
**ALEX SALES ANDRADE**

# SEGURANÇA DA INFORMAÇÃO COM FOCO EM INFRAESTRUTURA: UM ESTUDO DE CASO EM UMA EMPRESA DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

**LAVRAS - MG**

**2011**

**ALEX SALES ANDRADE**

# SEGURANÇA DA INFORMAÇÃO COM FOCO EM INFRAESTRUTURA: UM ESTUDO DE CASO EM UMA EMPRESA DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

Monografia apresentada ao colegiado do Curso de Ciência da Computação, para a obtenção do título de Bacharel em Ciência da Computação.

Orientador:
Dr. Luiz Henrique Andrade Correia

**LAVRAS - MG**
**2011**

**ALEX SALES ANDRADE**

# SEGURANÇA DA INFORMAÇÃO COM FOCO EM INFRAESTRUTURA: UM ESTUDO DE CASO EM UMA EMPRESA DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

Monografia apresentada ao colegiado do Curso de Ciência da Computação, para a obtenção do título de Bacharel em Ciência da Computação.

APROVADA em ____ de _____ de _____

| | |
|---|---|
| Dr. Rêmulo Alves Maia | UFLA |
| Dr. Tales Heimfarth | UFLA |

Dra. Luiz Henrique Andrade Correia
Orientador

**LAVRAS - MG**
**2011**

*Aos meus pais Wilson e Leila.*
*Aos meus irmãos Artur e Maira que me deram apoio durante toda jornada.*
*À todos que me ajudaram de alguma forma.*

**DEDICO**

**AGRADECIMENTOS**

Primeiramente, agradeço a Deus, que incomparável em sua infinita bondade, me concedeu a necessária coragem e determinação para atingir mais esse objetivo.

À minha família, em especial aos meus pais, Wilson e Leila, que não pouparam esforços para que eu conquistasse e concluísse essa etapa da minha vida. Pelo sacrifício, amor, incentivo e confiança em todos os momentos.

Aos meus irmãos, Maira e Artur, pelo apoio incondicional e troca de conhecimentos durante toda a caminhada.

À todos que, de alguma forma, me ajudaram durante o curso de Ciência da Computação, meus sinceros agradecimentos.

Ao professor e orientador Luiz Henrique, que mesmo com o tempo limitado, depositou confiança em mim e me ajudou a desenvolver este trabalho. Pelo comprometimento e pela paciência.

Aos professores e funcionários do DCC – Departamento de Ciência da Computação.

“O único lugar onde o sucesso vem antes do trabalho é no dicionário” Albert Einstein

## RESUMO

Este trabalho tem como objetivo analisar a infraestrutura da organização no aspecto da segurança da informação. Apesar da segurança da informação ter três princípios essenciais, o foco se deu apenas na disponibilidade da informação. Os princípios de integridade e confidencialidade comprometeriam a organização. A análise foi considerada necessária pelo fato da segurança da informação não se tratar de um esforço único. Desta forma, a empresa deve estar sempre sendo avaliada e reavaliada para identificar novos riscos e constatar a eficácia da solução de combate contra os riscos já identificados. Para esta análise, foi realizado um levantamento da topologia da rede de computadores da empresa tanto na matriz quanto em sua filial. Informações adicionais como o estado de recursos computacionais também foram identificados. Com base no material obtido no levantamento, a topologia das redes de computadores foram modeladas no software de simulação *OPNET IT Guru Edition*. O cenário atual da topologia e um cenário proposto com as possíveis melhorias foram modelados, simulados e comparados. A comparação dos resultados foi baseada na latência da rede e no tráfego nos *switches*. A latência da rede apresentou uma melhora de 40% em relação ao cenário atual. Por sua vez, o tráfego nos *switches* (bits por segundo) apresentou uma diminuição de até 13,6 vezes em relação ao cenário atual. Como a segurança da informação é considerada um processo de gestão dentro da empresa e envolve todos os setores de uma organização, este trabalho não conseguiria abranger todos os aspectos. Porém, baseado em quatro funcionários da organização, dois gerentes, um desenvolvedor e um responsável pela infraestrutura, foi feita uma avaliação da infraestrutura em relação à segurança física, lógica e de recursos humanos. A avaliação foi feita através do QBASI(Questionário Básico de Avaliação da Segurança da Informação) proposto por Fontes. Nesta avaliação, a empresa obteve 47,14% de eficácia em sua segurança física, 60% na segurança lógica e 17,5% na segurança em recursos humanos. Considerando a segurança da infraestrutura como um todo, a empresa obtém um total de eficácia em sua infraestrutura de 41,55%. Deste modo, os pontos fracos e positivos da infraestrutura da organização não encontrados na simulação são identificados no questionário e devem ser analisados com o intuito de melhorar a sua eficácia e garantir sua continuidade no mercado.



Palavras-chave**:**



## ABSTRACT

This paper aims to analyze the infrastructure of the organization in

the aspect of information security. Although information security has three basic principles, the focus was only on the availability of information. The principles of integrity and confidentiality would jeopardize the organization. The analysis is necessary because the information security is not obtained with a single effort. Thus, the company must always be evaluated and reviewed to identify new risks and to verify the effectiveness of the solution to combat the risks already identified. For this analysis, a survey was conducted on the topology of computer network of the company both at headquarters and in its subsidiary. Additional information such as the status of computing resources were also identified. Based on material obtained in the survey, the topology of computer networks were modeled in the simulation software OPNET IT Guru Edition. The current scenario of the topology and a proposed scenario with possible improvements were modeled, simulated and compared. The comparison of the results was based on network latency and traffic on the *switches*. Network latency showed an improvement of 40% over the current scenario. In turn, the traffic in the *switches* (bits per second) showed a decrease of up to 13.6 times compared to the current scenario. As information security is considered a management process within the company and involves all sectors of an organization, this work could not cover all aspects. However, based on four employees of the organization, two managers, a developer and responsible for the infrastructure, an assessment was made of the infrastructure in relation to physical security, logical and human resources. The evaluation was done using QBASE (Basic Assessment Questionnaire Information Security) proposed by Fontes. In this evaluation, the company achieved 47.14% efficiency in their physical security, logical security at 60% and 17.5% for safety in human resources. Considering the safety of the infrastructure as a whole, the company gets a total effectiveness in its infrastructure of 41.55%. Thus, the weaknesses and strengths of the organization's infrastructure that were found in the simulation are identified in the questionnaire and should be analyzed in order to improve its effectiveness and ensure its continuity in the market.

Keywords*:* Information Systems, Computer Networks, *OPNET IT Guru Academic Edition*.

**LISTA DE FIGURAS**

## LISTA DE TABELAS

**SUMÁRIO**

# 1 INTRODUÇÃO

Atividades e soluções providas por recursos computacionais ganharam muito espaço nos dias atuais. As finalidades em que são empregados são diversas. Usuários domésticos fazem uso através de jogos, atividades escolares ou profissionais, correio eletrônico e outros. No contexto organizacional, os recursos são empregados com o intuito de armazenar, compartilhar, criar e acessar informações.

As redes de computadores, meio de comunicação utilizado para o compartilhamento das informações, apresentaram enorme crescimento comparada com as primeiras décadas da sua criação. Inicialmente eram utilizadas por tipos específicos de usuários com o intuito de enviar mensagens de correio eletrônico ou compartilhar algum recurso computacional como a impressora. Apesar das inúmeras vantagens oferecidas pelas redes de computadores como o compartilhamento de recursos e a interatividade de seus usuários, vários problemas têm ocorrido no últimos anos. Um destes problemas consiste nos ataques virtuais praticados por diversos tipos de pessoas maliciosas. Dependendo do contexto em que se esteja, as pessoas maliciosas podem ser estudantes, executivos, vigaristas, contadores e até mesmo terroristas com os seus respectivos objetivos. Este problema despertou uma necessidade vital para a continuação do uso das redes de computadores, a segurança (TANEMBAUM, 2003).

A partir daí, medidas de segurança da informação foram aplicadas ao contexto de redes de computadores para garantir uma utilização de forma mais segura. As medidas seguem os seguintes princípios: privacidade, autenticação, integridade e não-repúdio (FOROUZAN, 2006).

Porém, assim como houve a evolução da utilização das redes de computadores, a tecnologia está em constante evolução. Ao mesmo passo que surgem novas tecnologias que modificam o modo de interação homem e máquina, há a criação de tecnologias que facilitam burlar as medidas de segurança. Deste modo, a segurança da informação dentro das organizações deve ser atualizada e monitorada continuamente para evitar riscos. A segurança da informação é vista como um processo exclusivo de boas práticas dentro das organizações pois reflete diretamente na reputação e na competitividade da organização no mercado atual (*COBIT Security Baseline*, 2007).

## 1.1 Objetivo

O presente trabalho tem como objetivo geral analisar sobre o conceito de segurança da informação a infraestrutura da organização em questão. Analisar-se-á a segurança física, lógica e de recursos humanos da empresa baseando-se na norma ISO 27002:2005 e no QBASI (Questionário Básico de Avaliação da Segurança da Informação) proposto por Fontes. Dessa forma, tenta-se descobrir se a empresa está gerenciando e monitorando adequadamente as suas instalações tendo em vista as boas práticas. Tal abordagem irá identificar riscos que possam afetar de algum modo a continuidade do negócio e busca reduzi-los ao identificar a causa, de modo que a empresa possa continuar a trilhar a sua trajetória no mercado de forma mais segura. Destaca-se que a empresa atua no ramo de desenvolvimento de soluções para a área de mineração. O objetivo da mesma é se tornar líder no mercado em seu segmento de atuação.

Para atender o objetivo geral, o levantamento de dados a respeito da segurança da informação na empresa foi realizado. Para a infraestrutura, foi efetuado o mapeamento da topologia da rede de computadores. Com base nas informações coletadas e no mapeamento, uma simulação foi feita no simulador *OPNET IT Guru Edition* e propostas de melhorias foram apresentadas baseadas nos resultados das simulações. Um controle para melhor gerenciamento e monitoramento dos riscos foi proposto com base na norma. Finalmente, para se obter um retorno do estado atual em que se encontra a empresa em relação à segurança da informação, uma avaliação foi realizada baseada no QBASI proposto por Fontes. Esta avaliação servirá como um medidor de desempenho da empresa numa futura avaliação. Com isso, se espera obter uma melhora na gestão da segurança da informação da organização.

## 1.2 Motivação

Atualmente, a empresa se encontra em processo de crescimento e conquista de mercado. Sendo assim, a preocupação com a segurança dos ativos se faz necessária. A informação presente nas organizações já se tornou um recurso estratégico. Segundo o Ponemon Institute (2010), em seu estudo anual, o valor por dado perdido ou roubado das empresas em 2009 foi de US$204 por registro. Isto demonstra que o valor das informações das empresas se tornou muito valioso já que há cinco anos atrás seu valor era de US$66 por registro.

Este levantamento foi baseado em informações de quarenta e cinco

empresas que assumiram publicamente a violação dos dados confidenciais de clientes ao longo de 2009. Diante disso, uma análise da segurança da informação na empresa se torna válida, já que o seu monitoramento deve ser feito dentro de períodos pré-definidos a fim de estar sempre alinhado com a evolução das tecnológica.

## 1.3 Definição do problema

Sabendo que o ramo de atuação da empresa envolve recursos financeiros e vem ganhando mais espaço a cada dia, a organização passa a ser visada pelas concorrentes e por pessoas curiosas devido ao seu crescimento e propaganda. Com isso, se os dados da empresa vierem a ser comprometidos por algum concorrente, pessoas não autorizadas ou até mesmo por causas naturais como enchentes e incêndios, situações desagradáveis podem acontecer. Tais acontecimentos podem afetar a reputação da empresa com seus clientes, bem como comprometer a atuação no mercado, devido à intensidade dos danos causados. Portanto, uma análise e um posterior planejamento e monitoramento de um controle de segurança da informação, auxiliam significativamente na conquista da segurança. Pode-se perceber a prioridade deste processo dentro das organizações pelo simples fato da criação de um guia de boas práticas (*COBIT Security Baseline*) exclusivo para a segurança da informação, assim como a existência de normas específicas para o assunto como a ISO 27002:2005. Contudo, a maioria das organizações têm consciência da necessidade da segurança da informação mas não se atentam ao fato de ser um esforço contínuo. As tarefas diárias de seus colaboradores, com foco no objetivo do negócio da organização, muitas vezes podem estar inibindo esforços em relação à segurança. O fato de existir algumas medidas de segurança implementadas não implica em estar imune a todos os riscos. Quando menos se espera, as atividades diárias podem ser interrompidas, impactando nas tarefas diárias. Portanto, uma verificação do nível da segurança da informação é necessária de tempos em tempos.

## 1.4 Solução proposta

A segurança da informação é vista como um processo essencial dentro das organizações atuais. Para garantir uma melhor gerência deste processo, controles são implementados com a finalidade de manter a

continuidade e avaliar a eficiência. Sendo assim, para implementar controles, deve-se analisar os riscos existentes.

Com a análise dos riscos, a escolha de uma solução que o combata e a definição de um controle para posterior monitoração devem ser feitas.

Neste trabalho, efetuou-se uma avaliação da segurança da organização baseado apenas na sua atual infraestrutura. Primeiramente, realizou-se uma análise da estrutura atual da rede de computadores. Posteriormente, uma modelagem e simulação da rede mapeada foi feita no programa *OPNET IT Guru Academic Edition* com o intuito de descobrir algum risco. A partir daí, riscos foram identificados, quantificados e tiveram sua causa descoberta. Desta forma, uma solução foi proposta para auxiliar na redução ou minimização dos riscos contra a disponibilidade da informação. Um controle, baseado nos guias de boas práticas *COBIT Security Baseline* e na norma ISO 27002 foi proposto para verificar a eficácia da solução e uma possível melhora futura.

A implementação do controle é um adicional importante para evitar que os riscos contra a disponibilidade ocorram novamente e aumentem ainda mais. Adicionalmente, a utilização de controles é fundamental para a criação de um processo de segurança da informação completo e descentralizado dentro da empresa. Como a estrutura de rede de computadores é a base para a comunicação e disponibilidade dos dados, o foco deste trabalho esteve na garantia do seu funcionamento.

Ao final, um questionário de avaliação da segurança da informação proposto dor Fontes foi aplicado à organização a fim de descobrir em que nível a empresa se encontra e servir de base para uma posterior comparação. A avaliação se deu nos segmentos de segurança física, lógica e de recursos humanos.

Por motivos de segurança, a análise da segurança da informação se baseou apenas na questão da garantia de disponibilidade dos dados. Uma análise de integridade e confidencialidade dos dados dentro da organização poderia revelar dados que facilitariam algum tipo de ataque à organização.

## 1.5 Organização do trabalho

No que se refere à estrutura formal do trabalho, tem-se que no capítulo 2, são apresentados os conceitos de informação, segurança da informação, ameaças, controle de acesso e norma de segurança da

informação ISO/IEC 27002:2005. A metodologia utilizada neste trabalho é apresentada no capítulo 3, juntamente com informações sobre o processo de simulação, norma ISO 27002 e o questionário QBASI utilizado. No capítulo 4, o levantamento de dados e da topologia das redes de computadores é apresentado. No capítulo 5, os cenários da simulação da rede de computadores atual e a proposta são comparados e discutidos, assim como os resultados da avaliação da empresa pelo questionário QBASI. Já no capítulo 6, a conclusão do trabalho é apresentada. Em anexo, as perguntas do questionários são fornecidas, assim como a sua nota, justificativa e possível solução proposta quando aplicável.

# 2 REFERENCIAL TEÓRICO

A informação sempre teve o seu valor dentro das organizações. O contraste existente entre os dias atuais, é que há algum tempo elas eram guardadas e trancadas dentro de gavetas e cofres. Atualmente, os computadores processam e armazenam a maioria das informações operacionais e estratégicas dentro da empresa. Sabendo disso, independente do estágio de tecnologia da organização, a proteção da informação deve ser uma das preocupações dos executivos e proprietários das empresas (FONTES, 2008).

## 2.1 O que é informação?

Segundo a norma ISO 27002 (2005), informação “é um ativo, que

como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente precisa ser adequadamente protegida". Ainda segundo a mesma norma, entende-se ativo como " qualquer coisa que tenha valor para a organização". Através deles as informações são criadas, processadas, armazenadas, compartilhadas ou eliminadas.

Baseado nas definições anteriores, as formas de existência da informação dentro das empresas podem ser inúmeras. Pode estar representada em uma impressão, escrita em papel, armazenada eletronicamente, em filmes ou conversas e pode ser transmitida por correio eletrônico, caixas e outros.

Segundo Fontes (2008), a segurança da informação envolve diversos aspectos dentro de uma organização. Em relação à infraestrutura, podemos dividi-la em física, lógica e recursos humanos (pessoas). Os conceitos apresentados estão sumarizados na tabela 1 a seguir. A relação das duas primeiras colunas envolvem o tipo de segurança e o seu conceito. As duas colunas seguintes apresentam exemplos e medidas de proteção aos ativos envolvidos com o tipo corrente.

| Segurança de Ativos | Conceito | Exemplos de ativos | Medidas de Proteção |
|---|---|---|---|
| Segurança Física | Local onde estão os ativos de informação e devem ser protegidos contra ameaças que gerem algum dano à utilização do ativo para o negócio | Equipamentos como servidores, notebooks, no-break, geradores e documentos | chaves, cadeados, cartões, biometria, cofres, portas e outros |
| Segurança Lógica | Procedimentos para o controle de acesso lógico que visa garantir que apenas usuários cadastrados e previamente autorizados acessem a informação de acordo com o seu tipo de permissão: leitura, escrita, alteração e remoção | Dados armazenados em servidores, computadores e redes de dados. | criptografia, firewall, vpn, anti-vírus, permissões de usuários nas aplicações utilizadas pela empresa e muitas outras medidas que previnem o controle de acesso lógico. |
| Segurança em Recursos Humanos | Funcionários e todos os colaboradores da empresa devem saber de suas responsabilidades em relação à segurança da informação. Este recurso deve ser analisado antes da contratação e no momento de sua saída. | funcionários, estagiários e outros colaboradores | procedimentos internos e políticas |

Tabela 1 – Relação entre os tipos de segurança

Com base na tabela 1 apresentada, nota-se que a segurança de ativos dentro da organização se apresenta de acordo com o ativo em questão e diversas medidas podem ser empregadas a fim de conseguir a mesma segurança. Um papel pode ser guardado num cofre, numa sala que utilize chave, cartão ou biometria para acesso.

Desse modo, a empresa deve definir o nível de segurança mais adequado para ela. No cenário em que as empresas estão cada vez mais interconectadas, a informação sofre exposição a inúmeras ameaças e vulnerabilidades, que aumentam a cada dia com a evolução tecnológica ( ISO 27002, 2005).

Segundo a norma ISO 27002, ameaça é "uma causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização" e vulnerabilidade é definida como a "fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças".

Com o surgimento de novas tecnologias a todo momento, ações de segurança devem ser levadas em consideração a cada novo recurso utilizado pela organização. Deste modo, permite-se a continuidade da proteção mesmo com a constante evolução da tecnologia (FONTES, 2008).

## 2.2 Segurança da Informação

Segundo o guia de boas práticas em segurança da informação *COBIT Secutiry Baseline*, a segurança refere-se à proteção de ativos valiosos para os usuários contra indisponibilidade, perda, uso indevido, a divulgação ou danos. Neste contexto, os bens valiosos são as informações gravadas, processadas, armazenadas, compartilhads, transmitidas ou recuperadas de qualquer meio.

### 2.2.1 O que é Segurança da Informação?

Neste presente trabalho, é utilizada a seguinte definição quando nos referirmos à segurança da informação.

" Segurança da informação é a proteção da informação contra possíveis ameaças com o intuito de garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ISO 27002, 2005).

O objetivo fundamental da segurança da informação é proteger o interesse daquelas pessoas que confiam na informação, assim como sistemas e meios de comunicações que fornecem a informação de falhas de disponibilidade, confidencialidade e integridade (COBIT Security Baseline, 2007).

Sendo assim, os três princípios considerados os pilares da segurança da informação pela literatura são definidos a seguir.

- **Confidencialidade** – A privacidade dos dados em questão deve ser garantida. Os dados devem ser protegidos contra acesso não autorizado (COMER, 2007).

- **Integridade** – A veracidade dos dados deve ser garantida. A existência de proteção contra mudanças não-autorizadas no sistema deve ser existir (COMER, 2007).

- **Disponibilidade** – O sistema deve fornecer as informações sempre que for solicitado. O serviço não pode ser interrompido (COMER, 2007).

### 2.2.2 Necessidade da Segurança da Informação

Segundo a norma ISO 27002, a informação, os sistemas, as redes e os processos de apoio à informação são ativos muito importantes para o negócio. Com o intuito de assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização perante ao mercado, as atividades de definir, alcançar, manter e melhorar a segurança da informação se tornam essenciais.

Pode-se perceber que a definição de segurança da informação definida pela norma está diretamente relacionada com a evolução das redes de computadores. Nos primórdios de sua existência ela era utilizada por apenas alguns tipos específicos de usuários. Em contrapartida com os dias de hoje ela está acessível a milhões de usuários de diversos tipos por todo o mundo e com acesso cada vez mais fácil e barato. Sendo assim, as ameaças que envolvem a informação são causadas em grande parte por esta interconexão.

A grande parte dos problemas enfrentados pela segurança é causada

por pessoas maliciosas que tentam obter algum benefício, chamar atenção ou prejudicar alguém. Dentre os invasores mais comuns estão estudantes que tentam se divertir, executivos que tentam descobrir a estratégia de marketing da concorrente e até mesmo terroristas que tentam obter segredos de órgãos governamentais para a sua atuação Devido a estes diversos tipos de usuários de redes de computadores por todo o mundo com os mais diversos anseios a segurança se tornou um fator inevitável para todos os tipos de usuários e organizações.

Órgãos governamentais devem ser ainda mais cautelosos com esta questão já que possuem informações que muitas vezes não foram e nem podem ser divulgadas ao público em geral. O impacto seria mundial se um terrorista obtivesse informações, por exemplo, a respeito da construção de armas bacteriológicas (TANEMBAUM, 2003).

Um caso recente e que se encaixa perfeitamente neste assunto é a existência do site *wikileaks*. Nele são publicados *posts* de fontes anônimas, documentos, fotos e informações confidenciais vazadas de governos ou empresas a respeito de diversos assuntos. Um caso que chamou a atenção foi o vazamento de milhares de documentos confidenciais por parte de um de seus soldados que atualmente se encontra preso e acusado por vinte e dois crimes pela justiça militar dos Estados Unidos da América. A informação se encontra em http://www.jb.com.br/wikileaks/noticias/2011/03/02/soldado-preso-que-colaborou-com-wikileaks-e-acusado-de-conluio-com-o-inimigo/ , acessada em 07/05/2011.

### 2.2.3 Impactos de incidentes de segurança

Com a utilização dos recursos computacionais para o armazenamento de informações ao invés do uso apenas de papéis, a segurança das informações contidas nestes recursos não se tornou uma tarefa simples e apenas de segurança física. As mudanças tecnológicas passaram para um patamar mais complexo, no qual não basta apenas a segurança física. A segurança lógica, também conhecida como controle de acesso lógico, apresenta medidas de segurança que devem sempre estar sendo atualizadas de acordo com a criação de novas tecnologias.

Os sistemas de informação, por sua vez, passaram a fazer parte das organizações e se tornou peça chave dentro delas. Sem os computadores e as redes de comunicação que atualmente conectam o mundo inteiro, a prestação

de serviços de informação pode se tornar inviável (TCU, 2007). Sendo assim, se um sistema de informação é afetado em um dos princípios de segurança da informação há conseqüências fortes para a organização. A figura 2 a seguir, ilustra o fluxo de um incidente de segurança e as suas conseqüências para uma organização.

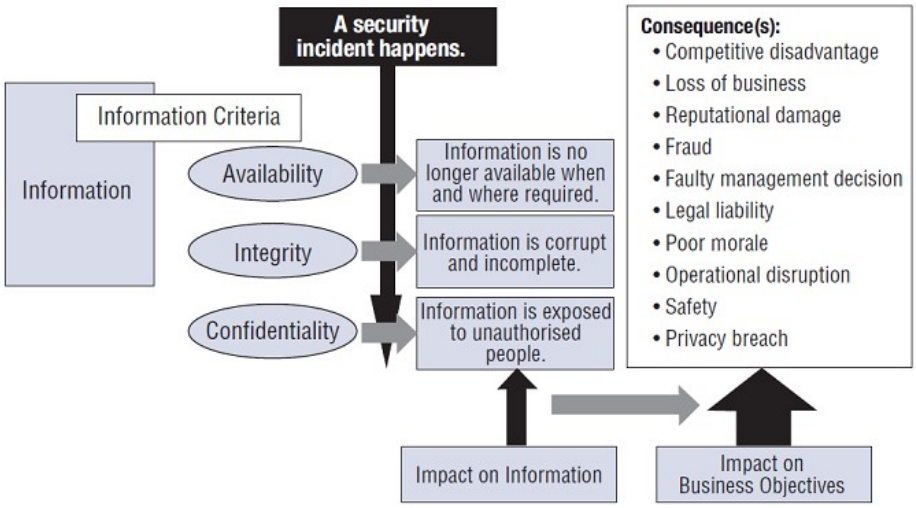


Figura – Incidente de Segurança

Detalhando o fluxo apresentado na figura 2, um incidente de segurança acontece quando um dos princípios da segurança da informação é violado. O impacto para a informação consiste nela não estar mais disponível, estar corrompida ou tendo seu acesso por pessoas não autorizadas. Por consequência deste impacto na informação da organização, um impacto nos objetivos de negócios também ocorre. Dentro deste impacto nos objetivos de negócio, as consequências geradas para a organização são: desvantagem competitiva, perda de negócios, perigo para a reputação, fraude, decisão de gerenciamento defeituosa, responsabilidade legal, perda de moral, rompimento de operações, segurança e violação de privacidade.

Segundo a norma ISO 27002, controle é a “forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal” e o risco é “a combinação da probabilidade de um evento e de suas conseqüências”. A fim de prevenir tais conseqüências, o processo de

segurança da informação deve estar implementado e ser frequentemente monitorado através de seus controles.

### 2.2.4 Estrutura do processo de segurança da informação

Quando se desejar criar um processo de segurança da informação, deve-se primeiramente analisar os riscos que envolvem cada parte da organização e encontrar soluções que minimizem ou eliminem tais riscos. Feito isso, a seleção de controles e implementação dos mesmos deve ser realizada. Com a criação dos controles, a organização consegue através dos responsáveis pelo monitoramento de cada controle descobrir como está a eficácia dos controles e da sua segurança como um todo. Em resumo, um processo de segurança da informação consistem num conjunto de controles relacionados à segurança da informação.

Nos dias atuais tem-se falado em governança corporativa e da segurança da informação. Uma definição proposta por Fontes (2008) é que governança "é a gestão da gestão". Portanto, para se ter uma governança da segurança da informação, primeiramente deve-se ter o processo de segurança da informação implementado dentro da organização com o seu conjunto de controles. Só a partir daí é possível analisar e avaliar a gestão da segurança da informação.

Os controles do processo de segurança da informação, quando em eficácia, preservam a confidencialidade, integridade e disponibilidade das informações dentro da organização. Outros princípios tais como responsabilidade, autenticidade e não repúdio podem ser utilizados na busca da segurança da informação (ISO 27002, 2005).

A seguir serão definidos tais princípios:

- **Autenticidade –** Consiste no processo de constatar a identidade de alguém. O acesso do usuário ao sistema só se dá mediante de senha ou alguma medida de identificação (KUROSE, 2003).

- **Responsabilidade** - Se refere aos requisitos de uma auditoria, ou seja, tem o foco nos responsáveis por cada item e a maneira como armazenam os registros de acesso e mudança (COMER, 2007).

- **Não Repúdio –** Consiste no fato de constatar que determinada pessoa realizou uma ação, ou seja, deve-se obter uma forma de provar que a pessoa realmente efetuou a ação e não poder negar o feito (FOROUZAN, 2006).

Sendo assim, deve-se analisar os riscos dentro do ambiente organizacional a fim de evitar as ameaças existentes, tanto físicas quanto lógicas.

## 2.3 Principais Ameaças

São diversos os tipos de ameaças que uma organização pode sofrer. Analisando a parte física, a organização pode sofrer conseqüências derivadas desde fenômenos da natureza até mesmo por funcionários que queiram se vingar. A fim de minimizar estes riscos, serão apresentadas ameaças físicas e lógicas que podem existir em um ambiente organizacional e quais medidas de segurança podem ser tomadas (TANEMBAUM, 2003).

### 2.3.1 Ameaças Físicas

O ambiente da organização, em sua maioria, é composto por salas, andares, escritórios, ambiente de produção e outros, dependendo do ramo de atuação. Como são inúmeras as ameaças que podem ocorrer e o foco do trabalho não está em sua listagem, citaremos apenas algumas apontadas por Fontes (2008) e Tanembaum (2003).

- Incêndio,
- Água (enchentes, vazamentos e outros),
- Tremores e abalos sísmicos,
- Roubo,
- Interrupção de energia,
- Interrupção de comunicação,
- Falhas em Equipamentos.

### 2.3.2 Ameaças Lógicas

Como os computadores passaram a armazenar, processar e criar informações, o seu acesso também passou a ser controlado. Algumas das ameaças que podem ocorrer no ambiente de redes de computadores é apresentado a seguir.

#### Códigos Maliciosos

O Centro de Estudo, resposta e tratamento de Incidentes de segurança no Brasil, conhecido como CERT, fornece de forma gratuita uma cartilha de segurança para Internet para os interessados. A cartilha possui recomendações e dicas para o usuário melhorar a sua segurança na Internet. Ela apresenta de forma clara os termos, conceitos utilizados na Internet e fornece procedimentos que visam o aumento da segurança. Exemplos de códigos maliciosos fornecidos pela cartilha e seus significados são apresentados a seguir:

- **Vírus**: Programas ou partes de programas que se propagam infectando computadores. Normalmente maliciosos, inserem cópias de si mesmo e se tornam parte de outros programas e arquivos do computador. Para se tornar ativo e continuar o processo de infecção o

vírus necessita da execução do progama ou arquivo hospedeiro.

- ***Backdoor****:* Após o sucesso na invasão através dos métodos utilizados pelo invasor, na maioria das vezes o atacante procura garantir um meio de retorno ao ambiente comprometido. *Backdoor* é o termo usado aos programas que possibilitam o retorno do invasor ao ambiente através do uso de serviços criados ou modificados. Em grande parte das vezes acontece sem que o atacante seja notado .

- ***Worms****:* Denominação dada para programas que possuem a capacidade de se propagar enviando cópias de si mesmo de computador para outro computador através de redes de computadores. Ao contrário do vírus, estes programas não embutem cópias de si mesmo em outros programas e arquivos e não dependem da execução para se tornarem ativos. Através da exploração das vulnerabilidades ou falhas de configuração de softwares instalados em computadores é que se dá a sua propagação.

- **Bots**: O Bot se assemelha muito ao worm. Ele possui características de propagação automática e exploração de vulnerabilidades ou falhas de configuração. O que gera o diferencial entre os dois é que o bot apresenta mecanismos de comunicação com o invasor permitindo que este seja controlado remotamente.

- **keyLogger**: é um programa com a capacidade de capturar e armazenar as teclas digitadas no teclado de um computador pelo usuário.

- **Cavalos de Tróia**: O nome do programa surgiu da analogia com a mitologia grega, na qual conta que o "cavalo de tróia" foi uma grande estátua que serviu como arma para a conquista da cidade de Tróia pelos gregos. A estátua que seria um presente, na verdade era um disfarce para a entrada de soldados escondidos no seu interior.

  Esta analogia, no campo da informática, indica um programa que é geralmente recebido como "presente". O presente pode ser em forma de cartão virtual, álbum de fotos, protetor de tela e outros como jogos. Este programa imita a estátua da mitologia ao executar

funções para as quais foi projetado. Porém, assim como os soldados, executa funções que em sua maioria são maliciosas e sem o conhecimento do usuário. As funções do cavalo de tróia podem ser a instação de *keylogger*, furto de senhas e outras informações sensíveis como cartões de crédito, insclusão de backdoors e alteração ou destruição de arquivos.

- **Adwares e Spywares**: *Adwares* são um tipo de software projetado com o intuito de apresentar propagandas ao usuário de alguma forma. Geralmente utiliza-se o browser para isso, mas programas instalados no computador também podem apresentar esse comportamento.

  *Spyware*s é a denominação utilizada para se referir a uma grande categoria de *software* cujo objetivo está no monitoramento das atividades de um sistema e envio das informações coletadas para terceiros. Pode ser utilizados de forma legítima, mas na grande parte dos casos a sua forma é não autorizada e maliciosa.

  Algumas vezes um *adware* pode ser considerado um spyware pelo fato de monitorar o usuário durante a navegação na Internet com o intuito de lhe apresentar as propagandas que causariam maior interesse.dentre as funções de um spyware pode-se incluir o monitoramento de URLs, alteração da página inicial do navegador, varredura de arquivos armazenados no disco rígido do computador, monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto, instalação de outros spywares, monitoramento de teclas digitadas pelo usuário e captura de senhas.

  Este tipo de programa compromete a privacidades e a segurança do computador do usuário. Se este computador pertence a uma empresa, compromete a segurança da informação da empresa. Deve-se ficar atento para a existência dos mesmos dentro de uma organização pois não se sabe quais informações são monitoradas e enviadas para terceiros .
- **Rootkits** : Para assegurar a presença de um invasor em um ambiente comprometido, utiliza-se mecanismos para esconder o feito. O conjunto de programas que limpam os rastros de um atacante no ambiente é conhecido como *rootkit*. Utiliza-se as ferramentas para

manter o acesso já obtido no sistema. Após a instalação deste rootkit, o atacante terá acesso privilegiado ao computador comprometido sem necessitar de reutilizar os métodos usados para obter o acesso ao computador. Esse conjunto de ferramenta esconde as suas atividades no computador dos responsáveis.

**Ataques**

A seguir serão apresentados alguns tipos de ataque com o intuito de demonstrar alguns riscos que os usuários podem enfrentar.

- **Negação de serviço**

Neste tipo de ataque, o atacante utiliza um computador para tirar do ar um serviço ou um computador conectado à Internet.

- **Spam**

Spam é a denominação para correios eletrônicos não solicitados encaminhados para um grande número de pessoas. Os usuários de correio eletrônico podem enfrentar diversos problemas com este ataque. Um deles é o não recebimento de correios eletrônicos devido ao enchimento da sua caixa de entrada, que geralmente, possuem um tamanho fixo. Outros problemas estão a perda de tempo para deletá-los, perda de produtividade e até prejuízos financeiros, já que atualmente são muito utilizados para disseminar esquemas fraudulentos que tentam induzir os usuários a atitudes maliciosas. Este ataque pode ser realizado aumentando o processamento do computador, aumentando o tráfego de dados para uma rede ou tirando do ar serviços importantes que deixem usuários de correio eletrônico impossibilitados de acessar o servidor de correio eletrônico (CERT, 2006).

- **Interceptação de pacotes ( *Man-in-the-Middle* )**

O ataque em questão envolve uma pessoa  interceptando uma conversa entre duas pessoas. Como exemplo, uma pessoa fictícia A envia uma mensagem a pessoa fictícia B. Uma pessoa má intencionada, denominada por C, coloca a sua placa de rede em modo promíscuo e passar a servir de analisador de pacotes dentro da rede. Sendo assim, todos os quadros

que estão sendo transmitidos para todos hospedeiros são recebidos por C. Deste modo, C pode se passar por uma das pessoas, A ou B, e obter informações confidenciais (KUROSE, 2003).

### 2.3.3 Ameaças em Recursos Humanos

A segurança não é obtida apenas com recursos lógicos e físicos. A segurança consiste em um conjunto de medidas que quando associadas garantem uma segurança satisfatória para alguém ou organização. Sendo assim, as pessoas também devem ser levadas em consideração.

- **Engenharia Social**

Baseado na persuasão, no abuso da ingenuidade ou da confiança de alguma pessoa, o atacante tenta obter informações nas quais ele possa utilizar para obter acesso não autorizado a computadores ou informações.

O atacante pode utilizar de diversos métodos para obter a informação. Um exemplo deste método seria o envio de emails falsos com *links* que redirecionam o alvo para páginas falsas semelhantes às oficiais do banco. Com a inserção dos dados no site falso pelo alvo o atacante obtém os seus dados e os utiliza de modo malicioso. Além de métodos técnicos com o uso de estórias que levam o usuário a cair em armadilhas, existem métodos que o usuário obtém acesso à informações privilegiadas por telefone. Em suma, este método consiste em criar situações através de mentiras para obter informações privilegiadas que possam levar o atacante a obter alguma vantagem disto (cert, 2006).

## 2.4 Controle de Acesso

A maioria das ameaças listadas acima está relacionada com o acesso indevido à informação. Para combater estas ameaças e tentar minimizar a chance de ocorrência de alguma delas, técnicas de segurança tanto física quanto lógicas foram criadas.

### 2.4.1 Medidas de Segurança Física

A seguir, serão apresentadas algumas medidas relacionadas às ameaças físicas apresentadas.

- **Biometria**

A leitura biométrica consiste na identificação dos funcionários de uma empresa através da utilização de características próprias dos indivíduos. O usuário precisa ter a sua digital cadastrada no aparelho. Além disso, uma senha pode ter que ser informada para a liberação do funcionário. A segurança de acesso físico com o controle de funcionários é garantida ().

- **Geradores e No-Break**

No-break é a denominação para um aparelho constituído de baterias, normalmente próximas umas das outras, que possuem a finalidade de armazenar energia e alimentar um computador por alguns minutos caso haja falta de energia. Assim, o usuário ao detectar a falta de energia obtém tempo de salvar e fechar os arquivos abertos. Isso evita que o equipamento se danifique com a queda repentina de energia e que o usuário perca dados.

Geradores são dispositivos que convertem energia mecânica, química ou outra forma de energia em energia elétrica. Desta forma, quando há interrupção no fornecimento de energia, o gerador é acionado e garante o funcionamento do estabelecimento durante um período de tempo. Este tipo de dispositivo é muito utilizado em hospitais e outros locais em que a falta de energia não pode ocorrer (MULLER; NETTO; PEREIRA, 2010).

### 2.4.2 Medidas de Segurança Lógica

A seguir serão apresentadas possíveis medidas para combater o acesso lógico indevido. As medidas foram baseadas no *checklist* da cartilha de segurança na Internet proposto pelo Centro de Estudo, Resposta e Tratamento de incidentes de segurança no Brasil.

- **Senhas**

Para evitar o acesso de outra pessoa com a sua identificação no sistema deve-se atentar em alguns aspectos relativos à construção, armazenamento e rotatividade da mesma (CERT, 2006). O checklist proposto pelo cert.br sugere os seguintes procedimentos:

- Elaborar senhas que contenham no mínimo oito caracteres, compostos por números, letras e símbolos.

- Nunca utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, telefones ou datas que possam ser relacionadas com você ou encontradas em dicionários

- Utilizar uma senha diferente para cada serviço. Evita que o atacante ao descobrir uma senha obtenha acesso a todos os seus serviços.

- Alterar a senha com certa frequência

- Criar o número de usuários que possuem privilégios normais igual ao número das pessoas que utilizam seu computador.

- Utilizar o privilégio de Administrador (ou root no linux) somente quando for estritamente necessário.

- **Backup**

A realização de cópias de segurança dos dados armazenados no computador são importantes para se proteger de conseqüências resultantes de invasões ou infecção por vírus. É um procedimento que também possibilita a recuperação dos dados devido a eventuais falhas de sistemas ou *softwares* (cert, 2006). O checklist proposto pelo cert.br sugere os seguintes procedimentos:

- Realização de cópias dos dados do computador com certa regularidade

- Criptografar dados sensíveis

- Armazenas as cópias dos dados em local de acesso restrito e com segurança física

- Considerar a necessidade de armazenamento das cópias em um local fora da organização

- **Criptografia**

O uso da criptografia evita que pessoas obtenham acesso à informação que não estão autorizadas e consigam ler ou entendê-la. A criptografia pode ser utilizada tanto em arquivos quanto em canais de comunicação. Dentre os objetivos da criptografia estão a autenticação da identidade do usuário, autenticação e proteção do canal de comunicação e garantia da integridade de transferências eletrônicas de fundos (cert, 2006).

- **Antivírus**

Os antivírus são programas que possuem como objetivo a detecção, anulação ou remoção de vírus do computador. Adicionalmente aos antivírus atuais, funcionalidades para prevenção contra cavalos de tróia e outros códigos maliciosos também tem sido incorporadas (cert, 2006).

- **Firewall**

Os firewals são dispositivos constituídos pela combinação de hardware e software que limitam e controlam o acesso entre redes de computadores. Um firewall bem configurado pode impedir o acesso de um atacante a uma *backdoor* instalada no ambiente. O antivírus não consegue fazer isto. Além disso, pode identificar a origem de tentativas de ataque assim como possibilitar o seu bloqueio. Em resumo, em relação à segurança, nenhum ambiente está seguro com a utilização de apenas um recurso. Deve-se tentar obter esforços complementares como é o caso da utilização de antivírus e firewalls ao mesmo tempo. O ditado popular “a união faz a força” se encaixa perfeitamente no conceito de segurança (cert, 2006).

- **Vulnerabilidades**

Alguns softwares instalados no computador podem apresentar falhas de segurança que podem ser exploradas por atacantes através da utilização de algum software de scanner de rede. Sabendo disso, existem sites que contém uma lista de vulnerabilidades em softwares e sistemas operacionais. O

usuário deveria olhar com certa freqüência esses sites com o intuito de evitar que a falha seja descoberta primeiramente pelo atacante (cert, 2006). Alguns desses sites são:

- http://www.cert.org/
- http://cve.mitre.org/
- http://www.us-cert.gov/cas/alerts/.

Um aspecto interessante na segurança é que, para se descobrir se o seu sistema está seguro, você deve testá-lo antes que uma outra pessoa faça.

### 2.4.3 Medidas de Segurança em Recursos Humanos

As medidas de segurança em recursos humanos está relacionada às pessoas que trabalham ou colaboram de alguma forma com a organização. As pessoas, como dito neste trabalho, é um ativo essencial para a organização.

O treinamento dos usuários tem o objetivo de informar aos funcionários novos e antigos as regras da organização, políticas que devem ser seguidas e leis. Com isto, a organização define um comportamento aceitável para as pessoas dentro da organização e minimiza as chances do ataque de engenharia social. A continuidade do negócio é o maior ganho para a empresa que fornece treinamentos para os usuários.

Algumas medidas propostas pelo checklist proposto pelo cert são as seguintes:

- Nunca fornecer dados pessoais como números de cartões e senhas através de contato telefônico.
- Estar sempre atento a e-mails ou telefonemas solicitando dados pessoais.
- Não acessar sites ou seguir links recebidos por e-mail ou presentes em páginas sobre as quais não se tenha certeza da procedência.
- Sempre que houver receio sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com as instituição

em questão para verificar a veracidade dos fatos.

## 2.5 ISO 27002:2005

O Brasil apresenta uma norma de segurança denominada por NBR ISO/IEC 27002. O conteúdo desta norma é equivalente ao da norma ISO/IEC 17799, elaborada no Comitê Brasileira de Computadores e Processamento de Dados pela Comissão de Estudo em Segurança Física em Instalações de Informática.

### 2.5.1 Estrutura da norma

A norma apresenta em sua estrutura 11 seções de controles de segurança da informação. Dentro de cada seção existem categorias. Ao todo existem 39 categorias principais de segurança e uma seção introdutória que aborda a análise e o tratamento de riscos. As seções são apresentadas a seguir:

1. Política de Segurança da Informação
2. Organizando a Segurança da Informação
3. Gestão de Ativos
4. Segurança em Recursos Humanos
5. Segurança Física e do Ambiente
6. Gestão das Operações e Comunicações
7. Controle de Acesso
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
9. Gestão de Incidentes de Segurança de Informação
10. Gestão da Continuidade do Negócio
11. Conformidade

Dentro de cada seção, existirá um número variável de categorias que compõem a seção em questão. Sendo assim, cada categoria terá a estrutura a seguir:

1. Um objetivo de controle – Será utilizado como um guia para o objetivo a ser alcançado pela categoria.

2. Um ou mais controles – Estes, por sua vez, poderão ser utilizados

com o intuito de obter o objetivo principal.

A seguir será apresentada as descrições existentes dentro dos controles:

1. Controle – O controle específico para atender o objetivo em questão será fornecido.

2. Diretrizes para a implementação - Informações detalhadas para auxiliar no processo de implementação do controle serão fornecidas. Tais informações atendem ao objetivo de controle. Pode existir casos em que algumas diretrizes não serão adequadas para a organização em questão. Portanto, outras diretrizes podem ser usadas. Cabe à pessoa que estiver utilizando a norma como base ter este olhar crítico.

3. Informações Adicionais – Informações que podem ser úteis no processo são relatadas. Normalmente são informações relacionadas a outras normas ou questões de legislação a serem consideradas.

### 2.5.2 Requisitos de Segurança da Informação

Um fator importante para a organização é a identificação dos seus requisitos de segurança da informação. As fontes principais para a obtenção deles são as três a seguir:

1. Análise de riscos para a organização, levando em conta objetivos e estratégias globais de negócio da organização. Por esta fonte, as ameaças aos ativos e as vulnerabilidades são identificadas. Uma avaliação da probabilidade da ocorrência das ameaças e o impacto para o negócio é realizada.

2. Legislação vigentes, estatutos, regulamentação e cláusulas contratuais que a organização, seus parceiros comerciais e provedores de serviço têm que atender além do seu ambiente sociocultural.

3. Conjunto particular de princípios, objetivos e requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para auxiliar as suas operações.

### 2.5.3 Analisando/Avaliando os Riscos de Segurança da Informação

Através da análise/avaliação sistemática dos riscos de segurança da informação, os requisitos de segurança da informação são identificados. Os gastos com os controles pela organização precisam ser coerentes com os possíveis danos que possam ocorrer com as potenciais falhas identificadas.

Com o resultado da análise dos riscos, aspectos importantes para a sua gerência ficam mais claros. Deste modo, ações gerenciais, prioridades de gerenciamento de riscos e seleção de controles a serem implementados para garantir a proteção são realizados com maior eficiência.

### 2.5.4 Seleção dos Controles

Após a avaliação dos riscos e a identificação dos requisitos de segurança da informação, a seleção dos controles adequados se torna possível. Os controles selecionados e implementados garantem que os riscos de segurança passem a existir em um nível aceitável.

Pode-se considerar alguns controles desta norma como princípios fundamentais para a gestão da segurança da informação. Um dos motivos para esta consideração é a possibilidade de implementação na maioria das organizações.

Os controles considerados essenciais para a organização são os três a seguir:

1. Proteção de dados e privacidade de informações pessoais
2. Proteção de registros organizacionais
3. Direitos de propriedade intelectual

Os controles que são considerados práticas para a segurança da informação são descritos a seguir:

1. Documento da política da informação
2. Atribuição de responsabilidades para a segurança da informação

3. Conscientização, educação e treinamento em segurança da informação
4. Processamento correto nas aplicações
5. Gestão de vulnerabilidades técnicas
6. Gestão da continuidade do negócio
7. Gestão de incidentes de segurança da informação e melhorias

Como o foco deste trabalho está na infraestrutura, será apresentada duas seções da norma ISO:IEC 27002. A primeira refere-se à segurança física da organização, enquanto a outra se relaciona com a segurança lógica. As seções serão apresentadas a seguir .

### 2.5.5 Segurança Física e do Ambiente

O objetivo desta seção é tentar reduzir ao máximo problemas relacionados com as instalações da empresa. Assim, a empresa estará mais preparada contra possíveis inconvenientes e mais segura em diversos aspectos físicos que possam gerar prejuízos à organização.

A seção de Segurança Física e do Ambiente é dividida em Áreas Seguras com a prevenção ao acesso físico sem autorização, danos e interferências com as instalações Segurança de equipamentos, que se atenta a impedir perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização.

**Áreas Seguras**

A. Perímetro de Segurança Física
   *Objetivo*: Utilização de perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação.

B. Controles de Entrada Física
   *Objetivo:* Assegurar o acesso somente às pessoas autorizadas através de controles apropriados de entrada.

C. Segurança em escritórios, salas e instalações
*Objetivo:* Aplicar a segurança física também aos outros locais da organização.

D. Proteção contra ameaças externas e do meio ambiente
*Objetivo:* Aplicar proteção física contra incêndios, enchentes, terremotos, explosões, perturbações de ordem pública ou outras formas de desastres naturais ou causados pelo homem.

E. Trabalhando em áreas seguras
*Objetivo:* Projeto e aplicação da proteção física, bem como diretrizes para o trabalho em áreas seguras.

F. Acesso do público, áreas de entrega e carregamento
*Objetivo:* Locais em que pessoas não autorizadas possam entrar na organização sejam controlados e , se possível, isolar das instalações de processamento de informação a fim de evitar o acesso não autorizado.

**Segurança de Equipamentos**

A. Instalação e proteção do equipamento
*Objetivo:* Colocar o equipamento em local seguro a fim de reduzir o risco de ameaças e perigos do meio ambiente. Adicionalmente, limitar ainda mais o acesso não autorizado.

B. Utilidades
*Objetivo:* Proteger equipamentos contra a falta de energia elétrica e outras interrupções causadas por falta de utilidades.

C. Segurança do cabeamento
*Objetivo:* Proteção de cabeamento de energia e telecomunicações contra a interceptação ou danos.

D. Manutenção dos equipamentos

*Objetivo:* Estabelecer uma manutenção correta dos equipamentos a fim de garantir sua disponibilidade e integridade permanentes.

E. Segurança de equipamentos fora das dependências da organização

*Objetivo:* Tomar medidas de segurança para com os equipamentos que operem fora da organização levando em considerações os diversos riscos que podem ocorrer.

F. Reutilização e Alienação segura de equipamentos

*Objetivo:* Examinar equipamentos que contenham mídia de armazenamento de dados antes do descarte com o intuito de assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobrepostos com segurança.

G. Remoção de propriedade

*Objetivo:* Equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

### 2.5.6 Controle de Acesso

A. Requisitos de negócio para controle de acesso

Objetivo: Controlar acesso à informação

B. Gerenciamento de acesso do usuário

Objetivo: Assegurar o acesso do usuário e prevenir o acesso não autorizado aos sistemas de informação

C. Responsabilidade dos usuários

Objetivo: Evitar o comprometimento ou o roubo de informações e recursos de processamento de informações. Também objetivo a prevenção contra o acesso não autorizado.

D. Controle de acesso à rede

Objetivo: Prevenir o acesso não autorizado aos serviços de rede

E. Controle de acesso ao sistema operacional

Objetivo: Prevenir o acesso não autorizado aos sistemas

operacionais

F. Controle de acesso à aplicação e à informação
   Objetivo: Prevenir o acesso não autorizado à informação contida nos sistemas de aplicação

G. Computação móvel e trabalho remoto
   Objetivo: Garantir a segurança da informação quando utilizar a computação móvel e recursos de trabalho remoto.

A seguir, o capítulo 3 abordará a metodologia utilizada no trabalho.

# 3 METODOLOGIA

Este capítulo descreve a metodologia usada no trabalho e que possibilitou que fossem alcançados os objetivos da pesquisa. Na primeira seção será apresentada a classificação da pesquisa quanto à natureza, ao objetivo e aos procedimentos. Em seguida serão descritos os procedimentos metodológicos da pesquisa.

## 3.1 **Tipo de pesquisa**

Quanto à natureza da pesquisa, ela pode ser caracterizada como aplicada ou tecnológica, pois tem como finalidade aplicar conhecimentos adquiridos durante o curso e formular um nova configuração para o processo de segurança da informação dentro da empresa em questão. Baseando-se no objetivo geral da pesquisa do projeto, ela pode ser considerada como descritiva, pois visa observar, registrar e analisar os fenômenos registrados em simulações na ferramenta *OPNET IT Guru Academic Edition* e no guia de boas práticas para a segurança da informação.

Quanto aos procedimentos, a pesquisa é considerada um estudo de caso, pois trata da investigação de um fenômeno dentro de um contexto real. Entende-se por pesquisa em campo aquela em que não se pode controlar as variáveis possíveis. Trata-se de ambientes reais onde ocorrem os fenômenos (ZAMBALDE; PADUA; ALVES, 2008). A aquisição de referências foi realizada por meio de procedimentos de pesquisa bibliográfica e documental.

## 3.2 **Procedimentos metodológicos**

A pesquisa possui basicamente duas etapas. A primeira delas é a obtenção dos requisitos essenciais para o desenvolvimento e evolução do trabalho. Nesta etapa ocorreu a definição do assunto abordado, a pesquisa bibliográfica e a análise da documentação encontrada, permitindo a aquisição de conhecimentos sobre a segurança da informação e redes de computadores. A segunda etapa é a implementação e avaliação dos resultados obtidos a partir da criação de cenários a respeito da rede de computadores da empresa no simulador de redes de computadores OPNET IT Guru Edition. A partir dos resultados das simulações, um cenário será proposto a fim de melhorar a segurança da informação dentro da empresa alvo. O guia de boas práticas para a segurança da informação irá fornecer a direção da avaliação e levantamento de dados a respeito do processo de segurança da informação e sua posterior atualização. Baseado no método de

avaliação proposto por FONTES, será efetuada a avaliação da empresa no aspecto da infraestrutura.

## 3.3 **Processo de Simulação**

A simulação tem como objetivo principal reproduzir uma situação do mundo real e, com base no modelo desenvolvido, realizar experiências e testes como intuito de avaliar e compreender melhor o comportamento de um determinado sistema (ALBERTI; MENDES; NETO, 1999). A simulação de redes de comunicação pode ser feita por três tipos de *softwares* de simulação: linguagens de simulação de propósito geral, linguagens de simulação orientadas às redes de comunicações e simuladores orientados às redes de comunicações (LAW; MCCOMAS, 1994). Uma linguagem de simulação de propósito geral é definida como um conjunto de simulação, que na teoria, pode ser usada em qualquer tipo de sistema. No entanto, algumas dessas linguagens possuem características especiais para redes de comunicação, como módulos para *Ethernet* , redes sem fio e outras. Pode-se citar como exemplos dessas linguagens de simulação: Arena (HAMMAN; MARKOVITCH, 1995) e BONeS DESIGNER (COMDISCO SYSTEMS, INC., 1993). As linguagens de simulação orientadas às redes de comunicação possuem como benefício a oportunidade de redução do tempo de programação e modelagem das construções voltadas para as redes de comunicação. O OPNET Modeler (SVENSSON; POPESCU, 2003) e o GNS (GNS3, 2009) destacam-se como exemplos deste tipo de software. Por outro lado, os simuladores orientados às redes de comunicação são softwares que possibilitam a simulação de uma classe específica de redes de comunicação. A facilidade de uso e a possibilidade de reduzir o tempo e a complexidade quanto à criação dos modelos são algumas das vantagens apresentadas por esse tipo de simulador. Como exemplos deste tipo de simulador, pode-se destacar: NIST (GOLMIE; KOENIG;1995) e QUARTS-II (SIVABALAN; MOUFTAH, 1998).

## 3.4 **Modelagem de redes de computadores**

Modelagem consiste no processo de criação de modelos de sistemas reais em um ambiente específico de simulação, de forma que eles representem do modo mais fiel possível o comportamento desses sistemas diante de determinadas situações. Dentro de um contexto característico, por

exemplo, segurança da informação, a modelagem é uma tarefa que não exige apenas o conhecimento do ambiente de simulação para o qual está se criando os modelos, mas também conhecimento teórico a respeito de segurança da informação. É importante se ter em mente, a diferença entre emulação e simulação. A emulação tem como propósito a imitação da rede, inserindo todos os detalhes envolvidos. Por outro lado, a simulação tem o propósito da obtenção de resultados estatísticos que descrevam a operação dessas redes de computadores. Deste modo, precisa-se de representar apenas as funcionalidades necessárias, cujos detalhes são importantes de acordo com as estatísticas de interesse. Não é necessário representar todas as funcionalidades envolvidas (ALBERTI; MENDES; NETO, 1999).

## 3.5 **A Ferramenta de simulação OPNET Modeler**

O *OPNET Modeler* é uma ferramenta de simulação desenvolvida pela OPNET Technology Inc. Esta ferramenta proporciona um ambiente virtual para modelagem, análise e prognóstico de desempenho de infraestruturas de TI, incluindo aplicações, servidores e tecnologias de redes de computadores. Este software é usado por governos, universidade e milhares de empresas por todo o mundo. A sua interface é amigável, oferece recursos gráficos e permite a criação de cenários de simulação de redes, nós, enlaces, sub-redes, protocolos, equipamentos e serviços (SVENSSON; POPESCU, 2003). A versão do software escolhida para criar cenários, simular e analisar resultados foi a versão OPNET *IT Guru Academic Edition* 9.1.A (Build 1998), destinada para fins acadêmicos. A escolha deste software se deu pelo fato de possuir um conjunto de ferramentas com os requisitos necessários e não exigir uma máquina de alto desempenho.

## 3.6 **Topologia**

A empresa em questão, utiliza o modelo cliente/servidor. Este modelo é amplamente utilizado nas aplicações e serviços de rede e constitui a base de grande utilização das redes. Sendo assim, os cenários foram desenvolvidos representando este modelo (TANEMBAUM, 2003). A Figura X.X ilustra uma rede local que se baseia no modelo cliente/servidor.

Os cenários construídos no OPNET têm por objetivo representar da maneira mais fiel possível a situação atual da rede de computadores da empresa. A figura 14 apresenta um esquema de modelo cliente/servidor.

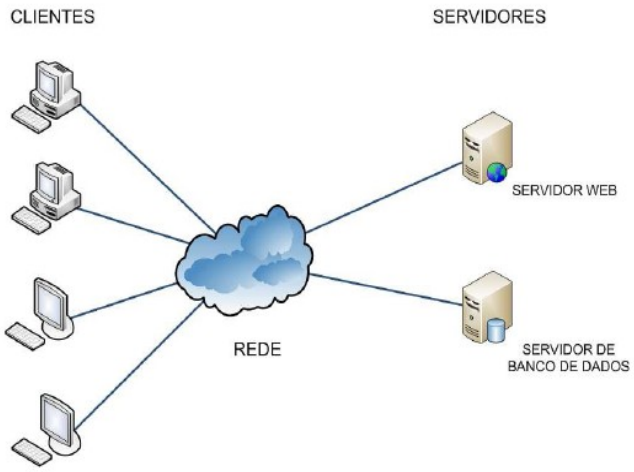


Figura  Rede de computadores utilizando o modelo cliente/servidor

## 3.7 **Definição das métricas e das aplicações**

As métricas que serão utilizadas no processo de simulação das redes de computadores da empresa para uma posterior comparação entre os cenários são as listadas a seguir:

- Latência
- Tráfego recebido nos switches

Foram utilizadas as seguintes aplicações no processo de simulação:

- HTTP
- Email
- Banco de Dados

Cada aplicação pode ser configurada com um dos três tipos de carga: *High Load*(carga alta), *Medium Load* (carga média) ou *Low Load*(carga baixa).

## 3.8 **Questionário QBASI**

O QBASI (Questionário Básico de Avaliação da Segurança da

Informação) é constituído por 123 questões relacionadas à segurança da informação dentro de uma organização. Neste trabalho, utilizaremos apenas as perguntas relacionadas à segurança lógica, física e de recursos humanos. Isto se deve ao fato de estarem relacionados à infraestrutura, objetivo principal do trabalho.

O questionário consiste em algumas perguntas propostas por Fontes, na qual o avaliador irá dar uma nota para cada pergunta baseando-se no padrão de avaliação a seguir.

| Notas | Significado |
|---|---|
| 0 | Não se aplica |
| 1 | Resposta : Não |
| 2 | Solução em planejamento inicial |
| 3 | Está planejada a implantação da solução |
| 4 | Parcialmente Implementada. Instável. Ainda não confiável |
| 5 | Possui o mínimo de atendimento aos requisitos |
| 6 | Prestes a ser melhorada |
| 7 | Quase totalmente implementada. Satisfatório para situações normais |

| | |
|---|---|
| 8 | Está funcionando bem |
| 9 | Totalmente implementada |
| 10 | Solução implementada é referência de mercado (melhor da classe) |

Tabela 2 – Padrão de avaliação do QBASI proposto por Fontes

Com o resultado dessa avaliação, a empresa saberá em um nível básico, como está a sua segurança em determinado aspecto. Esta avaliação será um complemento aos riscos identificados através da simulação.

A seguir, o capítulo apresenta o levantamento de dados efetuado na empresa. Neste levantamento de dados tanto informações relacionadas à topologia da rede de computadores quanto a aspectos relacionados à conservação dos recursos computacionais foram obtidas.

# 4 LEVANTAMENTO DE DADOS E MAPEAMENTO DA REDE DE COMPUTADORES

Para obtermos uma melhor análise da segurança da informação dentro da organização foi efetuado o mapeamento da rede de computadores. Com este passo, detalhes como topologia e localização de recursos foram obtidos.

A empresa em questão possui instalações em quatro andares de um prédio, e uma instalação em outro prédio, situados em Belo Horizonte - MG e Lavras - MG, respectivamente.

## 4.1 Mapeamento da rede de computadores da Empresa

A seguir serão apresentadas as figuras que ilustram a rede de computadores atual da empresa. Os quadrados que apresentam a letra ‘s’ dentro representam os *switches*, e os que apresentam a letra ‘r’ representam roteadores. Inicialmente, as figuras apresentadas correspondem aos andares da organização em Belo Horizonte–MG. Este ambiente apresenta dezenove cômodos.

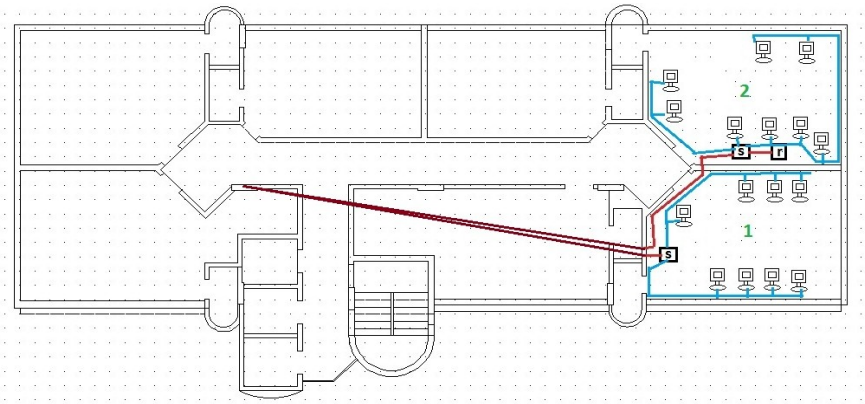


Figura - Terceiro Andar – BH

O terceiro andar é um dos últimos andares adquiridos pela empresa. A empresa possui apenas duas salas dentro do mesmo. Devido à necessidade de

mudança rápida da empresa, não houve muito planejamento da rede

de computadores do andar. Constatou-se a existência de roteadores e switches no chão sem nenhuma proteção e cabos de rede espalhados pelo chão.

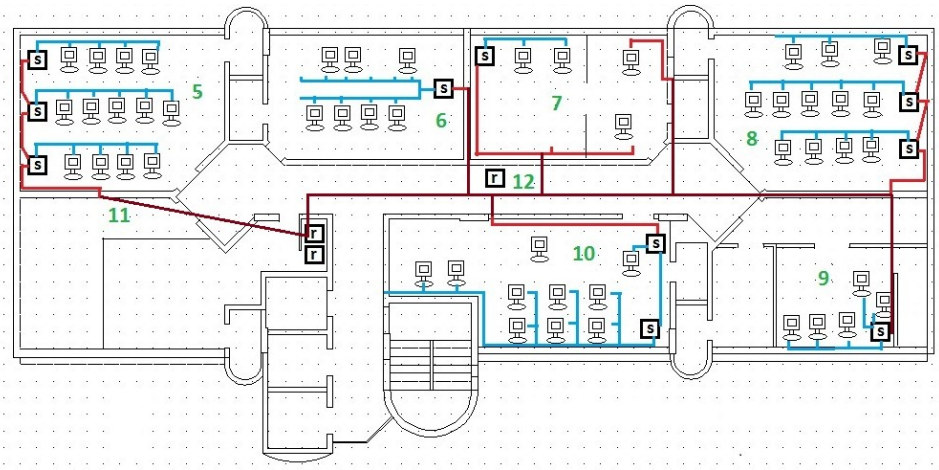


Figura - Sétimo Andar – BH

O sétimo andar é o andar principal em relação à rede de computadores. O serviço de Internet chega na sala 11 da figura. A empresa contrata dois serviços de Internet para que caso algum dos provedores de serviço de internet esteja com problema, o outro assuma a demanda. Nesta sala a rede de computadores se inicia e se divide para todos os outros três andares da empresa. Neste andar os cabos de rede estão encapados e os switches melhor posicionados do que no terceiro, mas ainda assim, sem muita proteção.

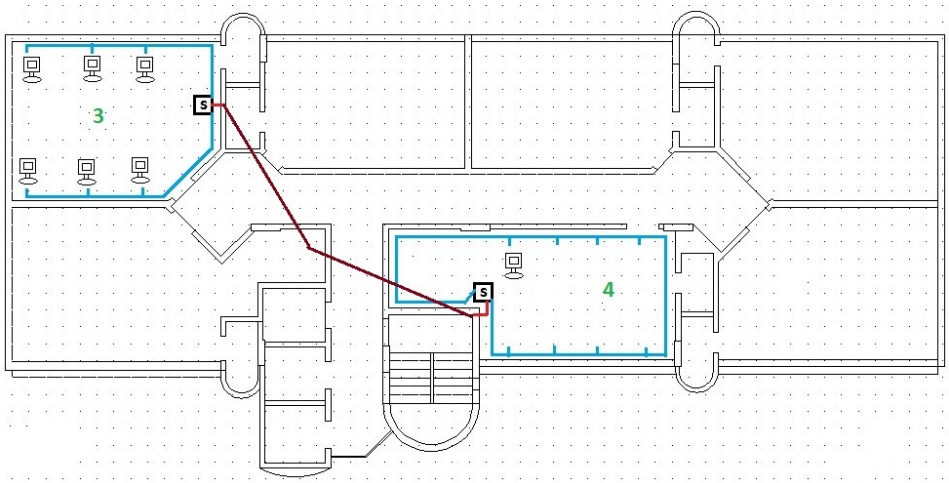


Figura - Oitavo Andar – BH

O oitavo andar, assim como o terceiro, apresenta apenas duas salas. Notou-se que na sala 4, a última adquirida do andar, o switch estava no chão.

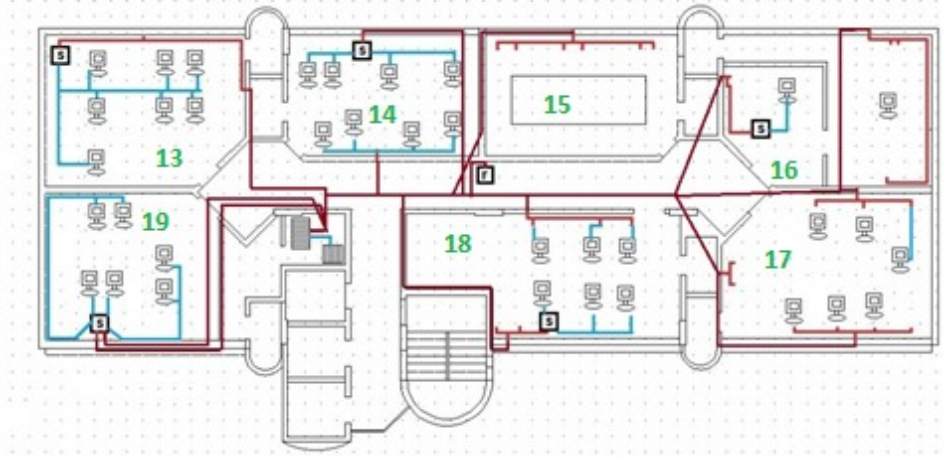


Figura - Décimo Segundo Andar – BH

O décimo andar é um andar muito importante para a empresa. Neste andar se localizam os servidores. Como a planta é a mesma para todos os andares, a localização dos switches se assemelha à de chegada do serviço de Internet do sétimo andar. A sala possui acesso restrito com o uso de chaves e apresenta ar condicionado para conservar os recursos computacionais. Há a

existência de um mecanismo contra incêndio dentro da sala. Mas mesmo que este seja acionado, os recursos podem ser comprometidos pelo jato de água. Notou-se a necessidade de uma melhora no mecanismo.

A figura 7 a seguir corresponde ao primeiro andar da organização em Lavras-MG.

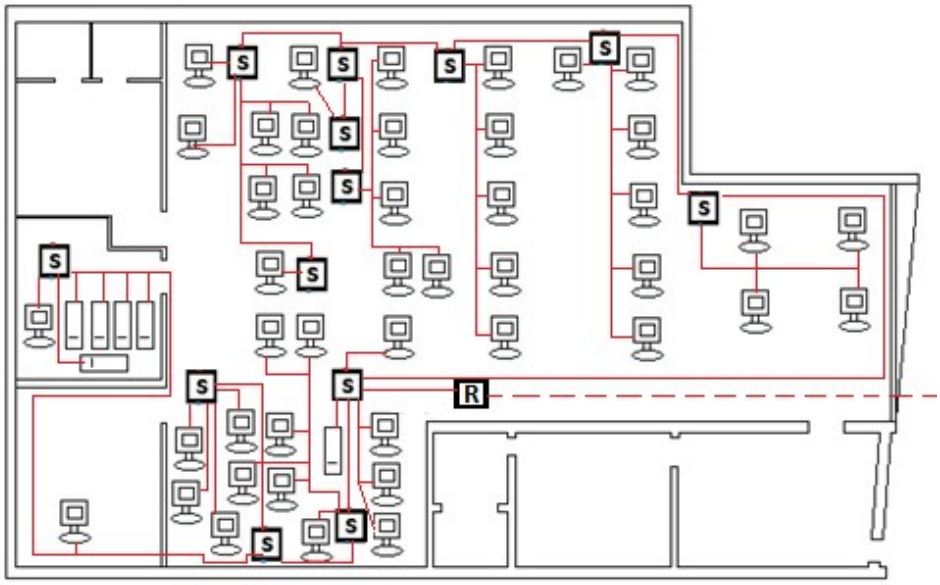


Figura - Primeiro Andar – Lavras

O andar em questão compreende toda a estrutura de funcionamento da organização em Lavras. Os servidores, serviço de Internet e computadores estão neste único andar. Existe dois serviços de Internet, assim como em Belo Horizonte. A sala dos servidores, apesar de possuir chave, não é trancada pois não possui recursos para conservação dos servidores como um equipamento de ar condicionado. Os cabos da rede de computadores inicial, se apresentam protegidos. Porém, não existiu um processo de adequação às novas instalações.

A medida que a empresa foi crescendo, aumentando o número de funcionário, os cabos passaram a ficar expostos no chão havendo o risco de danos. Os switches iniciais se apresentavam bem posicionados, apesar dos cabos estarem mal arranjados, como será mostrado mais a frente. Atualmente, sem um processo definido, quando da necessidade de pontos de

rede, um switch é adicionado sem nenhuma orientação e localização fixa. Eles ficam em cima das bancadas dos funcionários ou algum lugar que acharem mais conveniente.

A seguir, imagens de equipamentos como switches, cabos de rede e servidores serão apresentadas com o intuito de comprovar o que foi dito. As figuras se referem à organização situada em cidade de Lavras – MG.

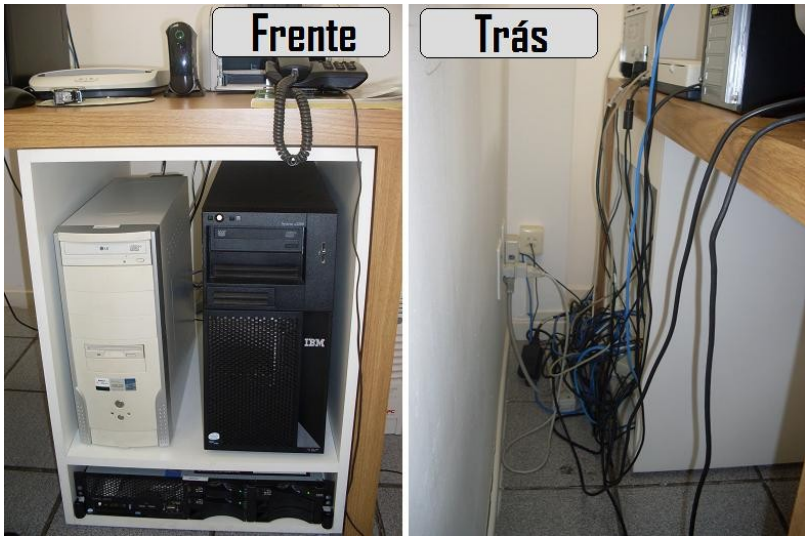


Figura – Servidores

Os servidores da empresa se encontram em uma sala sem ar condicionado. Não existe restrição de acesso para preservar o equipamento. Não estão situados em locais próprios para servidores.

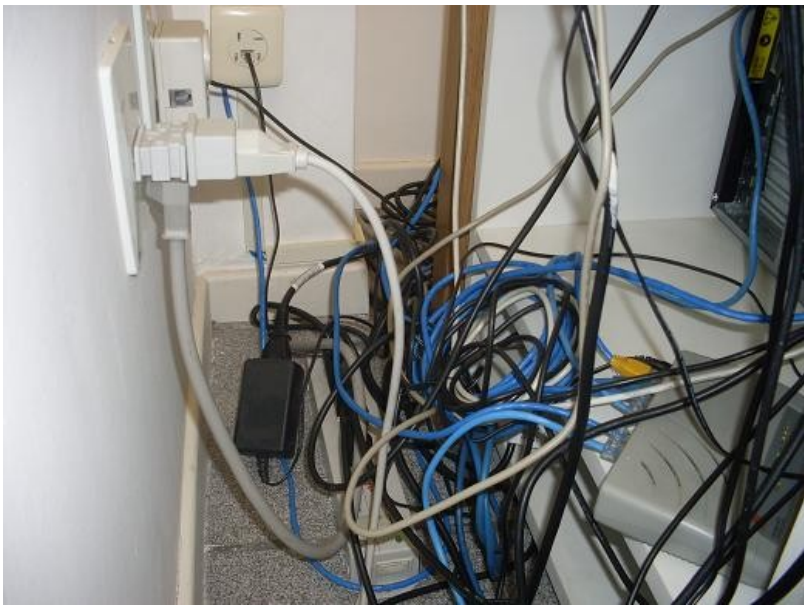

Figura - Cabos de rede de computadores

A figura 9 apresentada mostra a inexistência de um processo de manutenção da rede de computadores. O switch não possui local definido. Os cabos de rede estão totalmente embaraçados com cabos de energia. Não existe proteção dos cabos de rede. Nota-se uma necessidade urgente de um processo bem definido para a manutenção da rede de computadores.

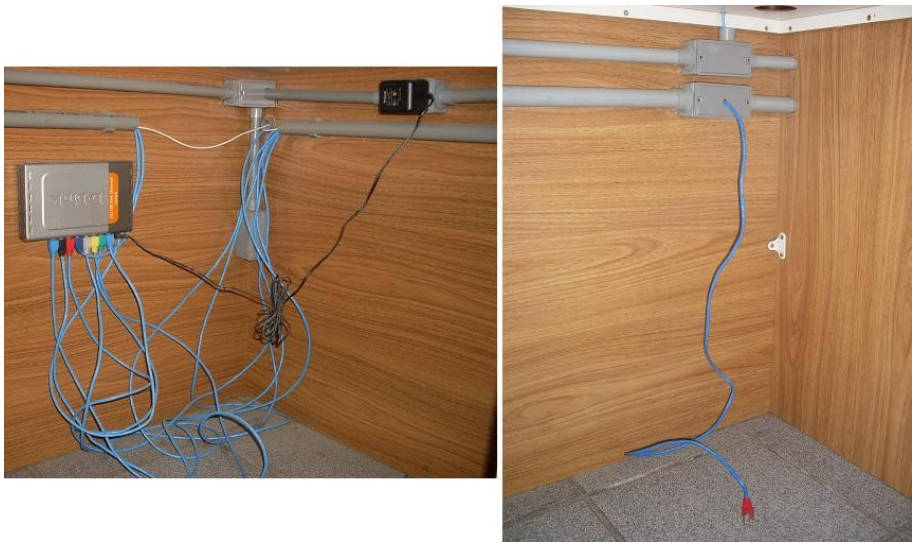

Figura – Switch instalado inicialmente

Quando a empresa se instalou no andar, a rede de computadores foi criada para atender os objetivos. Porém, com o crescimento, não houve a manutenção adequada da mesma. Na Figura 10, podemos constatar os cabos de rede saindo do cano e conectando ao switch. Porém, deve-se atentar ao fato dos cabos de rede estarem encostando no chão e soltos, propícios a danos.

Figura – Switch instalado sem processo

A figura abaixo apresenta a instalação de um switch devido à demanda de um novo ponto de rede. Mesmo a necessidade sendo apenas de um único ponto de rede, existiu a necessidade de instalação de um switch para este ponto. Este fato de adição de switch para um ponto só parece não ter nenhum sentido, mas o que foi constatado é que este ponto de rede já existiria se houvesse um processo para adição de pontos de rede definido. Uma economia com compra de equipamentos poderia ter ocorrido. Atualmente, o switch se encontra em cima de uma bancada, podendo ser trocado de lugar a qualquer momento.

## 4.2 Passos para a construção do cenário

A construção dos cenários da rede de computadores no simulador OPNET IT Guru Edition tem como fluxo de trabalho o seguinte esquema da figura X(SVENSSON; POPESCU, 2003).

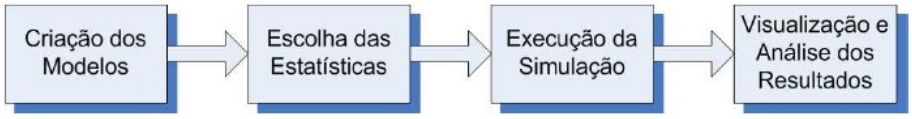


Figura – Esquema do processo de criação de cenários pelo OPNET

Primeiramente, deve-se fazer o mapeamento e o levantamento de informações a respeito da rede de computadores. Topologia, localização e tráfego utilizado devem ser levados em questão.

## 4.3 Criação dos cenários

Os cenários foram criado no simulador OPNET IT Guru Edition com as seguintes configurações da tabela 2.

| | |
|---|---|
| Nome Projeto | Projeto_Alex_Monografia |
| Nome Cenário | Cs_Monografia_Lavras |
| Create Empty Scenario | ok |
| Office | ok |
| Size meters | 100 x 100 |
| Tecnologia | Cliente - servidor |

Tabela 2 – Relação de configuração dos cenários no OPNET

## 4.4 Cenários modelados

Baseado no mapeamento da rede de computadores e levantamento de informações a respeito do tráfego da rede de computadores obtida através do

pessoal da infraestrutura da organização, os cenários foram modelados. Este tópico será dividido entre os cenários de Lavras e de Belo Horizonte. Os cenários atuais tanto em Lavras quanto em Belo Horizonte serão propostos. Por limitações do simulador, apenas o cenário proposto de Lavras foi realizado. A versão grátis do simulador para fins acadêmicos não deixa um nó da rede possuir mais de vinte enlaces. Como em Belo Horizonte a empresa é maior do que em Lavras, obteve-se este contratempo que não estava previsto.

### 4.4.1 Cenários de Lavras

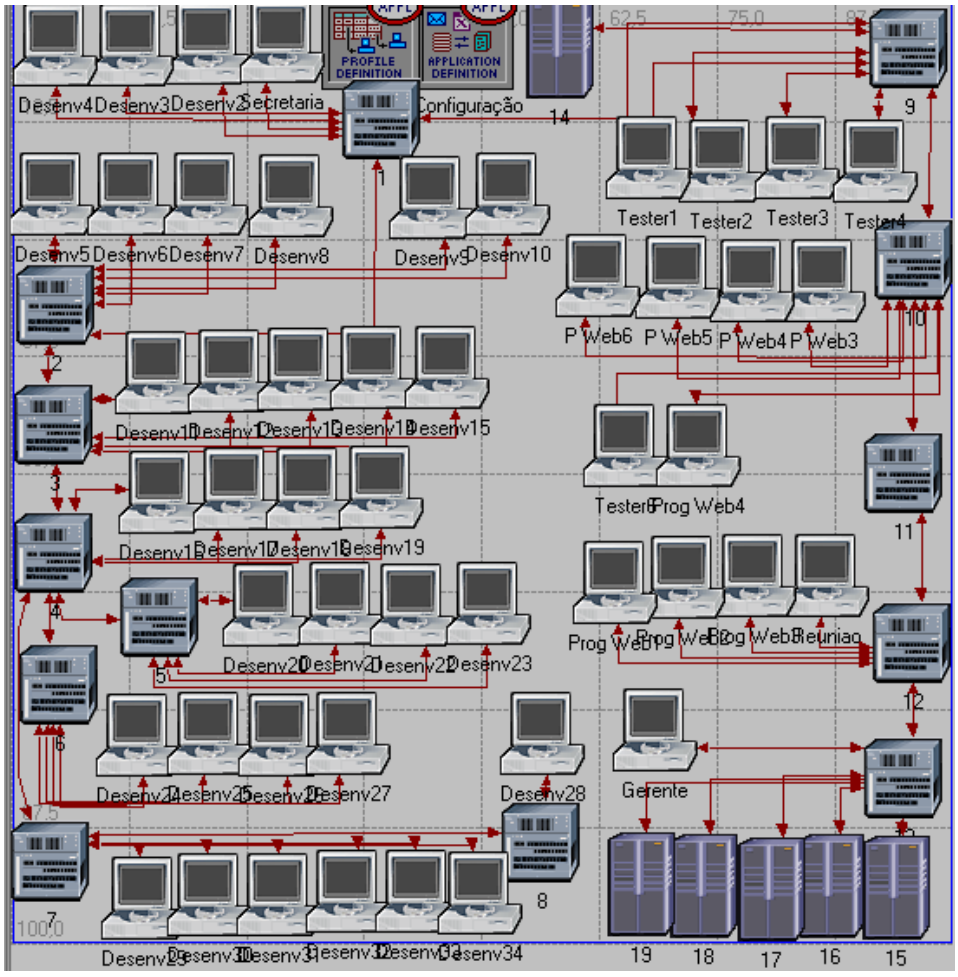


Figura - Cenário atual da empresa em Lavras

O cenário da rede de computadores da empresa em Lavras está representado na Figura 13. Deve-se atentar para a localização dos switches. O serviço de Internet chega no switch de número nove. A partir dele, a internet é então distribuída para os outros switches. O switch de número 8, se desejar transfeir algum arquivo para o computador do gerente, terá que passar por 10 switches no mínimo. Os servidores não se encontram localizados em um lugar apenas. Se encontram de forma espalhada pela empresa.

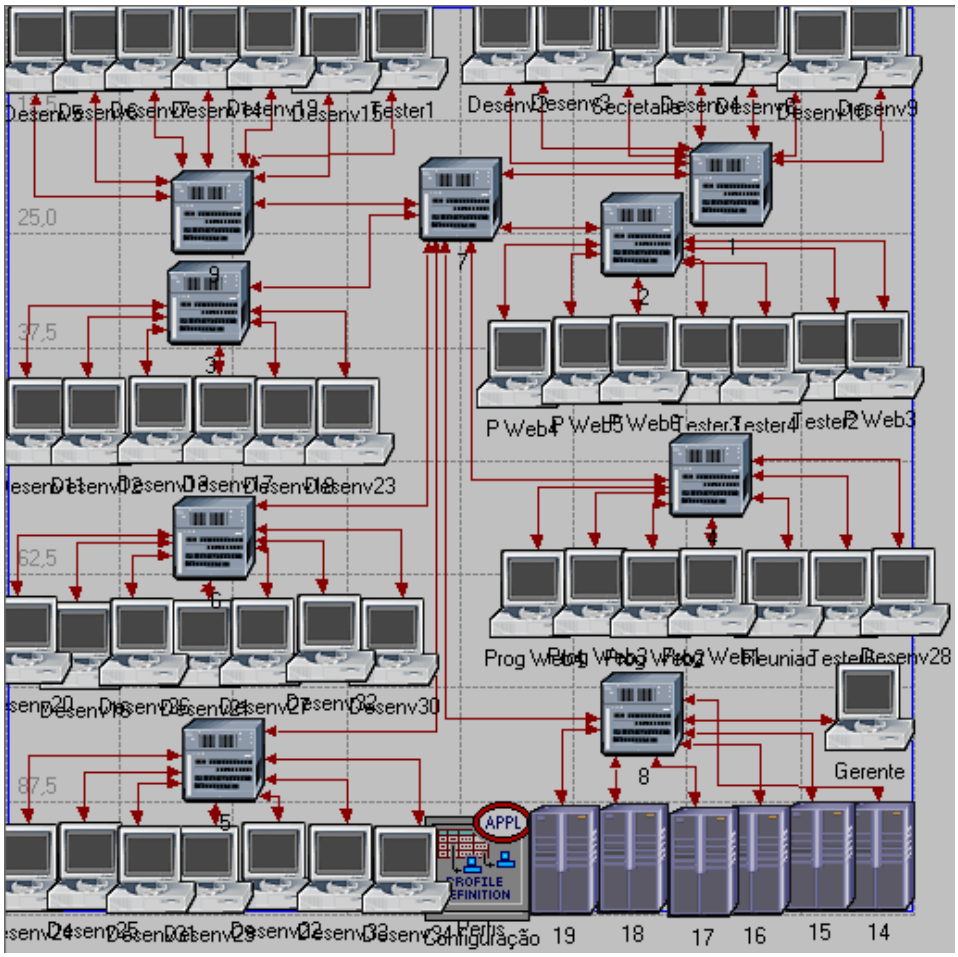


Figura - Cenário proposto para Lavras

Após analisar o cenário atual, algumas mudanças foram propostas para a rede de computadores. O serviço de Internet, neste cenário, está chegando no switch 7. A partir deste switch, todos os outros switches da empresa passam a ser “atingíveis”. Dessa forma, qualquer computador na rede que queira se comunicar com outro terá que passar apenas por três switches. O switch em que se encontra conectado, o switch de backbone de número 7 e o switch no qual o computador desejado se encontra. Os servidores se encontram agora agrupados num mesmo local. O desempenho deste esquema será analisado mais adiante na simulação.

### 4.4.2 Cenários Belo Horizonte

A seguir são apresentados os cenários atuais da organização em Belo Horizonte – MG.

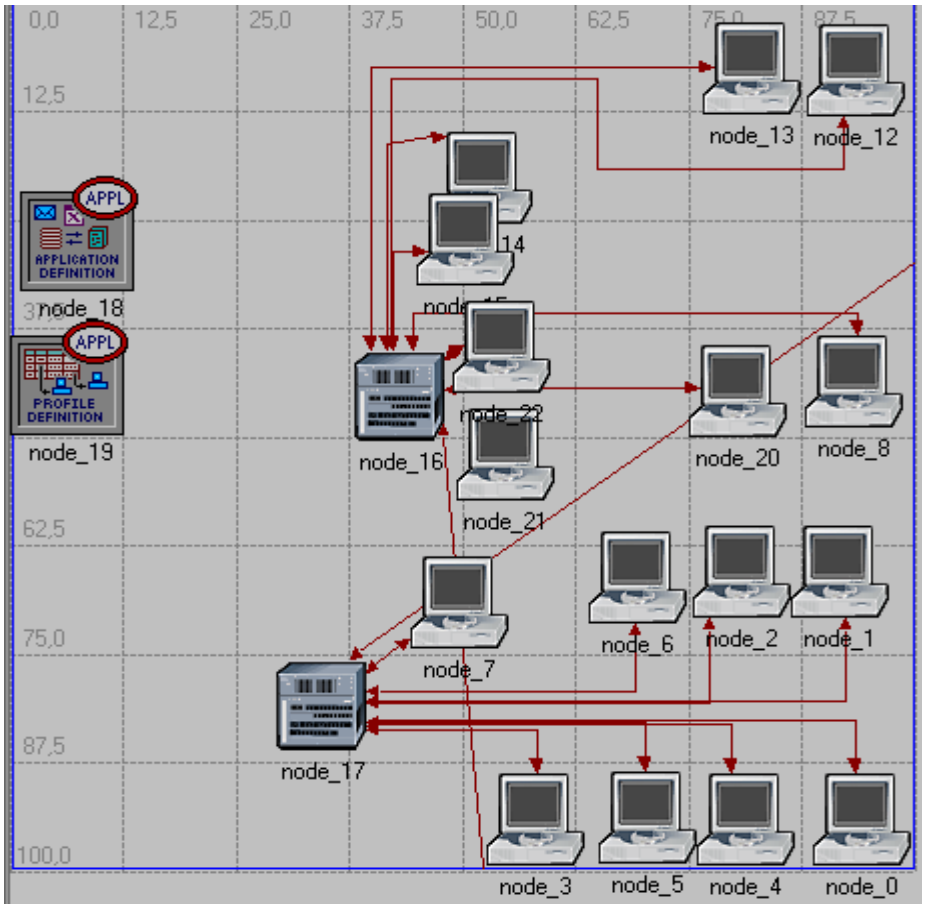


Figura – Terceiro andar

Os enlaces que se ligam ao switch na figura X não estão organizados pelo fato do programa não possibilitar a mudança do mesmo. Como se criou uma subrede no programa, ao ligarmos um switch no outro, o programa faz a ligação de forma automática. Deste modo, o cenário se apresenta um pouco bagunçado. A figura X apresenta apenas dois switches pelo fato de possuir só duas salas neste andar. Estes switches de contectam ao switch denominado

‘net’ na figura 16.

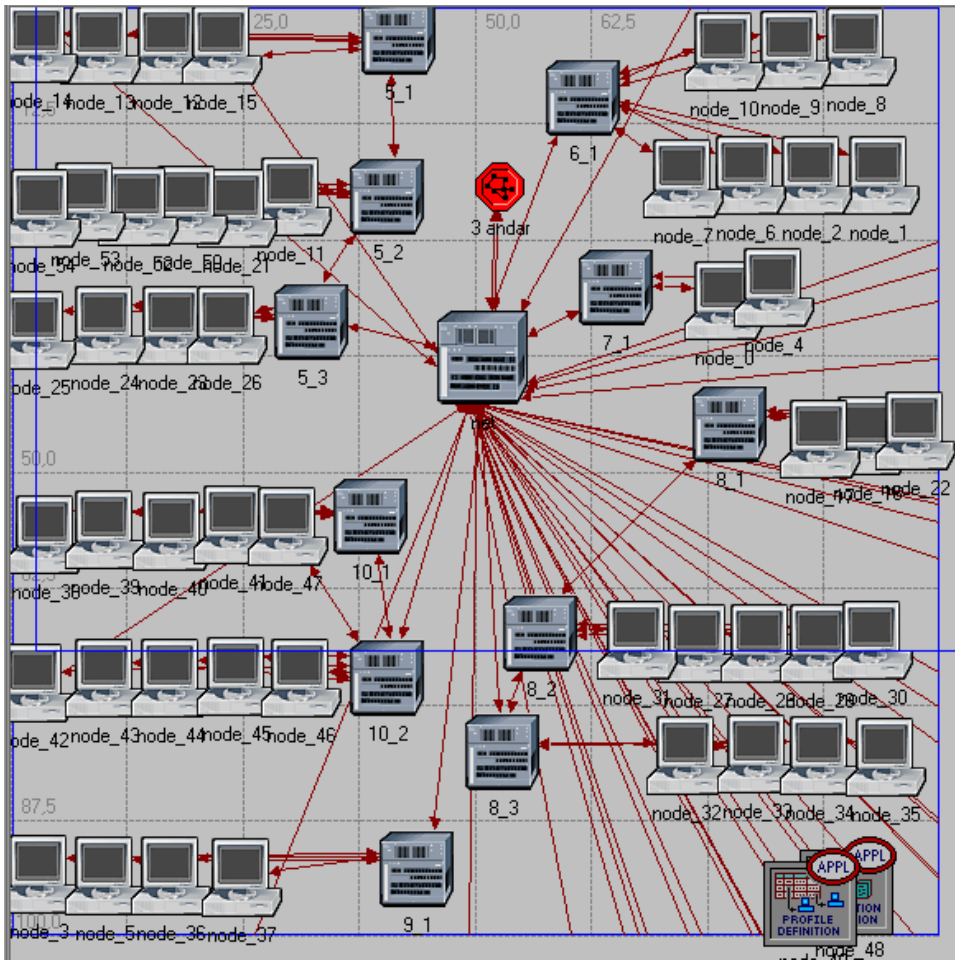


Figura – Sétimo andar

O sétimo andar, local onde o serviço de Internet chega, se apresenta o mais tumultuado de todos pelo fato de ser o inícioda rede de computadores.

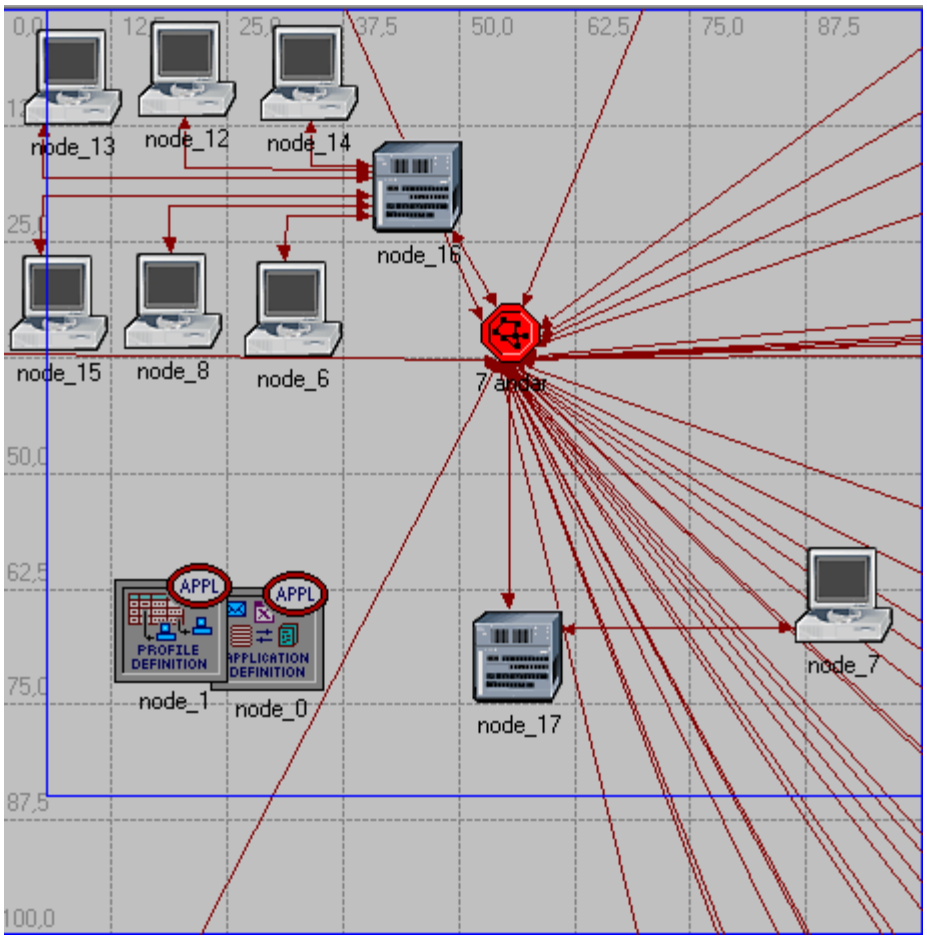


Figura – Oitavo andar

O oitavo andar é constituído apenas de dois switches por se tratar apenas de duas salas da empresa. Este andar se contecta com o switch ‘net’ do sétimo andar.

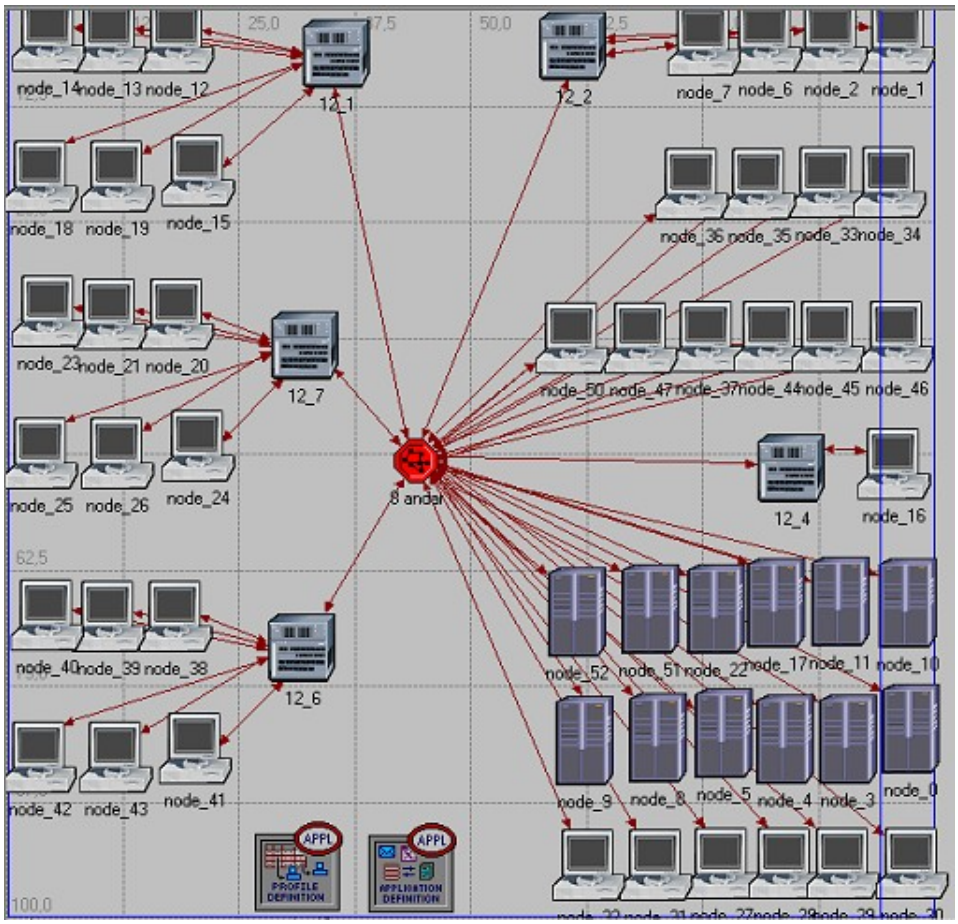


Figura – Décimo segundo andar

O décimo segundo andar, o último da organização em Belo Horizonte a ser apresentado, é o andar em que os servidores se encontram. Os servidores estão agrupados, alguns localizados em equipamento adequados e outro não. Com o aumento da demanda e a restrição do local, alguns servidores se encontram no chão. Os recursos estão ligados através da tubulação do prédio ao sétimo andar.

**Capítulo 5**

# 5 RESULTADOS E DISCUSSÃO

O objetivo deste capítulo é apresentar os resultados obtidos na simulação de redes de computadores da filial da empresa situada em Lavras. Por causa de limitações na versão gratuita do software OPNET IT Guru Edition a simulação não pode ser feita em Belo Horizonte. Os resultados serão apresentados a seguir.

## 5.1 Simulação em Lavras

### 5.1.1 LATÊNCIA

O cenário atual da rede de computadores da filial de Lavras não apresenta o conceito de switch de backbone. Quando há uma nova demanda por conexão de novos computadores na rede, não há um processo definido para essa conexão. Deste modo, com o crescimento da empresa, novos *switches* são adicionados a rede de maneira que se adapte ao ambiente ao invés da topologia. Este tipo de cenário apresenta atrasos e aumento de tráfego na rede. Com isso, há um comprometimento da disponibilidade da informação. O aumento do tráfego na rede além de gerar atrasos que implicam na produtividade, o aumento do tráfego na rede pode gerar a indisposição de um serviço, principalmente no caso de uma comunicação por áudio.

O cenário proposto tem por objetivo minimizar este problema e inserir um processo que evita o crescimento desordenado das conexões de computadores à rede. Nesta topologia, existirá um switch de *backbone* que possuirá os dois links de internet, Mastercabo e Velox. A partir deste, todos os outros *switches* serão conectados a ele, forçando assim um processo de conexão de novos switches na rede. Se não existir ponto de rede para novos computadores, um switch será conectado ao switch de backbone e posteriormente, conectado ao computador sem ponto de rede.

A seguir, será mostrada a comparação do resultado dos dois cenários em relação à latência. O tempo de simulação utilizado foi de 10 horas a fim de representar o tempo de um dia de serviço.

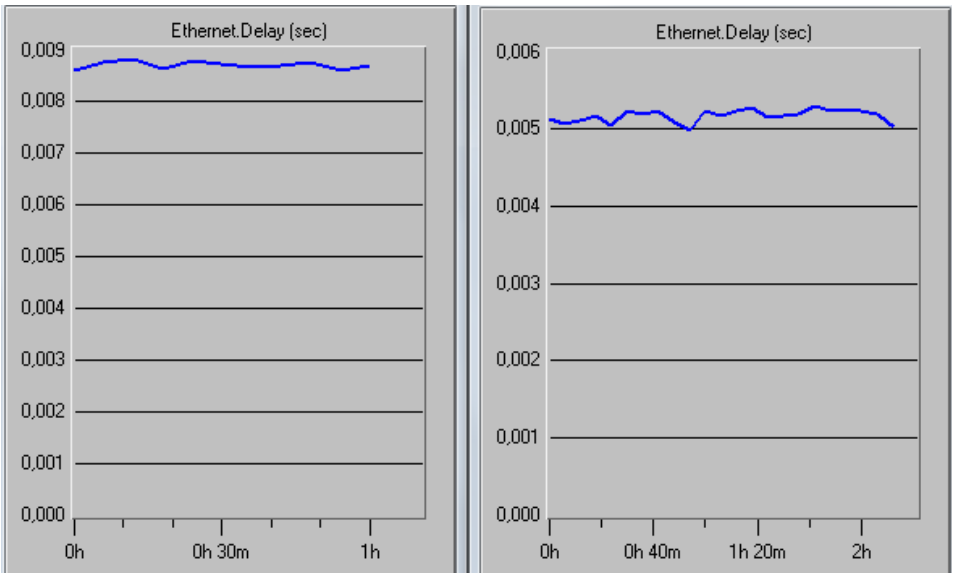


Figura – Comparação latência – Cenário atual (esquerda) e cenário proposto (direita)

O atraso da rede, também conhecido como *delay*, é o tempo gasto para um bit sair de uma máquina, trafegar pela rede de computadores e chegar até a outra máquina. O atraso pode ser medido em segundos ou frações de segundos. A localização entre o par de computadores na rede implica no aumento ou redução do atraso (COMER, 2007).

Com base na definição anterior sobre latência podemos comparar os gráficos. No cenário atual, o delay da rede está em torno de 0.009 segundos. Com a nova proposta de rede, o atraso passa a ter uma média de 0.005 segundos.

A partir deste gráfico, tirou-se o latência máxima e a mínima atingida na simulação. A figura a seguir demonstra os resultados.

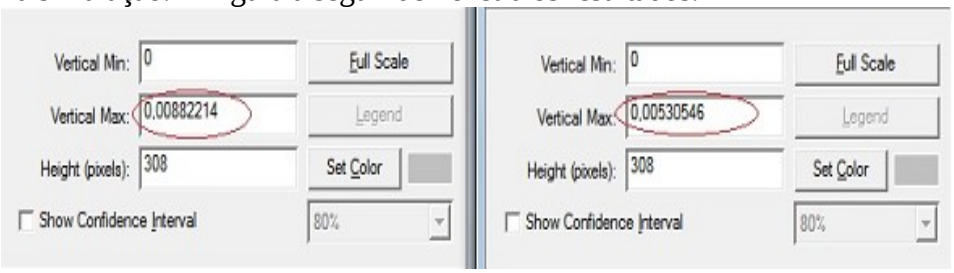

Figura – Comparação Latência máxima e mínima

No cenário atual a latência máxima está em 0.00882214 segundos. No cenário proposto, ela passa a ser de 0.00530546. Desta forma, obteve-se uma redução da latência da rede em 40%.

A redução ocorreu devido à nova topologia do cenário proposto. No cenário proposto, qualquer computador para transferir um bit para o outro, irá transferir este bit por 3 switches até atingir seu objetivo. No cenário atual, um dos problemas pode ser exemplificado pelo computador denominado Desenvolvedor 28. Esta máquina para transferir um bit de dados até o servidor denominado por 15, tem de passar por 11 dos 13 switches que compõem a rede.

Como um computador moderno pode processar mais de cem mil instruções em um milissegundo, a redução em 0.004 segundos no atraso na rede que parecia irrelevante se torna relevante para o computador (COMER, 2007).

Em relação ao aspecto de segurança da informação, a disponibilidade da informação se tornou mais ágil. Com a utilização da transmissão de voz e vídeo em tempo real através das redes de computadores, o jitter se tornou importante. Entenda-se jitter como a variação no atraso da rede. Se a rede tem jitter zero, sabe-se que cada pacote leva o mesmo tempo para atravessar a rede (COMER. 2007). Com o novo cenário, o atraso diminuiu e cada máquina está com a mesma distância uma da outra.

### 5.1.2 Tráfego recebido nos switches

Como a rede não segue uma topologia definida, a comunicação entre os switches precisam passar por vários switches até atingir seus destinos. Além disso, essa falta de topologia gera maior tráfego em determinados switches do que em outros. Este fato pode gerar perda de pacotes e exigir a retransmissão dos mesmos. Para exemplificar o que foi dito a respeito do aumento do tráfego nos switches, simulamos o tráfego recebido e encaminhado pelo switch número 4. A figura seguinte apresenta a comparação entre o tráfego no switch de número 4 no cenário atual (esquerda) e proposto (direita).

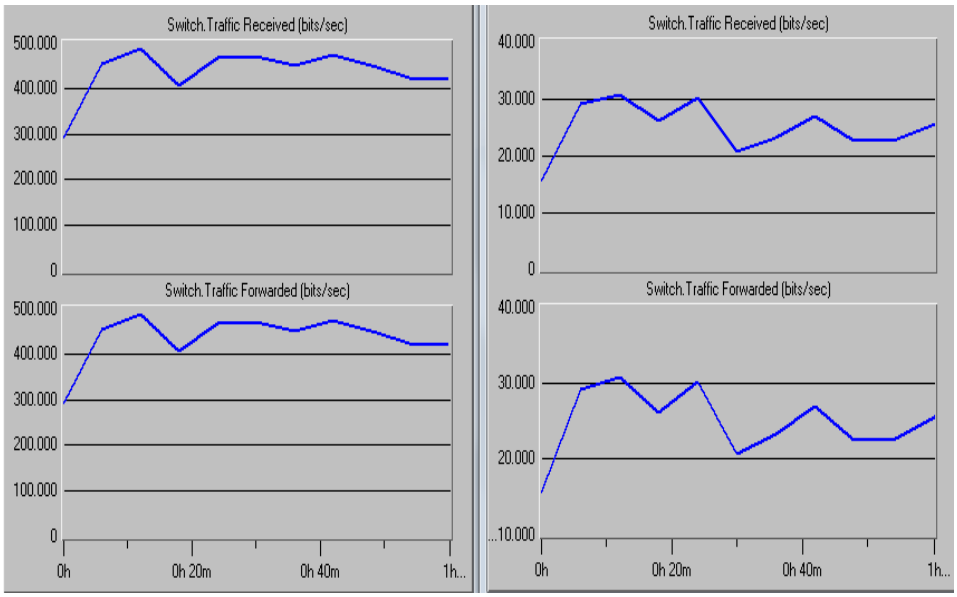


Figura – Comparação de tráfego recebido e encaminhado no switch 4 (cenário atual e proposto)

Como o switch no cenário atual se apresenta conectado a outros quatro switches, ele recebe um tráfego grande se comparado com o tráfego no cenário proposto. No novo cenário, o tráfego de bits recebidos está na casa dos 30.000 bits enquanto no cenário atual está na faixa de 500.000 bits.

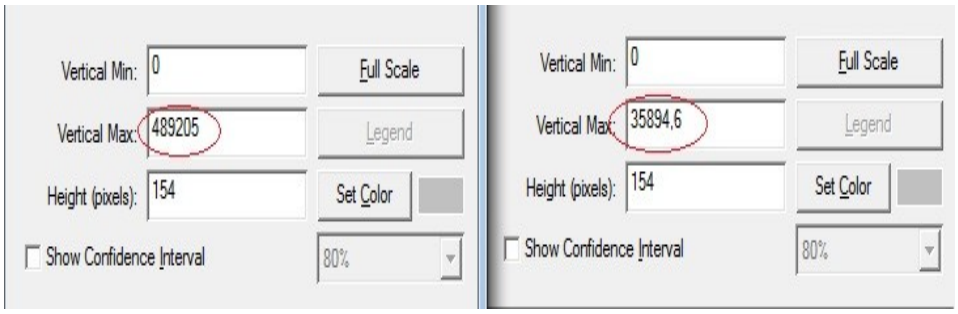


Figura – Valores máximos de tráfego no switch 4 (cenário atual e proposto)

A figura x acima apresenta os valores máximos de bits do switch nos dois cenários. No cenário atual, a quantidade máxima de bits recebida foi de 489205 bits. No cenário proposto, a quantidade máxima de bits foi de 35894,6 bits. O tráfego no switch diminuiu em 13,6 vezes em relação ao

cenário atual. Esta diminuição é um fator crucial para evitar a perda de pacotes no switch. Sendo assim, a disponibilidade da informação se torna mais ágil pois evita o atraso da transmissão da informação. Nesta simulação, utilizou-se apenas o switch de número 4 com o intuito de exemplificar a melhora da topologia proposta. O pior caso foi utilizado para demonstrar a diferença. Mas a diferença seria encontrada em quase todos os switches do cenário.

### 5.1.2 Controle proposto para a topologia da rede proposta

Baseando-se na norma ISO 27002, foi demonstrada a necessidade da segurança da informação. Em relação aos requisitos de segurança, obteve-se através da análise/avaliação dos riscos para a organização em relação à disponibilidade da informação. Não foram abordados riscos em relação à integridade e a confidencialidade das informações por motivos de segurança. Essas duas análises envolveriam a análise dos bancos de dados e escaneamento da rede com o intuito de identificar vulnerabilidades e falhas de segurança.

A partir daí, avaliou-se os riscos de segurança com o levantamento da topologia da rede de computadores da empresa e informações adicionais. Para avaliar os possíveis riscos, a simulação da rede de computadores foi feita no simulador OPNET IT Guru Edition. Com esta análise foi identificada a necessidade de um controle para a manutenção da topologia da rede de computadores proposta.

Desta forma, evita-se com o crescimento da empresa e aumento de funcionários a ruptura da topologia. Esta ruptura, provada através das simulações realizadas, gera danos à rede e atrapalha a disponibilidade da informação.

Um controle que se enquadraria na mudança da topologia, ou seja, na adição de um novo switch ou alteração em algum recurso relacionado à rede de computadores é o 10.1.1 da norma ISO 27002.

Esta seção trata do gerenciamento das operações e comunicações. A subseção 10.1.1 trata dos procedimentos e responsabilidades operacionais.

Sendo assim, a seção está definida a seguir:

**Seção 10:** Gerenciamento das operações e comunicações
**Objetivo:** Garantir a operação segura e correta dos recursos de

processamento da informação.

**Controle**: Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

Controle proposto baseado na subseção 10.1.1.

Objetivo: Evitar a ruptura da topologia da rede e qualquer alteração que possa afetar a rede de computadores com a adição ou remoção de algum recurso.

Passo 1) Documentação da rede de computadores. Mapear os recursos em uma planilha com as suas marcas, data de aquisição, localização, responsável pela operação e data da mesma.

Passo 2) Definir um funcionário responsável por adquirir o recursos mais adequado à necessidade e efetuar a operação de mudança.

Passo 3) Sempre que identificada a necessidade de adição de um recurso como switch, ponto de rede e outros, o funcionário responsável deve ser consultado para constatar a real necessidade. Este funcionário, após a aquisição do recurso, o instalará visando a integridade da topologia da rede atual.

Passo 4) Após a instalação, o passo 1 deve ser atualizado com os dados do novo equipamento adquirido ou operação realizada.

Passo 5) Deve-se estar explícito para os funcionários da organização a necessidade deste procedimento. Em algum local da empresa ou ambiente computacional, deve estar formalizado o procedimento e orientações para contato com a pessoa responsável.

O controle está definido pelos cinco passos acima. Se eles forem seguidos, há grande chance de não haver problemas em relação à quebra da topologia, garantindo assim, uma maior disponibilidade da informação.

Agora, baseando-se no Cobit Security Baseline, o guia de boas práticas em relação à segurança da informação, alguns indicadores para validar a eficácia do controle são necessários. Estes indicadores garantem que o controle criado está atendendo ao objetivo.

Indicador 1) Verificar de tempos em tempos, com a freqüência definida pela organização, se a topologia da rede de computadores da empresa. Se a topologia estiver correta, o controle está funcionando corretamente. Se existirem falhas, o controle deve ser revisado de acordo com as causas. As causas serão identificadas pelo rastreamento do recurso instalado que gerou a quebra da topologia.

Indicador 2) Análise da planilha de tempos em tempos, definido pela organização, se a planilha está atualizada corretamente e se existem falhas. Uma vistoria nas condições dos equipamentos ajudaria a validar a planilha. Ainda neste passo, alguma irregularidade em relação à condição de equipamentos poderia ser verificada. Equipamentos em estado de má conservação ou mal funcionamento poderiam ser identificados.

## 5.2 Simulação em Belo Horizonte

Por limitações do simulador, não foi possível a realização da simulação do ambiente empresarial sediado em Belo Horizonte. O simulador, em sua versão gratuita, está limitado à conexão de apenas vinte nós conectados a dois ou mais dispositivos. Como a maioria das ligações se dá no sétimo andar e possui mais de vinte pontos de rede, a simulação não pode ser realizada por esta limitação do simulador. Todos os outros três andares da empresa se conectam ao sétimo através da tubulação do prédio. Este fato ocorre pois o serviço de internet chega neste andar. A seguir, é apresentada a mensagem de erro do simulador.

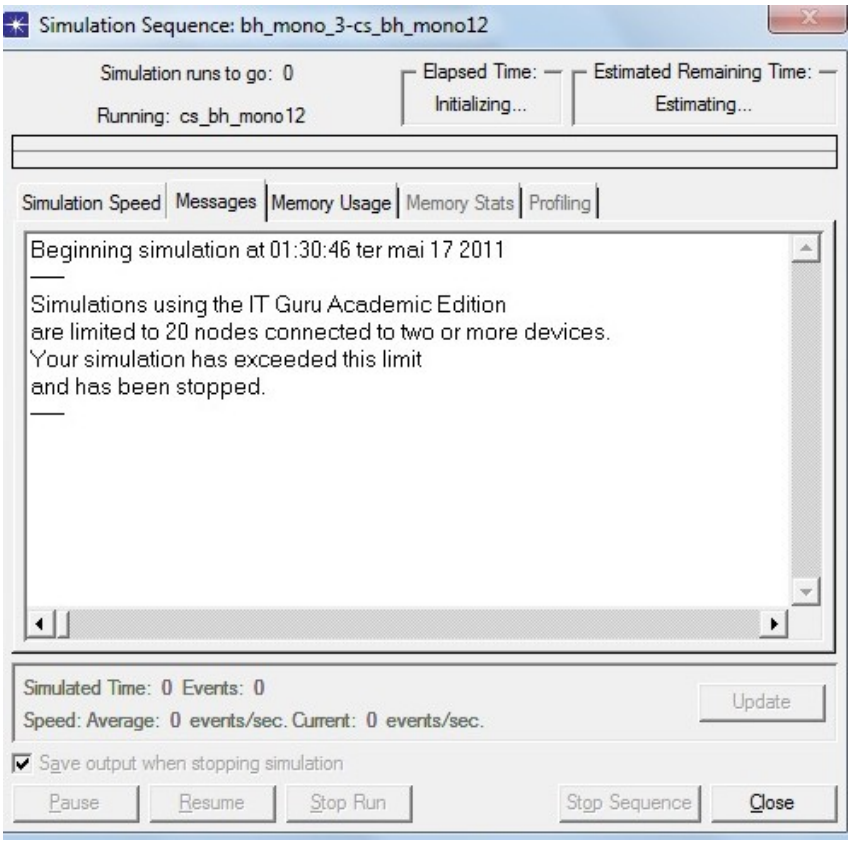


Figura – Mensagem de erro de limitação do simulador na versão gratuita

Sendo assim, apesar de todo o esforço gasto para coletar informações dos quatro andares e da implementação da rede no simulador, a execução não pode ser efetuada.

## 5.3 AVALIAÇÃO DA SEGURANÇA FÍSICA, LÓGICA E DOS RECURSOS HUMANOS PELO QBASI

Neste tópico, uma análise da segurança física, do ambiente e dos recursos humanos proposta por FONTES (FONTES, 2008) será feita. Ao

final, a porcentagem de eficácia da organização nos três aspectos de segurança será fornecido como resultado da avaliação.

| Avaliação do quesito | Nota (%) |
|---|---|
| Segurança Física | 47,14% |
| Segurança Lógica | 60% |
| Segurando de Recursos Humanos | 17.5% |
| Total | 41.55% |

Tabela 3 – Relação percentual da eficácia da organização nos três quesitos de segurança

A organização em questão foi baseada no questionário proposto por Fontes e nas informações levantadas durante a execução do trabalho. Das dezessete perguntas, apenas quatorze se aplicaram a ela. Um total que poderia chegar até 140 pontos, ela obteve 66 pontos na nota final. Uma porcentagem de 47,14% de eficácia na segurança física.

Essa porcentagem pode ser melhorada e muito se as possíveis soluções deste trabalho forem seguidas. Vale ressaltar que não se precisa obter a nota 10 nas perguntas. A nota 9 já é válida. Fiz esta ressalva pelo fato de que na maioria das vezes, a melhor solução também é a mais cara.

Para finalizar esta conclusão, gostaria de ressaltar que a segurança deve estar em contínuo processo de melhoramento. Esta nota de hoje, se nada for feito na organização, em uma futura reavaliação daqui a 5 anos por exemplo, a empresa pode ganhar nota igual ou mais baixa que esta. O padrão de avaliação também pode sofrer evolução.

Com base nesta última avaliação, pode-se perceber que o acesso lógico se apresenta melhor implementado que os outros. Dentro das 21 questões propostas, 19 são aplicáveis. Logo, dos 190 pontos que a organização poderia obter, ela obteve 114 pontos. Isso leva a uma porcentagem de 60% de eficácia da segurança lógica, baseada no QBASI.

Porém, mesmo com um resultado melhor do que os outros anteriores, o controle lógico ainda obteve um valor mediano de aproveitamento. Deve-se, portanto, focar no que está fraco ainda a fim de garantir uma melhor gestão. Essa melhoria deve ser contínua e após a implementação de soluções, a criação de controles para um possível monitoramento deve ser feita. Com isso a organização trilhará o seu caminho diante do seu objetivo de negócio

com mais segurança e correndo menos riscos que possam atrapalhar o andamento normal de suas atividades.

Nota-se que a segurança da informação com foco nos recursos humanos por parte da organização não se apresenta muito definida ainda. Deve-se tentar o mais rápido possível criar os documentos relativos à segurança da informação e conscientizar os usuários que o seu papel é essencial para o objetivo em questão. Todos os colaboradores devem estar envolvidos de forma a contribuir com a redução de incidentes de segurança que possam atrapalhar o negócio.

Como resultado, das cinco perguntas que foram propostas pelo questionário, apenas quatro foram aplicáveis à organização. Deste modo, as quatro perguntas que totalizam 40 pontos como o máximo atingível, a empresa obteve 7 pontos. Isto significa que a eficácia da organização em relação À segurança em recursos humanos é de 17,5%.

Portanto, a empresa deve focar mais nos recursos humanos pelo fato de serem eles que conduzem a empresa. Por mais automatizada que uma empresa seja, sempre haverá a necessidade de pessoas trabalhando nela. Daí a real necessidade de definir os direitos e deveres de cada um dentro da mesma.

# 6 CONCLUSÃO

A periodicidade da análise da segurança da informação pode ter sua necessidade notada por este trabalho. As organizações não devem achar que estão seguras pelo fato de terem feito uma análise de segurança da informação no passado e esquecerem de realizar análises futuras. Após a realização da análise da segurança da informação na empresa descobriu-se que a falta de implantação de controles no momento da implementação de soluções pode gerar problemas para a organização.

A análise constatou que não houve a criação de um controle que suportasse a evolução da estrutura da rede de computadores. A inexistência de controles gerou problemas, tais como o aumento desnecessário da latência e do tráfego nos switches. Apesar dos gráficos referentes ao tráfego recebido e encaminhado nos switches não terem sofrido alterações, o que indicaria uma possível perda de pacotes, notou-se que o tráfego no cenário proposto estava 13,6 vezes inferior que no cenário atual. A latência foi reduzida em 40%, o que representa um ganho de produtividade para a máquina que está transferindo dados para outra. Sendo assim, a simulação da rede de computadores no software *OPNET IT Guru Edition* deixou claro que a estrutura atual da rede de computadores não está em bom funcionamento e precisa ser revisada.

No presente momento, a empresa se apresenta em processo de mudança de local e o estudo da solução do trabalho está sendo estudada. Se a organização optar em implementar a solução proposta deste trabalho, com o intuito de utilizar os recursos computacionais já adquiridos, deve-se atentar para a compra de mesas apropriadas para armazenamento dos switches. Esta mesa é comumente denominada por "*hack*". Assim, os switches estariam centralizados em um local da empresa. Se possível, com acesso restrito. Deste local, sairiam apenas os cabos de rede. Uma opção para o transporte dos cabos seriam as eletrocalhas, nas quais os cabos percorreriam toda a empresa, não ficariam no chão expostos a danos e teriam fácil manutenção.

Caso a empresa não queira reutilizar os switches existentes, ela

poderia adquirir um switch 3Com, por exemplo, com 48 ou 50 portas que atenderia perfeitamente a sua filial. Nesta segunda solução, todos os computadores estariam conectados ao switch. Deve-se lembrar que esta solução atenderia a empresa no momento desta análise. Há a possibilidade de daqui a um tempo novos funcionários serem contratados e um novo ponto de rede não existir. Deste modo, voltamos à principal questão do trabalho, a necessidade de controles. Um controle deve ser pensado na implementação da solução, pois caso ocorra a necessidade de um novo ponto de rede, já exista um procedimento a ser realizado.

Como a matriz da empresa não foi avaliada por questões de limitação da versão gratuita do simulador, apenas a filial foi avaliada. Porém, a empresa deve se atentar às falhas encontradas na filial e verificar se também existem em sua matriz.

A avaliação realizada na filial com base no QBASI (Questionário Básico de Avaliação da Segurança da Informação ) proposto por Fontes, pode conduzir a empresa a atingir um nível superior em segurança e se tornar ainda mais competitiva no mercado. Atualmente, ela se apresenta com 41,55% de eficácia em sua segurança de infraestrutura.

Como a gestão da segurança da informação consiste em uma gestão dos processos relacionados à segurança da informação, os controles se tornam fundamentais para o gestor da segurança da informação. Os controles são a base que o gestor tem para descobrir se suas soluções estão sendo eficazes ou não.

Desta forma, a criação dos controles deve ser tida como alicerces para a organização. É com base neles que a organização irá efetuar novas análises quanto à segurança da informação e identificar riscos e possibilidades de melhoras. Com isso, a empresa estará mais protegida contra os diversos tipos de ameaças e, por consequência, mais competitiva no mercado.

## 7 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO 27002. ***Tecnologia da Informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação***. 2ª edição, 2007.

***Boas práticas em segurança da informação / Tribunal de Contas da União***. – 2. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.70 p. Disponível em https://acessoseguro.tcu.gov.br/portal/pls/portal/docs/684005.PDF. Data de acesso: 05/04/2011.

***Cartilha de Segurança na Internet***, versão 3.1. cert.br, 2006 Disponível em < http://cartilha.cert.br/ > Data de acesso: 05/04/2011.

***COBIT Security Baseline / IT Governance Institute***, 2ª edição. 2007. Disponível em < http://www.itgovernance.co.uk/products/885>. Date de acesso: 01/02/2011.

COMER, D. E. ***Redes de computadores e internet***. 4ª edição. Porto Alegre: Bookman, 2007.

FONTES, E.L.G. ***Praticando a segurança da Informação***. Rio de Janeiro: Ed: Brasport, 2008.

FOROUZAN, B. A. ***Comunicação de dados e redes de computadores***. ed. Porto Alegre. 840 p . Ed: Bookman, 2006.

GNS3. ***Graphical Network Simulator 3***. GNS3.net, 2009.Disponível em: <http://www.gns3.net/>. Data de acesso: 05/04/2011.

GOLMIE, N.; KOENIG, *A.* ***The NIST ATM Network Simulator, Operation and Programming***. *Version 1.0*.[S.I.], 1995.

KUROSE, J.F. ***Rede de Computadores e a Internet: uma nova abordagem***, 1ª edição. Ed: Addison Wesley. São Paulo, 2003.

LAW, A.M; MCCOMAS, M.G. ***Simulation software for communications networks: The state of the art***. *IEEE Communications Magazine*, p.44-50, Março 1994.

MULLER, I. ; NETTO, J. ; PEREIRA, C. E. ; Allgayer, R. S. . ***Rede de sensores sem fio aplicada no monitoramento de bancos de baterias***. In: XVIII Congresso Brasileiro de Automática, 2010, Bonito - RS. CBA 2010 - XVIII Congresso Brasileiro de Automática, 2010. v. 1. p. 2357-2363.

PONEMON INSTITUTE. 2009 ***Annual Study: Cost of a Data Breach***., 2009. Disponível em: <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf>. Data de acesso: 05/04/2011.

SANTOS, H.M.D.; Magalhães, S. ***Biometria e Autenticação***. In actas da IV Conferência da Associação Portuguesa de Sistemas de Informação ,2003. Porto.

SIVABALAN, M.; MOUFTAH, H. T. QUARTS-II: ***A Routing simulator for ATM Networks***. *IEEE Communications Magazine*, p.80,87, Maio 1998.

SVENSSON, T.; POPESCU, A. ***Development of laboratory exercises based on OPNET Modeler***. Dissertação (Mestrado) – Blekinge Institute of Technology, Junho 2003.

TANENBAUM, Andrew S. ***Redes de Computadores*** , 4ª edição. Rio de Janeiro: Ed: Campus, 2003.

UNIVERSIDADE FEDERAL DE LAVRAS. Biblioteca da UFLA. ***Manual de normalização e estrutura de trabalhos acadêmicos*****:** TCC, monografias, dissertações e teses. Lavras, 2010. Disponível em: <http://www.biblioteca.ufla.br/site/index.php> . Acesso em: 25/05/2011.

ZAMBALDE, A. L.; PADUA, C.I.P.S.; ALVES, R.M. ***O documento científico em Ciência da Computação e Sistemas de Informação***. Lavras, Minas Gerais: Notas de aula – rascunho, texto em construção sem revisão de português e criações, Departamento de Ciência da Computação, UFLA, 2008. 74p.

## ANEXO A - Questionário

A seguir, será apresentada a tabela 4 de padrão de avaliação que será utilizada para avaliar a organização. Posteriormente, as perguntas do questionário, suas respectivas notas, justificativas e possíveis soluções serão apresentadas.

| Notas | Significado |
|---|---|
| 0 | Não se aplica |
| 1 | Resposta : Não |
| 2 | Solução em planejamento inicial |
| 3 | Está planejada a implantação da solução |
| 4 | Parcialmente Implementada. Instável. Ainda não confiável |
| 5 | Possui o mínimo de atendimento aos requisitos |
| 6 | Prestes a ser melhorada |
| 7 | Quase totalmente implementada. Satisfatório para situações normais |
| 8 | Está funcionando bem |
| 9 | Totalmente implementada |
| 10 | Solução implementada é referência de mercado (melhor da classe) |

Tabela 4 – Padrão de avaliação Fonte: FONTES, 2008

Perguntas do questionário básico de avaliação da segurança da informação.

### 7.1.1 Segurança Física

**Pergunta 1:**

Cada pessoa tem autorização de acesso físico apenas aos ambientes que necessita acessar para desempenhar as suas funções profissionais na organização?
**Nota**: 7
**Justificativa**:

Em BH: Cada funcionário possui apenas a chave da sua porta e o controle do acesso ao andar é feito por biometria. Porém, na matriz, nada impede que um funcionário acesse outra sala em que não esteja autorizado no horário de funcionamento. Pode ser que neste momento não haja ninguém na sala. Já em Lavras, a sala dos servidores é aberta. Não há controle de acesso por chave na mesma. Apesar disso, passa se ter acesso ao único andar da empresa é necessária a chave e a senha do alarme. Sendo assim, apenas funcionários acessam a empresa. Em situações normais não haverá problemas.

Em Lavras: Todos funcionários, com exceção da faxineira, possuem a chave da empresa. O acesso ao ambiente de trabalho se dá através de chave e senha única do funcionário. Biometria não está funcionando no momento.
**Possível solução**:

Apesar de existir a chave da sala dos servidores em Lavras, a sala fica aberta com o intuito de resfriar o equipamento. Dever-se-ia comprar um ar condicionado e instalá-lo na sala para obter o resfriamento necessário. Com isso, a sala poderia ser fechada e o acesso limitado.

Outra medida, esta vale tanto para Lavras quanto para a matriz em Belo Horizonte, envolve a segurança de equipamentos. Notou-se que o *hack* de servidores está cheio e servidores estão no chão. Dever-se-ia comprar um novo *hack* para melhor acomodar os recursos e, adicionalmente, com proteção contra um incêndio ou vazamento de água por exemplo.

**Pergunta 2**

O acesso físico das áreas da organização é controlado, impedindo que pessoas não autorizadas acessem ambientes em que não estão autorizadas?
**Nota** : 8
**Justificativa**:

A organização apresenta controle biométrico para acesso aos andares da empresa e cada funcionário possui a chave de sua sala. Porém, existem situações em que uma pessoa não autorizada conseguiria ter acesso ao andar e às salas quando em funcionamento.
**Possível solução**:

Está funcionando bem, porém a utilização de câmeras deveria ser estudada por parte da organização. Tal medida seria um fator que complementaria a segurança existente.

**Pergunta 3**

O acesso físico de cada pessoa fica registrado, permitindo uma auditoria?

**Nota**: 7

**Justificativa**:

O acesso físico é controlado pela biometria caso o andar esteja fechado ou seja o primeiro a chegar. O acesso às salas é controlado por chaves e lançamento de horas online. Você pode chegar na empresa, o andar estar aberto, entrar na sala, utilizar o computador e ir embora sem ter registrado nada.

**Possível solução**:

Controle através de roletas eletrônicas nos andares. O acesso seria permitido via cartão. Neste caso, cada pessoa seria obrigada a passar pela roleta. Assim, o acesso seria mais restrito e melhor registrado.

**Pergunta 4**

Para os ambientes restritos, o controle de acesso obriga o acesso individual e evita que alguém entre de carona quando uma pessoa autorizada acessa o ambiente?

**Nota**: 1

**Justificativa**:

Como explicado na pergunta três, o acesso não é restrito e individual.

**Possível solução**:

Idem a solução da pergunta três.

**Pergunta 5**

Os visitantes são identificados individualmente e têm registradas sua entrada e saída dos ambientes?

**Nota**: 1

**Justificativa**:

Em alguns andares da empresa os visitantes são identificados pelas secretárias. Em outros, por ser compartilhado com outras empresas, a identificação é feita nas salas. Não há registros.

**Possível solução:**

Com a solução da roleta eletrônica implementada, o acesso do visitante se daria mediante ao cartão do visitante que estaria de posse da secretária ou responsável pelo andar. Com isso, o registro do visitante seria feito.

**Pergunta 6**

Existe o monitoramento e a gravação de imagens dos principais pontos de acesso ao ambiente físico, pontos de vigilância e do perímetro do terreno?

**Nota**: 1

**Justificativa**:

Não há monitoramento na empresa por câmeras.

**Possível solução**:

Estudo da viabilidade e necessidade para um posterior planejamento, implementação e manutenção.

**Pergunta 7**

As imagens são armazenadas durante um período previamente estabelecido, podendo ser recuperadas neste período?

**Nota**: 0

**Justificativa**:

Não se aplica

**Possível solução**:

Não se aplica

**Pergunta 8**

As imagens são guardadas em um local protegido adequadamente de forma que não seja possível (ou muito difícil) o roubo delas com o objetivo de desaparecimento de provas?

**Nota**: 0

**Justificativa**:

Não se aplica

**Possível solução**:

Não se aplica

**Pergunta 9**

As pessoas são avisadas de que o ambiente é monitorado e gravado?

**Nota**: 0
**Justificativa**:
Não se aplica
**Possível solução**:
Não se aplica

**Pergunta 10**
Foi feita uma análise das ameaças existentes por causa da vizinhança e conseqüente gestão dos riscos?
**Nota**: 8
**Justificativa**:
A análise foi feita pelos responsáveis. Atualmente a empresa está com a idéia de mudar de lugar de Lavras e Belo Horizonte. Tais análises estão sendo feitas e balanceados os pontos positivos e negativos de cada nova possível localização.
**Possível solução**:
Já está sendo feita a análise pelas pessoas responsáveis. Não se aplica.

**Pergunta 11**

Foi feita uma análise de risco contemplando as principais ameaças (incêndio, roubo, enchentes, vazamento de água) e foram planejadas e desenvolvidas medidas preventivas e corretivas?

**Nota**: 6

**Justificativa**:
A empresa possui alguns requisitos contemplando as ameaças, porém, algumas precisam ser melhoradas. A sala de servidores precisa ser melhor protegida e os equipamentos precisam ser melhor posicionados.
**Possível solução**:
A melhoria do local dos servidores contra incêndio deve ser feita. Em Belo Horizonte, a sala dos servidores possui no teto medidas preventivas contra incêndio. Porém, o equipamento estragaria com a água que saísse do teto com o intuito de apagar o fogo do mesmo jeito. Os equipamentos tanto em Lavras quanto em Belo Horizonte, se apresentam muitas das vezes no chão, sem proteção nenhuma, de fácil acesso e cabos espalhados pelo chão.

Esta localização mal definida pode gerar problemas como indisponibilidade da rede e afetar algum setor da empresa. Uma reorganização da localização dos equipamentos assim como a proteção dos cabos seria de grande valia para a continuidade do negócio.

**Pergunta 12**

Existe um processo contínuo garantindo a efetividade das medidas de controle existentes?

**Nota**: 5
**Justificativa**:
O processo foi criado mas não há sinais de melhoria contínua. Aparecem por demanda.
**Possível solução**:
Definir um responsável para o processo a fim de que este se organize para monitor e melhorar sempre a estrutura atual.

**Pergunta 13**

Existe um controle para a saída e entrada de material?

**Nota**: 5
**Justificativa**:
O processo de saída dos materiais é feita através de processo dentro da empresa. Porém, em horário de funcionamento, o controle pode ser feito. Em horários fora do expediente, o controle não é feito.
**Possível solução**:
Instalação de câmeras de vigilância na empresa.

**Pergunta 14**

Existem pontos de vigilância que cobrem todo o ambiente físico da organização, bem como a periferia do terreno/ambiente?

**Nota**: 1
**Justificativa**:
Não existem câmeras de vigilância
**Possível solução**:
Possível instalação visando atender ao objetivo, caso seja viável por se tratar de um prédio.

**Pergunta 15**

Sempre que possível é utilizado material retardante a fogo, que dificulta o início e a propagação do incêndio?

**Nota**: 8
**Justificativa**:
Há extintores de incêndio pelos andares apesar de não ter sido necessário a utilização.
**Possível solução**:
Não se aplica

**Pergunta 16**

É realizado treinamento de combate a incêndio pelo menos uma vez por ano para todo o pessoal?

**Nota**: 1
**Justificativa**:
Não existe treinamento.
**Possível solução**:
Realizar treinamentos de combate a incêndio.

**Pergunta 17**

Existe sinalização de emergência indicando as saídas e saídas de emergência?

**Nota**: 7

**Justificativa**:

Em Belo Horizonte existe a sinalização correta das saídas pelos elevadores e pela escada. Já em Lavras, só há uma maneira de entrar e sair do prédio.

**Possível solução**:

Em uma mudança de local da organização, caso haja apenas uma saída, estudar a viabilidade de construção de uma porta para saída de emergência e sua sinalização devida.

### 7.1.2 Segurança em Recursos Humanos

**Pergunta 1**

Existe um processo de conscientização e treinamento de usuários em segurança da informação?

**Nota:** 1

**Justificativa:**

Ninguém possui a responsabilidade de ditar as regras em segurança da informação. Existe o documento de propriedade intelectual apenas, mas, um documento a respeito da informação e segurança na organização não são passados formalmente.

**Possível solução:**

Definir um processo formal e explícito para todos os usuários com os seus deveres para com a organização em relação à segurança da informação.

**Pergunta 2**

Cada usuário participa do processo de conscientização e treinamento em segurança da informação pelo menos uma vez por ano?

**Nota:** 1

**Justificativa:**

Os usuários da organização não recebem treinamentos em relação à segurança. O que se sabe foi passado pelos funcionários com o decorrer do tempo.

**Possível solução:**

Definir um responsável por dar estes treinamentos. Porém, antes de tudo, deveriam ser feitos esforços para se construir um processo de segurança da informação descentralizado com os seus respectivos responsáveis.

Isto se torna necessário, pois, quando uma pessoa é responsável por

algo ela cuida. Quando não tem nada definido formalmente, ela faz o que pode quando da tempo e sem muita dedicação.

**Pergunta 3**

Todo tipo de usuário (funcionário, prestador de serviço, estagiário) participa do processo de conscientização e treinamento em segurança da informação?

**Nota:** 0

**Justificativa:**

Não se aplica pois não existem treinamentos.

**Possível solução:**

Implementar a pergunta 2 e incluir todos os colaboradores da empresa no treinamento.

**Pergunta 4**

Todo usuário antes de iniciar suas atividades profissionais na organização recebe orientações em relação à segurança da informação e toma conhecimento dos regulamentos existentes?

**Nota:** 4

**Justificativa:**

Quando o usuário se inicia ele assina o termo de propriedade intelectual. Regras relativas a uso de pen drives, músicas, instalação de programas nas máquinas da empresa, dentre outros não estão definidos explicitamente.

**Possível solução:**

Criação de um documento e veiculação do mesmo tanto por email quanto por fixação em locais estratégicos na empresa, como mural de anúncios. Sendo assim, quem por ventura não receber o email, terá a oportunidade de ler as exigências da organização frente à segurança da informação. Deste modo, incidentes de segurança causados por colaboradores serão minimizados.

**Pergunta 5**

Cada usuário formaliza o seu conhecimento dos regulamentos da organização em relação à segurança da informação através da assinatura de documento?

**Nota:** 1

**Justificativa:**

Não existe documento direcionado à segurança da informação.

**Possível solução:**

Criação do mesmo.

### 7.1.3 Segurança Lógica

**Pergunta 1**

A identificação do usuário é única e individual para qualquer tipo de usuário?

**Nota:** 9

**Justificativa:**

Cada usuário possui a sua senha com regras próprias de criação com o intuito de deixá-las ainda mais seguras

**Solução proposta:**

Não se aplica

**Pergunta 2**

Existe a garantia da não existência de identificações genéricas?

**Nota:** 8

**Justificativa:**

As identificações genéricas são utilizadas apenas pelo pessoal da InfraEstrutura e apenas eles tem acesso a esses usuários.

**Solução proposta:**

Não se aplica.

**Pergunta 3**

Em situações de exceção em que programas ou similar precisam ter identificação, existe um processo formalizado para garantir que essa situação será registrada e possui restrição ao uso?

**Nota:** 7

**Justificativa:**

Para programas de acesso remoto aos clientes por exemplo, existe uma documentação formalizada para cada cliente. Algumas situações não possuem processo formalizado.

**Solução proposta:**

**Pergunta 4**

A cadeia de caracteres que formam a identificação do usuário possibilita a ligação com os dados complementares e descritivos do usuário?

**Nota:** 9

**Justificativa:**

O processo está implementado. O login do usuário no sistema em alguns acesso são as iniciais do seu nome e em outros são a concatenação do nome e sobrenome separados por um caracter específico.

**Solução proposta:**

Não se aplica

**Pergunta 5**

Quando a autenticação é feita através de senha, essa senha é secreta e de conhecimento exclusivamente do usuário?

**Nota:** 9

**Justificativa:**

A senha é de conhecimento apenas do usuário. Ainda é possível a alteração da mesma caso ele esqueça via administrador de acesso.

**Solução proposta:**

Não se aplica

**Pergunta 6**

É declarado nas políticas que o usuário é responsável pelo acesso realizado com a sua identificação e autenticação?

**Nota:** 5

**Justificativa:**

Não existem políticas que deixem explícitas as responsabilidades de cada usuário. Sabe-se por bom senso.

**Solução proposta:**

Criação de uma política de segurança da informação na qual deixe claro as responsabilidades, direitos e deveres de cada um de modo a contribuir com a segurança da informação da empresa.

**Pergunta 7**

Todo acesso realizado ou tentativa de acesso ao/no ambiente computacional é gravado e guardado durante um tempo previamente definido pela segurança da informação?

**Nota: 1**

**Justificativa:**

Os logs internos são gravados mas os externos não.

**Solução proposta:**

**Pergunta 8**

Existe formalmente a função de gestor da informação, que é a pessoa que autoriza (ou não) o acesso à informação por qualquer pessoa da organização?

**Nota:** 1
**Justificativa:**
A função do gestor da informação é desempenhada pela equipe de Infra Estrutura da Empresa. Não existe um gestor definido.
**Solução proposta:**
Definição de um gestor ou a contratação de um funcionário para assumir o cargo para que ele organize melhor a informação com um processo de segurança da informação descentralizado e concentrado em responsáveis.

**Pergunta 9**
O gestor da informação foi formalizado pelo processo de segurança da informação e é de conhecimento de todas as pessoas a sua existência e responsabilidade?
**Nota:** 0
**Justificativa:**
Não se aplica pois não existe o gestor da informação.
**Solução proposta:**
Criação do cargo de gestor da informação e seleção de um funcionário para o cargo a fim de suprimir as devidas necessidades da empresa.

**Pergunta 10**
A informação é liberada para o usuário após a autorização do gestor da informação?
**Nota:** 8
**Justificativa:**
Mesmo não havendo o gestor da informação, há um processo para a autorização do acesso à informação gerido por outras pessoas. Varia dentro de cada diretoria este responsável.
**Justificativa:**
Este processo é realizado pela equipe de Infra Estrutura da Empresa.
**Solução proposta:** Criação de um gestor para centralizar essa necessidade.

**Pergunta 11**
O processo de liberação de acesso da informação para o usuário é formalizado e registrado, permitindo auditoria?
**Nota:** 9
**Justificativa:**

O usuário, após concluído o processo de inclusão no sistema, é notificado por email a respeito da sua inclusão com data, cumprimentos de boas vindas e outros detalhes.

**Solução proposta:**

Não se aplica.

**Pergunta 12**

Existe um processo de revalidação periódica pelo gestor, dos usuários que estão autorizados a acessar a informação que esse gestor autoriza?

**Nota:** 0

**Justificativa:**

Não há gestor. (A equipe da Infra verifica os usuários ativos e inativos na Rede Interna)

**Solução proposta:**

Criação do cargo e nomeação de uma pessoa para assumí-lo.

**Pergunta 13**

Existe um processo automático que retire os acessos do usuário quando ele é transferido para outra área organizacional?

**Nota:** 4

**Justificativa:**

Há casos em que funcionários trocaram de setores e ainda continuaram a receber emails de outros setores assim como a permissão de acesso à informação dos mesmos.

**Solução proposta:**

Melhorar o processo para que quando haja troca de funcionários dentro de setores da empresa, o seu acesso seja validado automaticamente com as devidas permissões atuais.

**Pergunta 14**

Existe um processo automático que retire (ou suspenda) a identificação do usuário quando ele encerra seu relacionamento profissional com a organização?

**Nota:** 9

**Justificativa:**

Quando um funcionário é desligado da organização seus acessos são excluídos e a sua senha do alarme como suas digitais são apagadas.

**Solução proposta:**

Não se aplica.

**Pergunta 15**

Existe um processo de gestão da identidade de usuário, garantindo o padrão de tratamento da identidade para todas as plataformas de tecnologia?
**Nota:** 9
**Justificativa:**
O acesso dos usuários nas tecnologias da organização são baseadas nos padrões das senhas. Seja por nome e sobrenome separados por caracter específico, email ou sigla com as iniciais do nome. Existem locais que podem ser acessados para descobrir quem é o usuário tanto por email quanto por sigla.
**Solução proposta:**
Não se aplica.

**Pergunta 16**
Existe uma gestão de autenticação de usuário que defina os requisitos mais ou menos rígidos para a autenticação do usuário, dependendo do canal de acesso ou equipamento que o usuário está utilizando?
**Nota:** 4
**Justificativa:**
Para rede Interna existe as políticas do Servidor de Dominio. Ferramentas utilizadas pela empresa utilizam níveis de acesso configuráveis de acordo com a função.
**Solução proposta:**

**Pergunta 17**
Quando do uso de senhas, o arquivo de senhas é criptografado?
**Nota:** 9
**Justificativa:**
Sim. O arquivo de senhas é criptografado com o algoritmo MD5. Tal algoritmo é confiável pois ele é só de ida, ou seja, não se consegue descobrir a senha por processo reverso de algoritmo. A única tentativa é por ataque de dicionário, que minimiza e muito as chances de um atacante descobri-la.
**Solução proposta:**
Não se aplica.

**Pergunta 18**
Existe uma política para a definição de uso(ou não) de criptografia quando do armazenamento, apresentação e transmissão de dados?
**Nota:** 4
**Justificativa:**
Apenas para transmissão de dados
**Solução proposta:**

**Pergunta 19**

Quando do uso de criptografia, foi considerada a situação de perda de chaves e o impacto dessa situação?
**Nota: 1**
**Justificativa:**
Não existe
**Solução proposta:**

**Pergunta 20**
Quando do uso de criptografia no ambiente computacional principal da organização, foi definida a forma de guarda das chaves?
**Nota: 1**
**Justificativa:**
Não existe
**Solução proposta:**

**Pergunta 21**
Quando existe tratamento de dados da organização por parte de prestadores de serviço, é garantido que esses terceiros possuem o mesmo nível de proteção da organização?
**Nota: 7**
**Justificativa:**
O prestador é acompanhado por alguém e somente os acessos necessários a estrutura da organização são concedidos. O SLA(acordo de nível de serviço) é realizado.
**Solução proposta:**