1 - \frac{|B_3|}{|S|}\right]$$

E portanto;

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

O método 2 não foi aplicado, pois não ocorreu interação entre as ocorrências.

Métrica M_4: “controle de utilização da banda de internet”

Para esta métrica tem-se o Espaço Métrico $S = S_1 \cup S_2$; onde S_1=*{computadores com acesso direto a internet}*, S_2=*{faixa de banda alocada}*

Não tem-se Ocorrências positivas.

As Ocorrências negativas:

B_1=*{valor médio de banda de utilizada}*

B_2=*{computadores que possuem acesso à Internet};*

Qualidade da métrica pelo método 1

$Q(M)$ será dada pela média aritmética da Qualidade das Ocorrências.

$Q(M) = Q(M)^- = \frac{Q(B_1)+Q(B_2)}{2}$ onde

$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right]$ e $Q(B_2) = \left[1 - \frac{|B_2|}{|S|}\right]$

Não aplicou-se o método 2 pois não ocorreu interseção entre as ocorrências

Métrica M_5: “Controle de segmentação da rede”

Para esta métrica tem-se o Espaço Métrico *S={sub redes}.* Não tem-se Ocorrências positivas. A ocorrência negativa é:

B_1 *={Número de domínios que acessam outros domínios de sub-rede não definidos pela política de segurança interna do NTIC}*

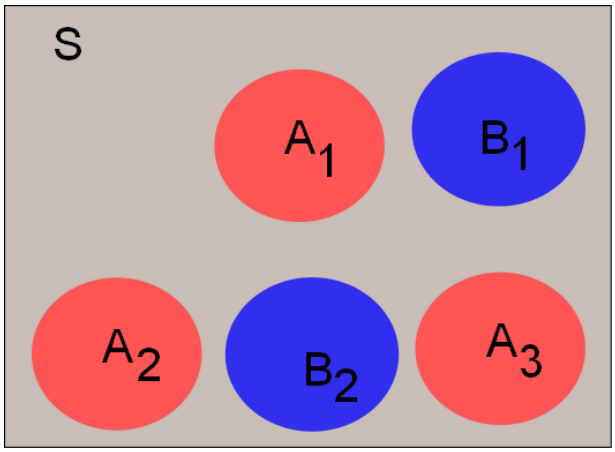
Qualidade da métrica aplicando o método 1

$Q(M)$ será dada pela média aritmética da Qualidade das Ocorrências. $Q(M) = Q(M)^- = Q(B_1)$ onde $Q(B_1) = \left[1 - \frac{|B_1|}{|s|}\right]$

Não aplicou-se o método 2 pois não ocorreu interseção entre as ocorrências.

Métrica M_6: “Controle de segurança interna de servidores”

Figura 18 – Métrica 6



Fonte: Nascimento (2013)

Para esta Métrica o Espaço Métrico será: S={Servidores da rede}

As ocorrências positivas serão:

A_1=*{Servidores que executam backup local a cada 24h}*

A_2=*{Servidores que executam backup remoto}*

A_3=*{servidores com acesso restrito. Somente administradores da rede têm acesso}*

Enquanto que as ocorrências negativas serão:

B_1=*{Servidores que não executam backup}*

B_2=*{Servidores com firewall desatualizado}*

$Q(M)$ será dada pela média aritmética da Qualidade das Ocorrências.

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Onde,

$Q(M)^+ =$ Média da Qualidade dos componentes positivos.

$$Q(M)^+ = \frac{Q(A_1) + Q(A_2) + Q(A_3)}{3}$$

Com:

$$Q(A_1) = \frac{|A_1|}{|S|}$$

,

$$Q(A_2) = \frac{|A_2|}{|S|}$$

e

$$Q(A_3) = \frac{|A_3|}{|S|}$$

.

Assim, tem-se:

$$Q(M)^+ = \frac{Q(A_1) + Q(A_2) + Q(A_3)}{3}$$

$Q(M)^- =$ Média da Qualidade dos componentes negativos

$$Q(M)^- = \frac{Q(B_1) + Q(B_2)}{2}$$

$$Q(B_1) = \left[1 - \frac{|B_1|}{|S|}\right]$$

$$Q(B_2) = \left[1 - \frac{|B_2|}{|S|}\right]$$

Assim, tem-se:

$$Q(M)^- = \frac{Q(B_1) + Q(B_2)}{2} =$$

Portanto a Qualidade final da métrica será:

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Métrica M_7: “Controle de acesso a informações confidenciais armazenadas em estações de trabalho”

O Espaço Métrico é*: S={Estações de trabalho que armazenam informação confidencial}.*

As ocorrências serão classificadas da seguinte forma:

Ocorrências Positivas:

A_1*={Estações de trabalho que utilizam software de criptografia}*

A_2*={Estações de trabalho que utilizam autenticação de usuário}*

A_3=*{Estações que executam backup diário}*

A_4=*{Estações com CPU lacrado fisicamente}*

Ocorrências negativas

B_1=*{Estações que armazenam informação confidencial e também são servidores web}*

B_2 =*{Estações de trabalho com antivírus freeware}*

A qualidade da métrica pelo método 2:

$$Q(M)^+ = \frac{4a_{1234} + 3a_{123} + 3a_{234} + 2a_{12} + 2a_{13} + 2a_{14} + 2a_{23} + 2a_{24} + 2a_{34} + a_1 + a_2 + a_3 + a_4}{32s}$$

Para as ocorrências negativas:

$$Q(M)^- = 1 - \frac{2b_{12} + b_1 + b_2}{s\big(2C(2,2) + C(2,1)\big)} = 1 - \frac{2b_{12} + b_1 + b_2}{s(4)}$$

Qualidade da Métrica é dada por:

$$Q(M) = \frac{Q(M)^+ + Q(M)^-}{2}$$

Métrica M_8: “Controle de atendimento de chamados para o SIE”

O Espaço Métrico é S=*{chamados do SIE}.*

As Ocorrências serão classificadas da seguinte forma:

Ocorrência Positiva:

A_1=*{chamados atendidos/fechados}*

Ocorrência negativa:

Não tem-se ocorrências negativas.

A Qualidade da Ocorrência A_1 será equivalente à Qualidade da Métrica:

$$Q(M) = Q(A_1) = \left(\frac{|A_1|}{|S|}\right)$$

Métrica M_9: “Controle de atendimentos do Suporte Técnico Alegrete”

O Espaço Métrico é S={ chamados abertos para o suporte}. As ocorrências serão classificadas da seguinte forma:

Ocorrência positiva:

A_1=*{chamados atendidos/fechados}*

Ocorrência negativa:

Não tem-se ocorrências negativas.

A qualidade da ocorrência A_1 será equivalente a qualidade da Métrica:

$$Q(M) = Q(A_1) = \left(\frac{|A_1|}{|S|}\right)$$

Métrica M_{10}: “Controle da utilização do VoIP”

O espaço métrico neste caso é $S = S_1 \cup S_2$, onde S_1=*{usuários de VoIP}*, S_2=*{ramais VoIP}.*

As ocorrências positivas:

A_1=*{usuários com senha alfanumérica}*

A_2=*{ramais instalados em softphones*[6]*}*

As ocorrências negativas:

B_1=*{ramais em aparelhos VoIP}*

B_2=*{ramais com autorização para usar DDD e DDI}*

Como existe interseção entre as ocorrências então neste caso é preferível utilizar o método 2.

$a_{12} = |A_1 \cap A_2|$

$$Q(M)^+ = \frac{2a_{12} + a_1 + a_2}{s\big(2C(2,2) + C(2,1)\big)}$$

[6] Software que é utilizado para fazer chamadas utilizando VoIP (Voice over IP) ou ToIP (telefonia IP).

$$Q(M)^{+} = \frac{2a_{12} + a_1 + a_2}{4s}$$

Para as ocorrências negativas:

$b_{12} = |B_1 \cap B_2|$

$$Q(M)^{-} = 1 - \frac{2b_{12} + b_1 + b_2}{s\big(2C(2,2) + C(2,1)\big)} = 1 - \frac{2b_{12} + b_1 + b_2}{4s}$$

Qualidade da Métrica é dada por:

$$Q(M) = \frac{Q(M)^{+} + Q(M)^{-}}{2}$$

3.3 Aplicação das métricas

Uma dificuldade enfrentada no desenvolvimento deste trabalho reside nas peculiaridades das Instituições Públicas de Ensino. Pelo fato deste trabalho ser de natureza acadêmica, e de seus proponentes não fazerem parte da equipe de TI da instituição e sua proposta não ter sua origem em um setor de gestão institucional, ou seja, a proposta de trabalho não teve sua origem do topo para baixo (top-down), teve-se que cumprir diversos trâmites desde janeiro de 2011, até conseguir os primeiros contatos positivos com a equipe de TI, em agosto de 2011, quando iniciou-se a escolha das ocorrências possíveis de serem medidas. Já em agosto a proposta inicial era abranger toda a rede da Unipampa; a intenção era de obter as ocorrências das métricas aplicando-as em todos os campi da Unipampa. Para isso enviou-se um memorando para os diretores de todos os campi, solicitando a colaboração da equipe de TI local e disponibilizou-se uma planilha online onde os dados seriam registrados. Infelizmente este memorando foi ignorado por 90% dos 10 campi. Assim, como conseguiu-se a colaboração da equipe do NTIC optou-se por limitar a abrangência deste trabalho a rede do campus Alegrete, pois o NTIC e duas pró-reitoras da Unipampa são sediadas em Alegrete, o que torna a rede deste campus a maior da Unipampa.

Iniciou-se a aplicação das métricas M_4 e M_2 com uma frequência mensal de medidas a partir de Abril de 2011.

Para a métrica M_4, monitoramento da rede RNP da UNIPAMPA, a ferramenta utilizada para obter os dados de utilização dos links da RNP chama-se Cacti e tem-se acesso através do PoP-RS (Ponto de Presença da RNP no Rio Grande do Sul). A partir dela, os dados do gráfico são importados para um arquivo CSV e a partir deste arquivo calculou-se a média de utilização conforme os horários presentes nos relatórios.

Para a métrica M_2, utilizou-se um software antivírus corporativo (Symantec Endpoint Protection), instalado em uma maquina virtual rodando Windows 2008 server R2; para gerar os relatórios da Contagem de detecções de risco e detecção por domínio.

As métricas M_8, M_9 e M_{10} foram aplicadas no primeiro semestre de 2013 e as demais métricas foram aplicadas no período entre janeiro de 2011 e novembro de 2012. As diferenças entre os períodos de aplicação das métricas se deu basicamente por questões de viabilidade técnica.

A relação de dados fornecidos à nossa equipe encontra-se no Anexo A.

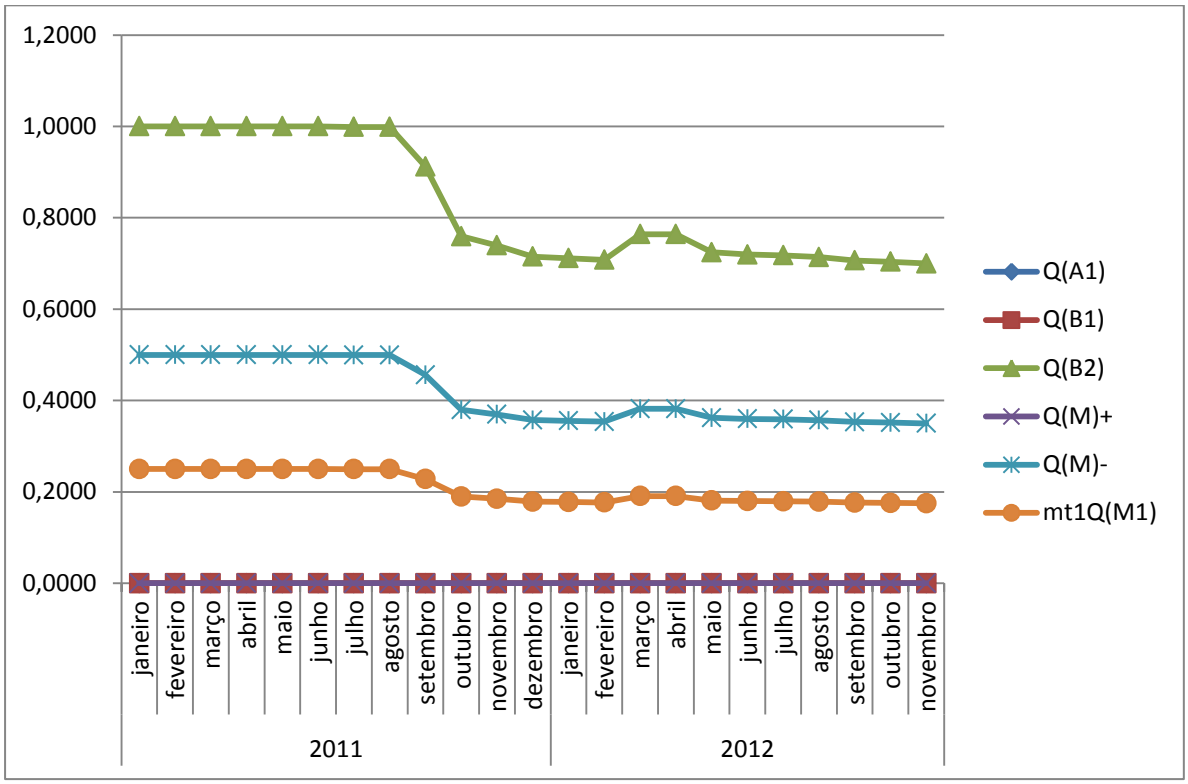
3.4 Análise de Resultados

Para a recepção e processamento dos dados registrados pela equipe do NTIC optou-se pela utilização da planilha eletrônica Microsoft Excel 14.0 (Office 2010) em função de atender as necessidades deste trabalho e ser a planilha eletrônica mais popular, presente na maioria dos computadores, o que facilita a aplicação e/ou aprimoramento desta proposta em qualquer ambiente organizacional e por qualquer equipe.

Métrica M_1: “Controle das contas de usuários”

Aplicando o método 1 obteve-se o gráfico 1.

Gráfico 1 – Resultados da métrica 1



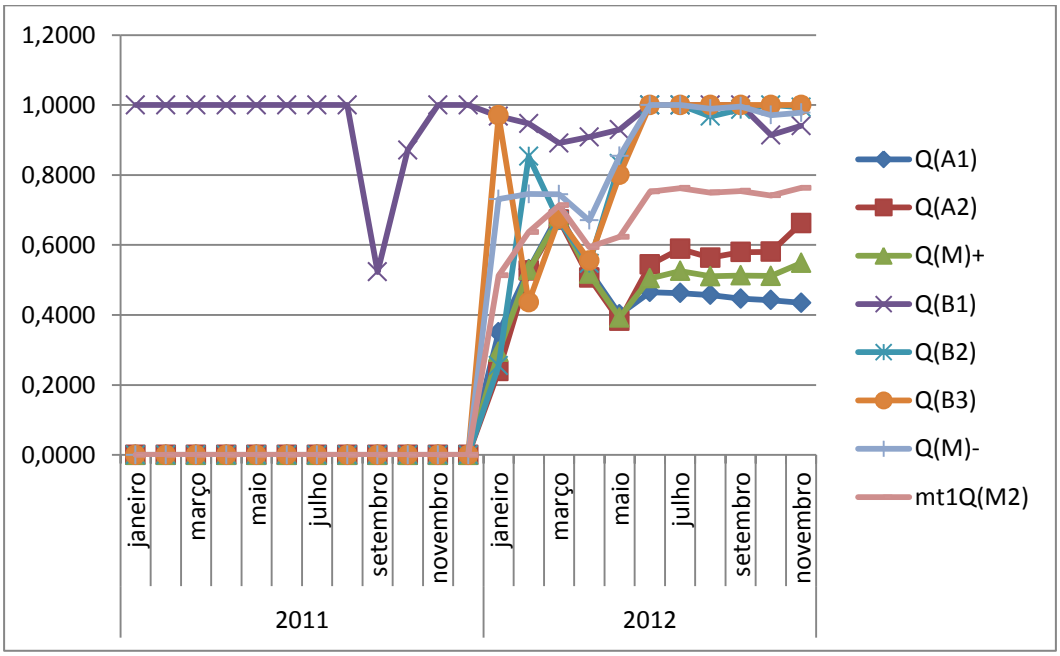
Fonte: Nascimento (2013)

Esta métrica apresenta resultado muito baixo tendendo a zero, pelo fato de, até aquele momento, o NTIC não dispunha de software para avaliar as senhas dos usuários. O desenvolvimento de um projeto para este problema foi proposto pelos autores deste trabalho ao NTIC durante o período de realização do mesmo.

Métrica M_2 : “Controle da proliferação de vírus”

Aplicando o método 1 obteve-se o gráfico 2:

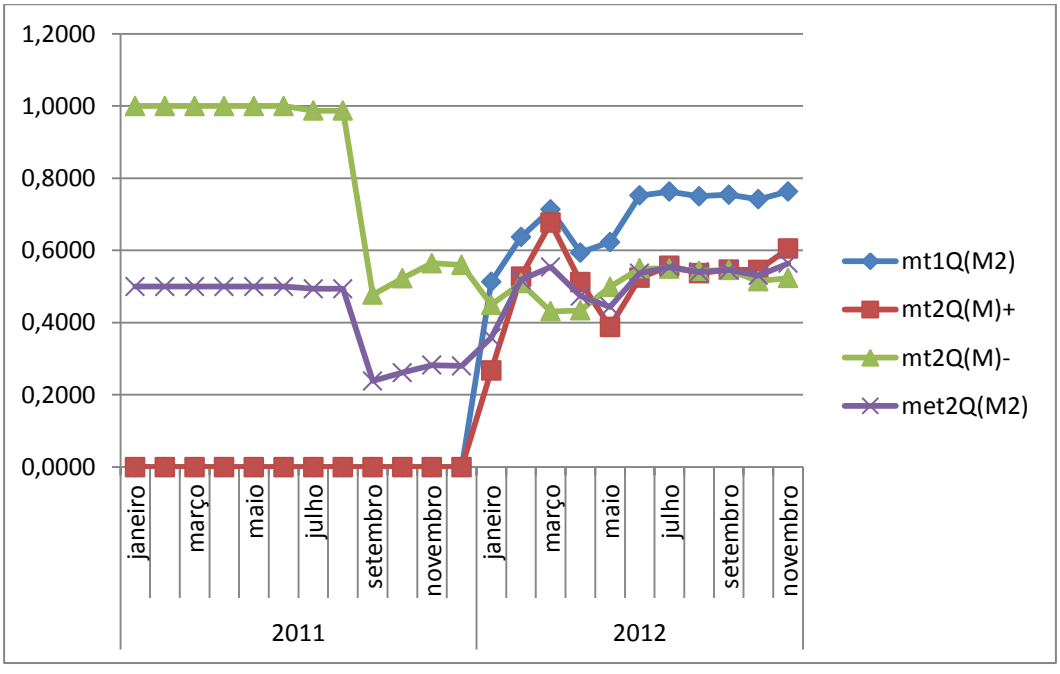
Gráfico 2 – Resultados da métrica 2



Fonte: Nascimento (2013)

No gráfico 3 apresenta-se a comparação entre a aplicação do método 1 e o método 2:

Gráfico 3 – Comparativo de resultados da métrica 2



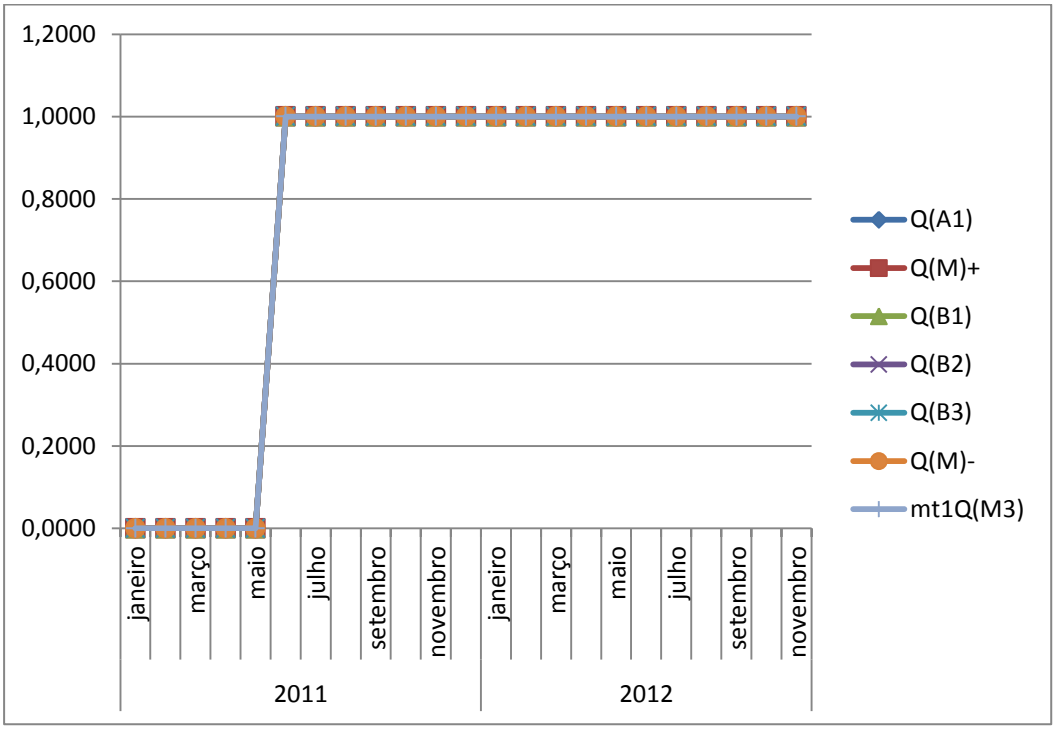
Fonte: Nascimento (2013)

Nesta métrica foi possível comparar a aplicação dos dois métodos em um mesmo espaço métrico. O segundo método mostra-se, como se esperava, mais rigoroso do que o primeiro. Um ponto negativo é que o SEP (Symantec Endpoint Protection), só informa um relatório de infecções dos últimos 03 meses, pois o banco de dados tem um grande crescimento. Muitos dados foram perdidos, pois o banco de dados estava muito grande e teve de ser deletado, sem o conhecimento dos autores, interrompendo a coleta de dados.

Métrica M_3: “Controle de segurança dos pontos de acesso de uma rede Wi-Fi”

Aplicando o método 1 obteve-se o gráfico 1.

Gráfico 4 – Resultado da métrica 3



Fonte: Nascimento (2013)

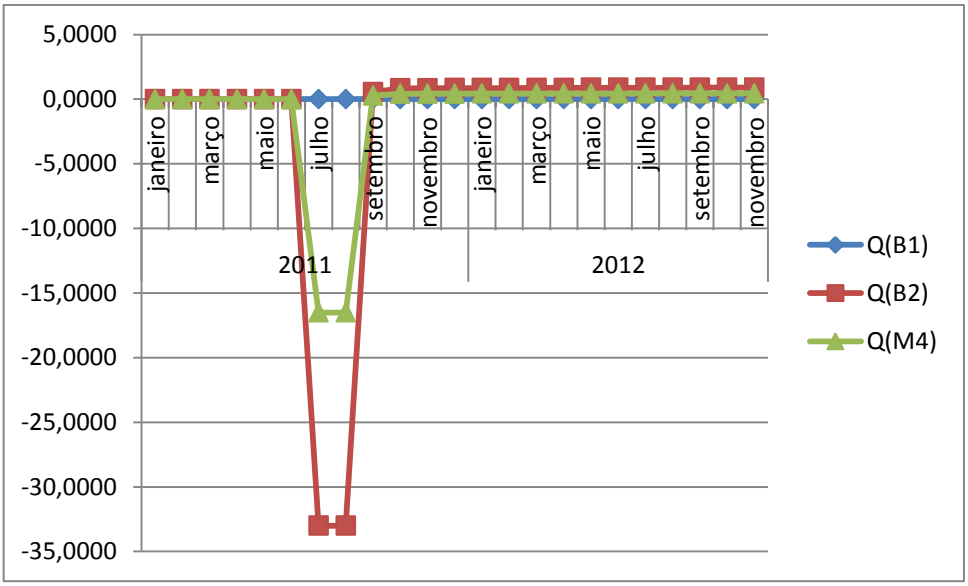
Estes dados somente puderam ser obtidos a partir de 2011 com a reestruturação da rede. Observa-se que o alto índice de qualidade deve-se ao fato dos pontos de acesso não possuírem senha; eles são interligados em um único controlador wireless. Este controlador possui senha definida pelo setor de TI. Cada um dos pontos de acesso fornece os 04 SSID's existentes (UNIPAMPA, UNIPAMPA

VISITANTES, UNIPAMPA ALUNOS E UNIPAMPA VOIP). A autenticação é realizada por WAP-RADIUS.

Métrica M_4: “controle de utilização da banda de internet”

Os valores obtidos para as qualidades estão na planilha do Apêndice A.

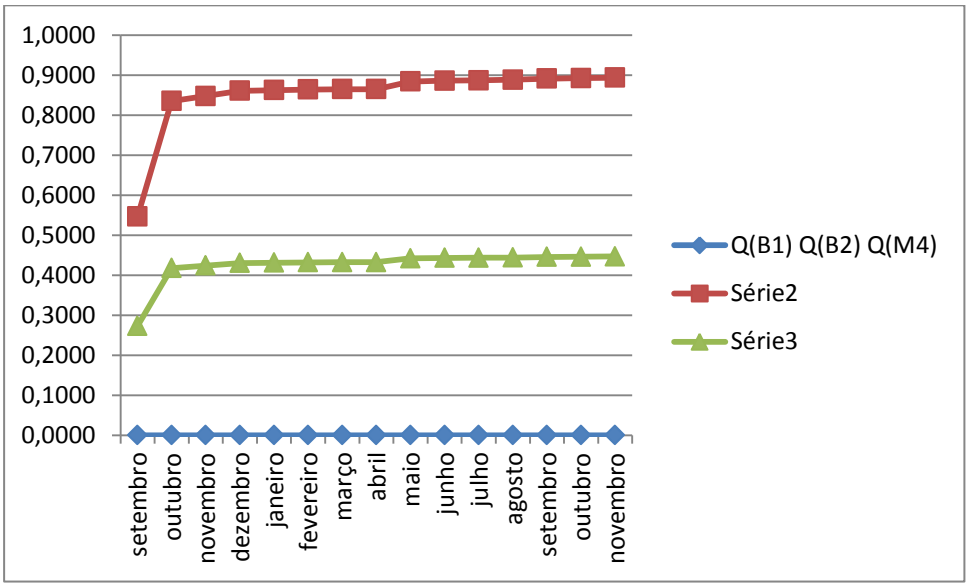
Gráfico 5 – Resultados da métrica 4



Fonte: Nascimento (2013)

O gráfico 6 apresenta os resultados considerando somente os dados significativos:

Gráfico 6 – Resultados da Métrica 4 – somente dados significativos



Fonte: Nascimento (2013)

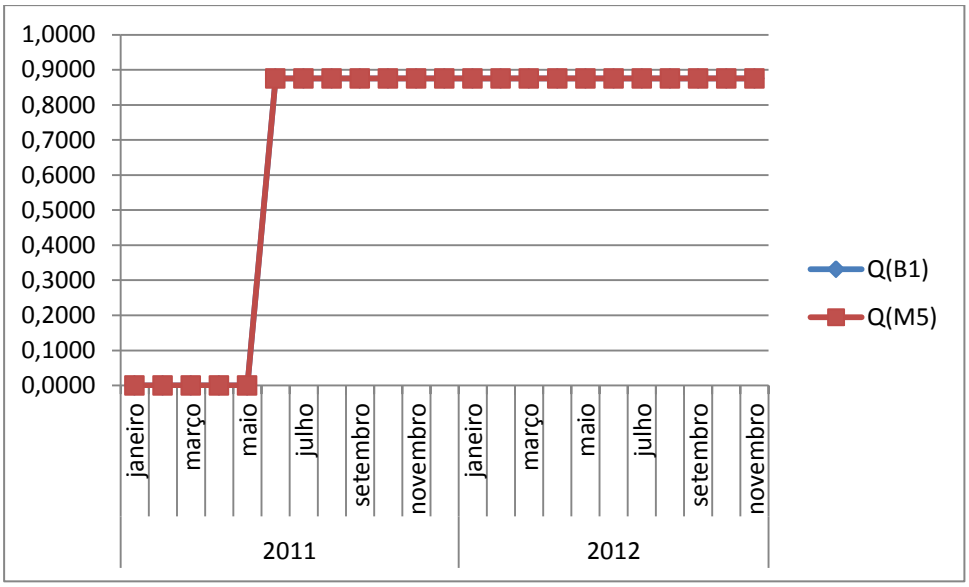
Existe uma inconsistência nos dados até agosto de 2011, mas não foi possível identificar sua origem, sendo excluídos estes dados desta análise.

De acordo com os dados fornecidos, em média, a banda de internet é utilizada no seu limite, isso prejudica o desempenho da rede e reflete no valor de qualidade desta métrica (linha verde). Observa-se também que até o início de 2011 qualquer computador com wi-fi dentro do alcance da rede do campus tinha acesso a rede.

Métrica M_5: “ Controle de segmentação da rede”

Os valores obtidos para as qualidades estão na planilha do Apêndice A.

Gráfico 7 – Resultados da métrica 5



Fonte: Nascimento (2013)

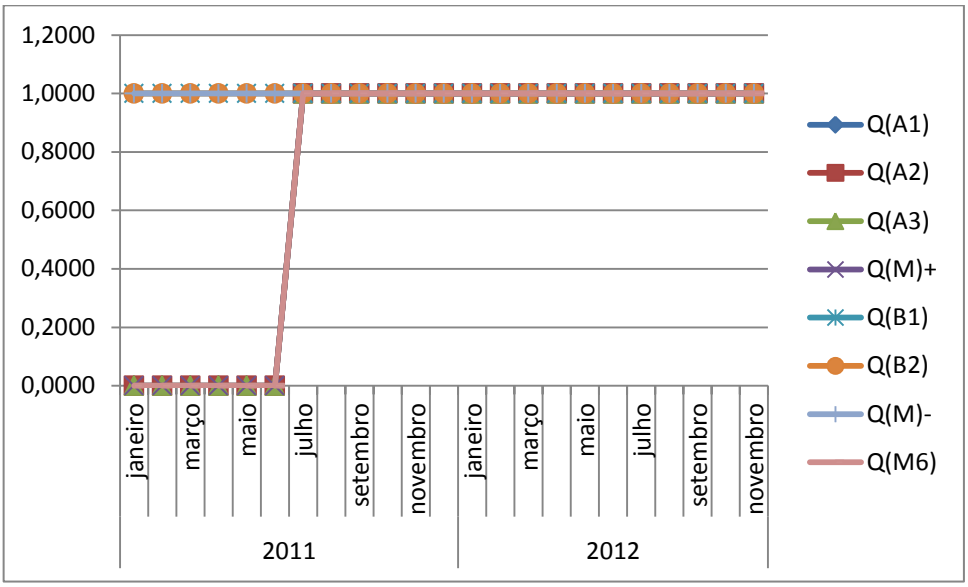
As sub-redes no campus são: Servidores, VoIP, Administrativos, Laboratórios, Visitantes, Docentes, Alunos, Bolsistas.

Nesta métrica a qualidade da ocorrência B_1 era igual a zero durante um período inicial e depois seu valor passou a ser próximo de 1, pois foi somente a partir de junho de 2011, que iniciou-se esta medida. Verificou-se que o número de ocorrências negativas manteve-se muito baixo e a qualidade das ocorrências positivas foi máxima. Observou-se também que até maio de 2011 não existia este controle. Qualquer computador com wi-fi dentro do perímetro do campus tinha acesso à rede e existiam sub-redes.

Métrica M_6: “Controle de segurança interna de servidores”

Os valores obtidos para as qualidades estão na planilha do Apêndice A.

Gráfico 8 – Resultados da métrica 6



Fonte: Nascimento (2013)

Nesta métrica a qualidade de todas as ocorrências foi igual a 1, pois, a partir do período onde foi possível medir todas as ocorrências, não obteve-se ocorrências negativas, neste caso em particular, e a qualidade das ocorrências positivas foi máxima.

Métrica M_7:"Controle de acesso a informações confidenciais armazenadas em estações de trabalho"

Aplicando o método 2 (mto2) na planilha eletrônica obtêm-se as Qualidades das Ocorrências.

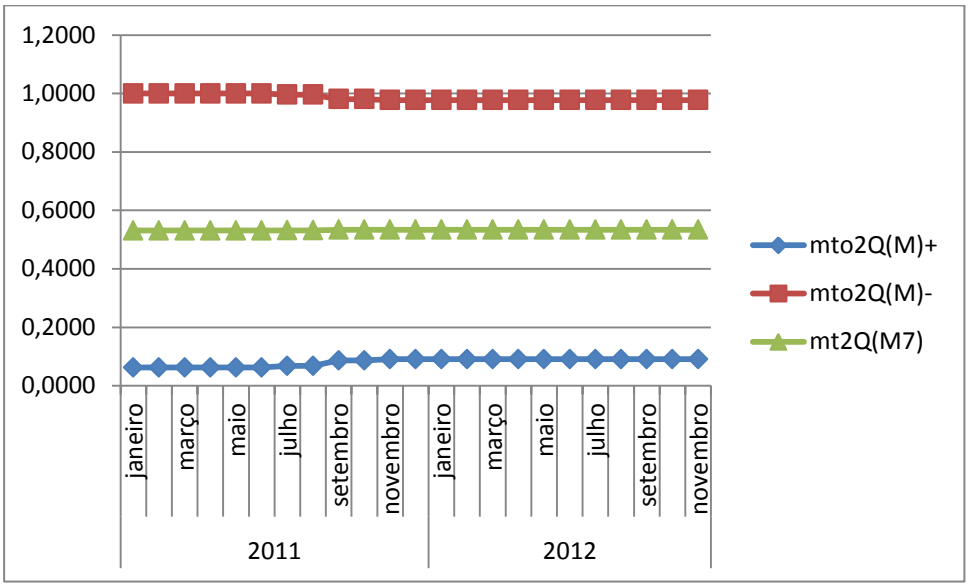
Abaixo apresentamos a forma de linguagem utilizada no Excel para os cálculos.

$Q(M)^+$= ((4(a1234)+(3*a123)+(2*a234)+(2*a12)+(2*a13)+ (2*a14)+ (2*a24)+ (2*a34)+a1+a2+a3+a4)/(s(4* COMBIN(4;4)+3*COMBIN(4;3)+2*COMBIN(4;2)+COMBIN(4;1)))*

*$Q(M)^-$=1-((2*b12)+b1+b2)/(s*(2*COMBIN(2;2)+COMBIN(2;1)))*

Os valores obtidos para as qualidades estão na planilha do Apêndice A.

Gráfico 9 – Resultados da métrica 7



Fonte: Nascimento (2013)

Pode-se perceber que a qualidade das ocorrências negativas está no estado ideal, ou seja, próximo ou igual a 1, pois não tem-se servidores que são utilizados como estação de trabalho e nem estações com antivírus freeware. No caso das ocorrências negativas não tem-se estações de trabalho que realizam backup ou que utilizem software de criptografia. Mas todas as estações são lacradas fisicamente e utilizam autenticação de usuário.

Métrica M_8: “Controle de atendimento de chamados para o SIE”

Aplicando o método 1 (mto1) na planilha eletrônica obtemos as qualidades das ocorrências.

$Q(M)^+$=(a1)/(s)

$Q(M)^+$= (615+74+207+1+8)/(619+76+208+2+2+10)

Tabela 4 - Resultados da Métrica 8

Qualidade	1º semestre 2013
Q(A1)	0,9869
Q(M8)	0,9869

Fonte: Nascimento (2013)

Esta métrica apresenta somente resultado para o primeiro semestre de 2013 em função de ter sido desconsiderada inicialmente pela equipe em 2010. Mas em função da reestruturação na rede foi possível realizar estas medidas em 2013. Esta métrica apresenta o desempenho da equipe de suporte no atendimento a chamados do SIE. Foram considerados e somados os chamados para Acadêmico; Acesso; Biblioteca; Infraestrutura; Patrimônio; Recursos Humanos. Nota-se que a qualidade desta métrica tende a 1, ou seja, este controle está operando bem próximo do que pode se considerar de estado ideal.

Métrica M_9: “Controle de atendimentos do Suporte Técnico Alegrete”

Aplicando o mto1 na planilha eletrônica obtemos as qualidades das ocorrências.

$Q(M)^+$=(a1)/(s)

$Q(M)^+$=(109)/(144)

Tabela 5 - Resultados da Métrica 9

Qualidade	1º semestre 2013
	0,7569
$Q(M9)$	0,7569

Fonte: Nascimento (2013)

Esta métrica apresenta somente resultado para o primeiro semestre de 2013 em função de ter sido desconsiderada inicialmente pela equipe em 2010. Mas em função da reestruturação na rede foi possível realizar estas medidas em 2013. Esta métrica apresenta o desempenho da equipe de suporte do Campus Alegrete no atendimento a chamados.

Métrica M_{10}: “Controle da utilização do VoIP”

Aplicando o mto2 na planilha eletrônica obtemos as qualidades das ocorrências.

$Q(M)^{+}$=*((2*a12)+a1+a2)/(s*(2*COMBIN(2;2)+COMBIN(2;1)))*

$Q(M)^{+}$=*((2*41)+115+41)/(4*(115))*

$Q(M)^{-}$=*1-((2*b12)+b1+b2)/(s*(2*COMBIN(2;2)+COMBIN(2;1)))*

$Q(M)^{-}$=*1-((2*4)+63+98)/(4*(104))*

Tabela 6 - Resultados da métrica 10

Qualidade	Ano de 2013
$Q(M)^{+}$	0,517
$Q(M)^{-}$	0,594
$Q(M7)$	0,556

Fonte: Nascimento (2013)

Em 2010 o Servidor VoIP do NTIC (Alegrete) possuía 299 ramais on line devido a inexistência de Servidores VoIP em todos os campi da Unipampa, com a expansão do projeto em 2011 esse número de ramais reduziu-se para 81 no Campus Alegrete.

No momento da autenticação todos os ramais são vinculados a uma senha alfanumérica. Atualmente existem 63 ramais registrados em aparelhos VoIP e 41 registrados em softphones. No campus Alegrete os DDD e DDI estão liberados para

98 ramais, os ramais que possuem restrição à realização deste tipo de chamada são portaria, guarita por exemplo.

Esta métrica apresenta somente resultado para o primeiro semestre de 2013 em função de ter sido desconsiderada inicialmente pela equipe em 2010. Mas em função da reestruturação na rede foi possível realizar estas medidas em 2013.

O valor da qualidade desta métrica é mediano em função do grande número de ramais em aparelhos VoIP, o que dificulta a identificação de qual usuário realmente está utilizando o serviço e também pelo número de ramais que podem realizar DDI.

4 CONCLUSÕES

Durante a realização deste trabalho foi optado por não realizar uma análise global de qualidade das métricas medidas (como por exemplo apresentar um valor médio da qualidade das dez métricas), pois isso poderia criar uma falsa ideia de segurança na rede da instituição. Como cada métrica tem uma natureza diferente e funciona como um controle, com objetivos distintos, não se acredita que um único valor consiga descrever o real estado de vários espaços métricos. Alguns destes espaços métricos são incompatíveis entre si. Logo, uma análise global iria suprimir falhas graves em pontos específicos da rede de computadores da instituição.

Uma das maiores dificuldades enfrentadas inicialmente, foi elaborar uma definição para métrica e seus componentes de forma que, devido a sua simplicidade, esta definição pudesse servir para auxiliar na criação de novas métricas e que as mesmas fossem relevantes para os objetivos de uma equipe de gestão de TI.

O volume de dados a serem coletados para as métricas é muito grande e suas fontes ainda dispersas. Isto contribui para o aumento de complexidade na gestão da rede pois, exige a liderança de uma grande equipe, formada por membros de setores distintos, que devem aprender a trabalhar como um time, acreditar na relevância da aplicação de métricas.

Neste trabalho propõe-se uma metodologia para o desenvolvimento de um programa para a aplicação de métricas. Essa metodologia consistiu na:

- Revisão na literatura da área para o levantamento de métricas adequadas para uma rede do porte da Unipampa e suas especificidades e do Método matemático para seu cálculo;
- Na realização de reuniões presenciais e web conferências com a equipe do NTIC responsável pela rede da Unipampa para discussão da viabilidade de registro das ocorrências;
- Na coleta de dados;
- Aplicação dos Métodos matemáticos escolhidos;
- Análise dos resultados;
- Apresentação das análises e conclusões para proposição de ações futuras.

O uso das métricas contribuiu para a detecção das áreas da rede da Unipampa com falhas de segurança e na detecção de serviços que apresentam baixo desempenho. Assim, as métricas possibilitaram mostrar estes resultados de uma forma mais quantitativa e menos qualitativa através de um método científico. Dessa forma, fomentando as propostas de melhorias na rede e seu controle de segurança. Fica evidente, como visto nos resultados das métricas, que o armazenamento de dados e informações sobre a rede, desde sua criação, é fundamental para o trabalho de aprimoramento da rede de computadores. Sem estes dados coletados durante um longo período, fica muito difícil afirmar o quão segura é uma determinada rede e o quanto é fiel determinada métrica.

Com o desenvolvimento desta proposta foi possível sugerir melhorias para a rede da instituição como por exemplo:

- O desenvolvimento de um sistema para que as senhas dos usuários fossem testadas e classificadas como boas ou não e o sistema solicitasse aos usuários a renovação periódicas destas senhas;
- Maior capacidade de armazenamento do banco de dados do antivírus;
- Logicamente, aumentar o tamanho da banda de internet para os campi em função da demanda;
- Pensar em uma política para o controle de acesso a informações confidenciais. Acredita-se que, na instituição, existem informações que são estratégicas e estas poderiam ser criptografadas;
- Maior controle no uso dos ramais instalados em aparelhos VoIP. Considera-se que o ideal seria que cada usuário precisasse logar para utilizar o serviço.

Ao final deste trabalho pode-se seguramente afirmar que o ponto mais importante do uso de métricas para redes de computadores em Instituições Federais de Ensino está no desenvolvimento do programa de métricas. Este programa deve ser desenvolvido de modo colaborativo por uma equipe multidisciplinar e é fundamental que seja desenvolvido como um projeto institucional onde todos os envolvidos tenham o compromisso de colaborar com seu desenvolvimento e almejem o seu sucesso. Também a instituição deve prever em seu orçamento, tanto a estrutura física, de pessoal, como também a aquisição ou desenvolvimento de softwares específicos para realizarem os testes e medidas necessárias.

Como proposta para dar continuidade a este trabalho tem-se:

- O desenvolvimento de novas métricas;
- A busca do desenvolvimento de um método mais genérico para ser aplicado a qualquer métrica, independente da existência de interação entre as ocorrências.
- Buscar uma forma de criar métricas para outros sistemas e serviços;
- Propor novas métricas para serem acrescidas ou substituir as propostas neste trabalho;
- Aplicar métricas a um grupo de instituições da mesma natureza da Unipampa, como os Institutos federais e comparar seus resultados;

E o que considera-se mais importante no momento é:

- Desenvolver um sistema informatizado capaz de realizar medidas de diversas ocorrências, armazenar estes dados, e calcular a qualidade de suas métricas e propor ações em função da qualidade específica de uma ocorrência.

Quanto mais automatizado for este processo mais rápida poderá ser a reação a uma possível falha. Em Vieira et al. (2012) é apresentada uma metodologia para automatizar a coleta de dados das métricas em redes de computadores.

REFERÊNCIAS

ARPASI, Jorge Pedraza; NASCIMENTO, Tiago Belmonte. Some necessary conditions for Abelian Group Codes with prime Information group. In: XXIX Simpósio Brasileiro de Telecomunicações, 2011, Curitiba. **Anais ...** Curitiba: Sociedade Brasileira de Telecomunicações (SBrT) 2011. Disponível em: <http://www.dee.ufma.br/~fsouza/Anais_SBrT_2011/papers/completos/84699.pdf>. Acesso em: 30 abr. 2012.

CAIS: **Estatísticas**. Rio de janeiro, 2013. Disponível em: <http://www.rnp.br/cais/estatisticas/index.php>. Acesso em: 30 jul. 2013.

CERT.br. 2012. Disponível em: <http://www.cert.org/>. Acesso em: 03 abr. 2012.

DELLA FLORA, Fernando. **A Influência do NAT na identificação e tratamento de incidentes de segurança da informação**. 2010. 81 p. Monografia (Especialização em Segurança de Redes de Computadores) – Universidade Gama Filho, Alegrete, 2010.

ISACA. **COBIT**. 2012. Disponível em: <http://www.isaca.org/cobit/Pages/default.aspx>. Acesso em: 13 abr. 2012.

JAQUITH, Andrew. **Security metrics:** replacing fear, uncertainty and doubt. Upper Saddle River, NJ: Addison-Wesley, c2007.

KOVACICH, Gerald. Information system security metrics management. **Computers & Security**, Mission Viejo, CA, v.16, n 7, p. 610–618, 1997. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404897807985#>. Acesso em: 03 mar. 2011.

LOWANS, Paul W. **Implementing a network security metrics program**. Global Information Assurance Certification Paper. Version 2.0. Bethesda, MD: SANS Institute, 2000 – 2002. Disponível em: <http://www.giac.org/paper/gsec/1641/implementing-network-security-metrics-programs/103004>. Acesso em: 10 mar. 2011.

MIANI, Rodrigo Sanches**. Aplicação de métricas à análise de segurança em redes metropolitanas de acesso aberto**. 2009. 103 p. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação. Campinas, SP, 2009. Disponível em :

< http://www.bibliotecadigital.unicamp.br/document/?view=000443391>. Acesso em: 03 mar. 2011.

NASCIMENTO, Tiago Belmonte. **Uma proposta de desenvolvimento de métricas para a rede da Unipampa**. 2013. 98 p. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Pampa, Campus Alegrete. Alegrete, RS, 2013.

NIST. Disponível em: <http://www.nist.gov/>. Acesso em: 20 de set. 2013.

NÚCLEO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO. **Histórico**. Disponível em: <http://ntic.unipampa.edu.br/quem-somos-2/historico/>. Acesso em: 03 jul. 2013.

PAYNE, Shirley C. **A guide to security metrics**. SANS Institute InfoSec Reading Room. Bethesda, MD: SANS Institute, 2006. Disponível em: <http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55?show=guide-security-metrics-55&cat=auditing>. Acesso em: 3 abr. 2012.

RNP. Rio de Janeiro, 20123. Disponível em: <http://www.rnp.br/>. Acesso em: 20 de set. 2013.

ROSENBLATT, Joel. Security metrics: a solution in search of a problem. **EDUCAUSE Quarterly**, v. 31, n. 3, p. 8–11, jul./set. 2008. Disponível em: <http://www.educause.edu/ero/article/security-metrics-solution-search-problem>. Acesso em: 8 abr. 2011.

SADEMIES, Anni. **Process Approach to Information SecurityMetrics in Finnish Industry and State Institutions.** Finland: VTT Technical Research Centre of Finland, 2004. (VTT Publications 544). Disponível em: <http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf>. Acesso em: 8 abr. 2011.

SECURITY and privacy controls for federal information systems and organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2013. (NIST Special Publication 800-5, Revision 4). Disponível em: <http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/NIST-SP80053-SecurityandPrivacyControls.pdf>. Acesso em: 30 abr. 2012.

SWANSON, Marianne et al. **Security metrics guide for information technology systems**. Gaithersburg, MD: National Institute of Standards and Technology, 2003. (NIST Special Publication 800-55). Disponível em: <http://www.rootsecure.net/content/downloads/pdf/nist_security_metrics_guide.pdf>. Acesso em: 13 abr. 2011.

SYMANTEC ENDPOINT PROTECTION. Disponível em: <http://www.symantec.com/pt/br/endpoint-protection>. Acesso em: 30 mar. 2012.
TANENBAUM, Andrew Stuart. **Redes de computadores**. Rio de Janeiro, RJ: Campus, c2003.

TARNES, Marte. **Information security metrics an empirical study of current practice**. 2012. 75 p. Project (Specialization) – Norwegian University of Science and Technology, Department of Telematics, Trondheim, 2012. Disponível em: <http://infosec.sintef.no/wp-content/uploads/2012/12/20121217-Marte-Taarnes-prosjekt-maaling-av-infosikkerhet.pdf>. Acesso em: 17 maio 2013.

UNIVERSIDADE FEDERAL DO PAMPA. Disponível em: <http://www.unipampa.edu.br/portal/universidade>. Acesso em: 03 abr. 2012.

VIEIRA, Liniquer Kavrokov et al. An architecture based on agent-manager model for automated data collection of security metrics. In: SECURWARE 2012: The Sixth International Conference on Emerging Security Information, Systems and Technologies. 2012, Roma**. Proceedings ...** Roma: IARIA, 2012. p. 85-91.Disponível em: <http://www.thinkmind.org/index.php?view=article&articleid=securware_2012_4_10_30122>. Acesso em: 17 maio 2013.

WORKSHOP ON INFORMATION SECURITY SCORING AND RANKING, 2001, Silver Spring. **Proceedings …** Silver Spring, MD: Applied Computer Security Associates, 2001. Disponível em: <http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf>. Acesso em: 1 mar. 2011.

BIBLIOGRAFIAS

JANSEN, Wayne. **Directions in Security Metrics Research.** Gaithersburg, MD: National Institute of Standards and Technology, 2009. (NISTIR 7564). Disponível em: <http://books.google.com.br/books?id=fXgyeLTsinQC&pg=PR1&lpg=PR1&dq=%22Directions+in+Security+Metrics+Research%22&source=bl&ots=Nv265B8ShR&sig=4VUVkyO34kYzyTa5mmcoCalTkHM&hl=pt-BR&sa=X&ei=-z9dUtG_CYq0igKpzIDACw&ved=0CIEBEOgBMAg#v=onepage&q=%22Directions%20in%20Security%20Metrics%20Research%22&f=false>. Acesso em: 5 abr. 2012.

KRAUTSEVICH, Leanid; MARTINELLI, Fabio; YAUTSIUKHIN, Artsiom. Formal approach to security metrics. What does “more secure” mean for you?. In: European Conference on Software Architecture, 4., 2010, Copenhagen. **Proceedings ...** Copenhagen, 2010. p.162-169. Disponível em: <http://wwwold.iit.cnr.it/staff/artsiom.yautsiukhin/Resources/KRAU-10-MESSA.pdf>. Acesso em: 9 maio 2012.

KUROSE, James F. **Redes de computadores e a internet:** uma abordagem top-down. 3 ed. São Paulo: Pearson, c2006.

MIANI, Rodrigo Sanches; ZARPELÃO, Bruno Bogaz; MENDES, Leonardo de Souza. Application of security metrics in a metropolitan network : a case study. In: 7th International Telecommunications Symposium, 2010, Manaus. **Proceedings...** Manaus, 2010. Disponível em: <http://www.researchgate.net/publication/234136530_Application_of_Security_Metrics_in_a_Metropolitan_Network__A_Case_Study>. Acesso em: 1 jan. 2011.

MIANI, Rodrigo Sanches et al. Metrics application in metropolitan broadband access network security analysis**.** In: SECRYPT 2008 - International Conference on Security and Cryptography, 2008, Porto. **Proceedings …** Porto: INSTICC Press, 2008. p. 473–476. Disponível em: <http://www.researchgate.net/publication/221436364_Metrics_Application_in_Metropolitan_Broadband_Access_Network_Security_Analysis>. Acesso em: 13 abr. 2012.

NASCIMENTO, Tiago Belmonte; ARPASI, Jorge Pedraza. Desenvolvendo métricas de segurança para a rede da UNIPAMPA. In: SALÃO INTERNACIONAL DE ENSINO, PESQUISA E EXTENSÃO, 4., 2012, Bagé. **Anais...** Bagé: UNIPAMPA, 2012. Disponível em: <http://seer.unipampa.edu.br/index.php/siepe/article/view/1022>. Acesso em: 13 abr. 2013.

PORTAL DO SOFTWARE PÚBLICO BRASILEIRO. **CACIC**: Configurador Automático e Coletor de Informações Computacionais. Disponível em: <http://www.softwarepublico.gov.br/ver-comunidade?community_id=3585>. Acesso em: 03 abr. 2012.

ROSS, Ron et al. **Recommended security controls for federal information systems.** Gaithersburg, MD: National Institute of Standards and Technology, 2005. (NIST Special Publication 800-53). Disponível em: < http://infohost.nmt.edu/~sfs/Regs/sp800-53.pdf>. Acesso em: 25 abr. 2012.

SECURITYMETRICS.ORG. Disponível em: < http://www.securitymetrics.org/>. Acesso em: 30 mar. 2012.

STALLINGS, William. **Redes e sistemas de comunicação de dados**: teoria e aplicações corporativas. Rio de Janeiro: Elsevier, 2005.

WEISS, Steffen; WEISSMANN, Oliver; DRESSLER, Falko. A comprehensive and comparative metric for information security. In: IFIP International Conference on Telecommunication Systems, Modeling and Analysis, 2005, Dallas, TX. **Proceedings …** Dallas, 2005, p. 1-10. Disponível em: <http://www.ccs-labs.org/bib/weiss2005comprehensive/weiss2005comprehensive.pdf>. Acesso em: 3 abr. 2012.

APÊNDICE - A - Tabelas de resultados das Qualidades das Métricas.

Resultados 2011

Métricas	Qualidade	2011											
		janeiro	Fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro	dezembro
Métrica 1 – Controle das contas dos usuários	Q(A1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B2)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	0,9988	0,9988	0,9124	0,7593	0,7395	0,7150
	Q(M)+	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(M)-	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,4994	0,4994	0,4562	0,3797	0,3697	0,3575
	mt1Q(M1)	0,2500	0,2500	0,2500	0,2500	0,2500	0,2500	0,2497	0,2497	0,2281	0,1898	0,1849	0,1787
Métrica 2 – Controle da ploriferação de vírus	Q(A1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(A2)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(M)+	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	0,5229	0,8708	1,0000	1,0000
	Q(B2)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!

	Q(B3)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!
	Q(M)-	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!
	mt1Q(M2)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!
	mt2Q(M)+	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	mt2Q(M)-	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	0,9872	0,9872	0,4771	0,5224	0,5645	0,5596
	met2Q(M2)	0,5000	0,5000	0,5000	0,5000	0,5000	0,5000	0,4936	0,4936	0,2385	0,2612	0,2822	0,2798
Métrica 3 – Controle de segurança dos pontos de acesso de uma rede Wi-Fi	Q(A1)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)+	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B1)	#VALOR!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B2)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B3)	#VALOR!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)-	#VALOR!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	mt1Q(M3)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
Métrica 4 – Controle de Utilização da Banda de Internet	Q(B1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B2)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	-33,0000	-33,0000	0,5467	0,8350	0,8475	0,8607

	Q(M4)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	-16,5000	-16,5000	0,2733	0,4175	0,4238	0,4303
Métrica 5 – Controle de Segmentação da rede	Q(B1)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750
	Q(M5)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750
Métrica 6 – Controle de segurança interna de servidores	Q(A1)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(A2)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(A3)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)+	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B2)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)-	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M6)	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
Métrica 7 – Controle de acesso a informações confidenciais armazenadas em estações de trabalho	mto2Q(M)+	0,0625	0,0625	0,0625	0,0625	0,0625	0,0625	0,0676	0,0676	0,0865	0,0865	0,0909	0,0909
	mto2Q(M)-	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	0,9959	0,9959	0,9808	0,9808	0,9773	0,9773
	mt2Q(M7)	0,5313	0,5313	0,5313	0,5313	0,5313	0,5313	0,5318	0,5318	0,5337	0,5337	0,5341	0,5341

Resultados 2012

Métricas	Qualidade	2012										
		janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
Métrica 1 – Controle das contas dos usuários;	Q(A1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B2)	0,7114	0,7079	0,7639	0,7639	0,7244	0,7197	0,7178	0,7140	0,7065	0,7037	0,6999
	Q(M)+	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(M)-	0,3557	0,3540	0,3819	0,3819	0,3622	0,3598	0,3589	0,3570	0,3532	0,3518	0,3500
	mt1Q(M1)	0,1779	0,1770	0,1910	0,1910	0,1811	0,1799	0,1794	0,1785	0,1766	0,1759	0,1750
Métrica 2 – Controle da proliferação de vírus;	Q(A1)	0,3500	0,5300	0,6901	0,5282	0,4018	0,4653	0,4625	0,4570	0,4464	0,4425	0,4347
	Q(A2)	0,2393	0,5265	0,6725	0,5070	0,3834	0,5438	0,5886	0,5638	0,5797	0,5805	0,6619
	Q(M)+	0,2946	0,5283	0,6813	0,5176	0,3926	0,5045	0,5255	0,5104	0,5130	0,5115	0,5483
	Q(B1)	0,9679	0,9470	0,8908	0,9085	0,9294	1,0000	1,0000	1,0000	1,0000	0,9138	0,9403
	Q(B2)	0,2551	0,8533	0,6684	0,5467	0,8321	1,0000	1,0000	0,9675	0,9870	1,0000	0,9935

Métricas	Qualidade	2012										
		janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
	Q(B3)	0,9701	0,4362	0,6754	0,5556	0,8000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)-	0,7310	0,7455	0,7449	0,6702	0,8538	1,0000	1,0000	0,9892	0,9957	0,9713	0,9779
	mt1Q(M2)	0,5128	0,6369	0,7131	0,5939	0,6232	0,7523	0,7628	0,7498	0,7544	0,7414	0,7631
	mt2Q(M)+	0,2670	0,5274	0,6769	0,5123	0,3880	0,5242	0,5571	0,5371	0,5464	0,5460	0,6051
	mt2Q(M)-	0,4491	0,5093	0,4313	0,4340	0,4988	0,5498	0,5495	0,5434	0,5457	0,5151	0,5234
	met2Q(M2)	0,3580	0,5183	0,5541	0,4732	0,4434	0,5370	0,5533	0,5402	0,5460	0,5305	0,5643
Métrica 3 – Controle de segurança dos pontos de acesso de uma rede Wi-Fi;	Q(A1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)+	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B2)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B3)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Métricas	Qualidade	2012										
		janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
	Q(M)-	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	mt1Q(M3)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
Métrica 4 – Controle de Utilização da Banda de Internet;	Q(B1)	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
	Q(B2)	0,8623	0,8640	0,8645	0,8645	0,8840	0,8859	0,8867	0,8882	0,8910	0,8921	0,8934
	Q(M4)	0,4312	0,4320	0,4323	0,4323	0,4420	0,4430	0,4433	0,4441	0,4455	0,4460	0,4467
Métrica 5 – Controle de Segmentação da rede;	Q(B1)	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750
	Q(M5)	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750	0,8750
Métrica 6 – Controle de segurança interna de servidores;	Q(A1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(A2)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(A3)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)+	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Métricas	Qualidade	2012										
		janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
	Q(B1)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(B2)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M)-	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
	Q(M6)	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000
Métrica 7 – Controle de acesso a informações confidenciais armazenadas em estações de trabalho;	mto2Q(M)+	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909	0,0909
	mto2Q(M)-	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773	0,9773
	mt2Q(M7)	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341	0,5341

Fonte: Nascimento (2013)

ANEXO A - Tabelas de dados fornecidos pelo NTIC

UNIPAMPA Campus Alegrete

Tabela de dados 2011

		2011											
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro	dezembro
Número total de contas de usuários		600	600	856	856	856	856	856	856	856	856	856	856
Número total de computadores (Desktops)	AD (Active Directory)	0	0	0	0	0	0	0	0	68	88	103	112
Número total de computadores (Laboratórios)	AD (Active Directory)	0	0	0	0	0	0	0	0	0	111	112	124
Número total de computadores (Notebooks)	AD (Active Directory)	0	0	0	0	0	0	0	0	2	2	2	2
Número total de computadores (Servidores)	AD (Active Directory)	0	0	0	0	0	0	1	1	5	5	6	6
Número de usuários com privilégios de administrador	AD (Active Directory)	0	0	0	0	0	0	1	1	75	206	223	244
Número de computadores utilizando a conta de Administrador como conta de trabalho	AD (Active Directory)	0	0	0	0	0	0	1	1	75	206	223	244
Número total de vírus reportado	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0		31599	32019		

		2011											
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro	dezembro
Número de computadores infectados	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0		52	31		
Número de computadores com antivírus instalado	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número de computadores com assinaturas de vírus desatualizadas	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número de vírus com alta criticidade	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número de computadores com antispyware instalado	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número de computadores com antispyware com assinaturas atuais	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número de computadores com antivírus e antispyware instalado	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0					
Número total de pontos de acesso	Wireless LAN Controller	0	0	0	0	0	17	17	17	17	17	17	17
Número de pontos de acesso com protocolos de segurança habilitados (todos usam protocolo WAP + WAP2)	Wireless LAN Controller	0	0	0	0	0	17	17	17	17	17	17	17

		2011											
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro	dezembro
Número de pontos de acesso que não foram trocadas as senhas padrão	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0	0
Número de pontos de acesso com o SSID padrão	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0	0
Número de pontos de acesso com versões desatualizadas de firmware e software	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0	0
Número de pontos de acesso com autenticação aberta	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0	0
Tamanho total da banda alocada para Internet	Cacti (em Mb)	34	34	34	34	34	34	34	34	34	34	34	34
Número de computadores que possuem acesso à Internet	AD (Active Directory)	0	0	0	0	0	0	1	1	75	206	223	244
Banda média de Internet utilizada	Cacti (em Mb)	34	34	34	34	34	34	34	34	34	34	34	34
Número de computadores que estão conectados à internet não distribuída	AD (Active Directory)	0	0	0	0	0	0	1	1	75	206	223	244
Número total de sub-redes	CNA (Cisco Network Assistant)	0	0	0	0	0	8	8	8	8	8	8	8

		2011											
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro	dezembro
Número de domínios que acessam outros domínios de sub-rede não definidos pela política de segurança interna	CNA (Cisco Network Assistant)	1	1	1	1	1	1	1	1	1	1	1	1

Fonte: NTIC (2012)

Tabela de dados 2012

NTIC/UNIPAMPA Campus Alegrete		2012										
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
Número total de usuários		856	856	1063	1063	1063	1063	1063	1063	1063	1063	1063
Número total de computadores (Desktops)	AD (Active Directory)	113	116	117	117	127	130	131	132	136	139	143
Número total de computadores (Laboratórios)	AD (Active Directory)	125	125	125	125	156	158	159	162	162	162	162
Número total de computadores (Notebooks)	AD (Active Directory)	3	3	3	3	4	4	4	4	8	8	8
Número total de computadores (Servidores)	AD (Active Directory)	6	6	6	6	6	6	6	6	6	6	6
Número de usuários com privilégios de administrador	AD (Active Directory)	247	250	251	251	293	298	300	304	312	315	319
Número de computadores utilizando a conta de Administrador como conta de trabalho	AD (Active Directory)	247	250	251	251	293	298	300	304	312	315	319
Número total de vírus reportado	SEP (Symantec Endpoint Protection)	103	434	4091	38773	39118	0	0	0	0	7032	5035
Número de computadores infectados	SEP (Symantec Endpoint Protection)	9	15	31	26	23	0	0	0	0	30	21
Número de computadores com antivírus instalado	SEP (Symantec Endpoint Protection)	98	150	196	150	131	154	154	154	154	154	153

NTIC/UNIPAMPA Campus Alegrete						2012						
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
Número de computadores com assinaturas de vírus desatualizadas	SEP (Symantec Endpoint Protection)	73	22	65	68	22	0	0	5	2	0	1
Número de vírus com alta criticidade	SEP (Symantec Endpoint Protection)	0	0	0	0	0	0	0	0	0	0	0
Número de computadores com antispyware instalado	SEP (Symantec Endpoint Protection)	67	149	191	144	125	180	196	190	200	202	233
Número de computadores com antispyware com assinaturas atuais	SEP (Symantec Endpoint Protection)	65	65	129	80	100	180	196	190	200	202	233
Número de computadores com antivírus e antispyware instalado	SEP (Symantec Endpoint Protection)	67	149	191	144	125	180	196	190	200	202	233
Número total de pontos de acesso	Wireless LAN Controller	17	17	17	17	17	17	17	17	17	17	17
Número de pontos de acesso com protocolos de segurança habilitados (todos usam protocolo WAP + WAP2)	Wireless LAN Controller	17	17	17	17	17	17	17	17	17	17	17
Número de pontos de acesso que não foram trocadas as senhas padrão	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0
Número de pontos de acesso com o SSID padrão	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0
Número de pontos de acesso com versões desatualizadas de firmware e software	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0

NTIC/UNIPAMPA Campus Alegrete						2012						
Ocorrência Medida	Software/Fonte dos dados	janeiro	fevereiro	março	abril	maio	junho	julho	agosto	setembro	outubro	novembro
Número de pontos de acesso com autenticação aberta	Wireless LAN Controller	0	0	0	0	0	0	0	0	0	0	0
Tamanho total da banda alocada para Internet	Cacti (em Mb)	34	34	34	34	34	34	34	34	34	34	34
Número de computadores que possuem acesso à Internet	AD (Active Directory)	247	250	251	251	293	298	300	304	312	315	319
Banda média de Internet utilizada	Cacti (em Mb)	34	34	34	34	34	34	34	34	34	34	34
Número de computadores que estão conectados à internet não distribuída	AD (Active Directory)	247	250	251	251	293	298	300	304	312	315	319
Número total de sub-redes	CNA (Cisco Network Assistant)	8	8	8	8	8	8	8	8	8	8	8
Número de domínios que acessam outros domínios de sub-rede não definidos pela política de segurança interna	CNA (Cisco Network Assistant)	1	1	1	1	1	1	1	1	1	1	1

Fonte: NTIC (2012)

Tabela de dados 2012

	Ano
	2012
Número de servidores em toda Unipampa (somando-se VM - Virtual Machines),	79
Servidores que realizam backup	36
Campus Alegrete	
Ramais VoIP	104
Usuários estavam cadastrados para o uso do VoIP	115
Ramais registrados em aparelhos VoIP	63
Ramais registrados em softphones.	41
Ramais com DDD e DDI liberados	98

Fonte: NTIC (2013)

Tabela de dados 2013

Área de atendimento	Período de 01/01/2013 a 01/07/2013	
	Chamados abertos	Chamados fechados
Suporte Técnico Alegrete	144	109
SIE (Acadêmico; Acesso; Biblioteca; Infraestrutura; Patrimônio; Recursos Humanos)	917	905

Fonte: NTIC (2013)