WARLISSON COSTA DE OLIVEIRA

IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA EMPRESA PNEUCAR COM BASE NAS DIRETRIZES DA ABNT NBR ISO/IEC 27005

BACHARELADO

EM

CIÊNCIA DA COMPUTAÇÃO

FIC - CARATINGA

2017

WARLISSON COSTA DE OLIVEIRA

IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA EMPRESA PNEUCAR COM BASE NAS DIRETRIZES DA ABNT NBR ISO/IEC 27005

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

2017

rede de ensino DOCTUM

FACULDADES INTEGRADAS DE CARATINGA

FOLHA DE APROVAÇÃO

O trabalho de Conclusão de Curso intitulado: IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA EMPRESA PNEUCAR COM BASE NA ABNT NBR ISO/IEC 27005, elaborado pelo aluno WARLISSON COSTA DE OLIVEIRA foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de Ciência da Computação das Faculdades Integradas de Caratinga, como requisito parcial da obtenção do título de

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Caratinga, 14 de Dezembro 2017

Prof. Wanderson Miranda Nascimento

Prof. Jonilson Batista Campos

Prof. Vagner Aquino Zeferino

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me dado forças e abençoado a minha vida, e todo este meu caminho para chegar até este momento.

Agradeço aos meus pais Wanderley e Maria Helena que nunca deixaram de me apoiar e sempre estiveram ao meu lado. Aos meus avós Getúlio e Nilza que sempre rezaram por mim e que se não fosse por eles eu não estaria realizando mais essa conquista em minha vida.

A minha namorada Grazieny que sempre me incentivou e está ao meu lado a todo momento. Agradeço também a todos meus familiares, amigos e colegas pelo apoio que recebi deles para chegar até aqui.

Agradeço ao professor Wanderson Miranda que foi ainda mais um orientador, demonstrando boa vontade, interesse e auxiliou com excelência na realização deste trabalho.

E por último, mas não menos importante, agradeço a todos os professores que desde o início do curso, ajudaram a trilhar todo este caminho.

Ao Sr. Gladson Ramalho, que permitiu que pudesse utilizar as dependências da sua empresa que foi fator chave para a realização deste trabalho.

Obrigado a todos por terem contribuído para essa conquista.

Ainda que eu ande pelo vale da sombra da morte, não temerei mal algum, pois tu estás comigo. Salmos 23:4

RESUMO

Segurança da informação é um assunto que as empresas devem dar importância. Atualmente existem muitas brechas que por mínimas que são, podem dar caminho para que uma pessoa com atitudes maliciosas cause diversos prejuízos a organizações de pequeno, médio e grande porte. Existem diversas ferramentas e métodos para garantir a segurança da informação em uma rede de computadores, vale lembrar que para um ambiente seguro, é necessário a colaboração de todos os envolvidos. Com auxílio da tecnologia e do ambiente a segurança pode ser garantida de forma satisfatória. Este estudo baseia-se nas normas propostas pela ABNT NBR ISO/IEC 27005 para analisar de forma exploratória a rede de computadores de uma empresa e aplicar políticas de segurança com base nos resultados dessa análise, tendo foco aos usuários, visando baixo custo por isso utilizando apenas os recursos presentes no ambiente com restrições que a administração da empresa julgar necessário. O intuito deste estudo é melhorar a segurança das informações, afim de minimizar a incidência e os impactos das vulnerabilidades existentes. Este problema será explorado com um estudo de caso realizado, afim de coletar informações com as técnicas e padrões especificados na ISO de estudo.

Palavras chaves: Políticas de segurança, Segurança da informação, redes de computadores.

ABSTRACT

Information security is a matter that companies should attach importance to, there are currently many loopholes that, however minimal, give way for a person with malicious attitudes to generate a lot of damage to small, medium and large organizations. There are several tools and methods to ensure the security of information in a computer network, it is worth remembering that for a safe environment, the collaboration of all involved is necessary. With the aid of technology and the environment, safety can be guaranteed satisfactorily. This study is based on the norms proposed by ABNT NBR ISO / IEC 27005 to analyze in an exploratory way the computer network of a company and to apply security policies, focusing on users, aiming at low cost, using only the resources present in the company and restrictions that management deems necessary to improve environmental safety. The purpose of this study is to improve information security in order to minimize the incidence and impacts of existing vulnerabilities. This problem will be explored with a case study carried out in order to collect information with the techniques and standards specified in the study ISO.

Key words: Security policies, Information security, computer networks.

LISTA DE FIGURAS

Figura 1. Gestão de riscos ISO 27005 19
Figura 2. Amarração IP e MAC 42
Figura 3. Configuração IP e MAC 42
Figura 4. Configuração limite de banda de internet 44
Figura 5. Relação de limite de internet por máquina 44
Figura 6. Sistema PPPR 45
Figura 7. Log sistema PPPR 46
Figura 8. Editor de registro do Windows 48
Figura 9. Alteração de registro do Windows 49
Figura 10. Conexões com a rede de computadores 50
Figura 11. Antivírus Kaspersky 51
Figura 12. Ferramentas do Antivírus Kaspersky 52
Figura 13. Configuração de verificação do Antivírus Kaspersky 53
Figura 14. Sistema de backup ProBKP 54
Figura 15. Configuração do Sistema de backup ProBKP 55
Figura 16. Resultado dos backups do Sistema ProBKP 55
Figura 17. Pendrives para armazenamento dos backups do Sistema 56
Figura 18. Upload do arquivo de backup 57
Figura 19. Painel do Google Drive 58
Figura 20. Execução do ping 64

LISTA DE TABELAS

Tabela 1. Critério de Impacto 32
Tabela 2. Critério para aceitação de risco 32
Tabela 3. Nível de impacto 33
Tabela 4. Critério de probabilidade de incidente 33
Tabela 5. Classificação do nível de probabilidade de incidente 34
Tabela 6. Análise e classificação dos riscos 37
Tabela 7. Critério para avaliação do risco 38
Tabela 8. Riscos por prioridade 39

LISTA DE GRÁFICOS

Gráfico 1. Medidas de segurança tomadas pela empresa 65
Gráfico 2. Bloqueios de mídias e acesso à internet 66
Gráfico 3. Qualidade atual da rede de computadores 67
Gráfico 4. Regras aplicadas a rede wi-fi 67
Gráfico 5. Reestabelecimento dos serviços 68
Gráfico 6. Usabilidade das políticas para realizar o trabalho 69
Gráfico 7. Viabilidade das políticas de segurança na empresa 69
Gráfico 8. O acesso aos sistemas que utiliza. 70
Gráfico 9. Necessidade que a empresa efetua mudanças na rede de computadores 71
Gráfico 10. Necessidade de investimento em segurança da informação 71
Gráfico 11. As políticas prejudicaram os serviços 72
Gráfico 12. Importância da segurança da informação para a empresa 73
Gráfico 13. Necessidade de melhorar em segurança da informação 73
Gráfico 14. A importância das informações e orientações sobre segurança da informação 74
Gráfico 15. Responsabilidade para manter a segurança das informações da empresa ... 74
Gráfico 16. Responsabilidade para manter a segurança das próprias informações na empresa 75
Gráfico 17. Qualidade dos serviços prestados 76

LISTA DE SIGLAS

ABNT / NBR – Associação Brasileira de Normas Técnicas

CF – Cupom Fiscal

CPU - *Central Processing Unit*

DHCP – *Dynamic Host Configuration Protocol*

DNS - *Domain Name System*

GBPS – Gigabits por segundo

HD - *Hard Drive*

HTTP - *Hyper Text Transfer Protocol*

HTTPS - *Hyper Text Transfer Protocol Secure*

ID - *Identification*

IEC - *International Electrotechnical Commission*

IP - *Internet Protocol*

ISO - *International Organization of Standardization*

ISP - *Internet service provider*

MAC - *Media Access Control*

MBPS – Megabits por segundo

NFe – Nota Fiscal Eletrônica

PPPR – Pacote Personalizado Prodata Retaguarda

SGBD - Sistema de Gerenciamento de Banco de Dados

SQL - *Structured Query Language*

TCP - *Transmission Control Protocol*

TI – Tecnologia da Informação

USB - *Universal Serial Bus*

SUMÁRIO

INTRODUÇÃO 14
1. REFERENCIAL TEÓRICO 16
1.1 Sistemas de Gerenciamento de Segurança da Informação 16
1.2 Segurança da Informação 17
1.3 Análise de falhas e riscos ISO 27005 18
1.4 Definição de Escopo 20
1.4.1 Critérios de risco 22
1.4.2 Critérios de avaliação de riscos 22
1.4.3 Critérios de impacto 22
1.4.4 Critérios de aceitação do risco 22
1.5 Análise e avaliação de riscos 23
1.5.1 Análise de riscos 23
1.5.2 Identificação de riscos 23
1.5.3 Identificação dos ativos 23
1.5.4 Identificação das consequências 23
1.5.5 Identificação das vulnerabilidades 24
1.5.6 Estimativa de riscos 24
1.5.7 Avaliação de riscos 24
1.6 Redes de Computadores 25
1.7 Google Drive 25
1.8 Kaspersky Antivírus 26
2. METODOLOGIA 27
2.1 OBJETO DE ESTUDO 27
2.2 AMBIENTE DE ESTUDO 28

2.3 ANÁLISE DE FALHAS E RISCOS 29
2.3.1 Definição de contexto 29
2.3.2 Definição de critérios para avaliação de risco 31
2.3.3 Análise dos riscos identificados 32
2.3.4 Análise de probabilidade de riscos 33
2.3.5 Classificação por nível de risco 34
2.3.6 Tabela de riscos por prioridade 38
2.3.7 Início da implantação das políticas 40
2.4 IMPLANTAÇÃO DAS POLÍTICAS DE SEGURANÇA 40
2.4.1 Políticas de uso da internet 41
2.4.2 Limitação de banda de internet 43
2.4.3 Políticas de Senha 45
2.4.4 Políticas de segurança com e-mail 46
2.4.5 Políticas de uso do computador de trabalho 47
2.4.6 Políticas de acesso à rede wireless 49
2.4.7 Políticas com antivírus 51
2.4.8 Políticas de backup 53
3. ANÁLISE DOS RESULTADOS 59
3.1 Análise de falhas e riscos com base na ABNT NBR ISO/IEC 27005 59
3.1.1 Conformidade com a ISO 60
3.2 Sobre as políticas de segurança 62
3.3 Responsabilidade dos envolvidos 62
3.4 Testes das políticas de segurança 63
3.4.1 Ping 63
3.4.2 Bloqueios nos computadores de trabalho 64
3.5 Questionário de segurança da informação 65
4. CONCLUSÕES 77

4.1 Trabalhos Futuros 78

REFERÊNCIAS 80

ANEXOS 82

Anexo 1 - Autorização da empresa para aplicação do trabalho. 82

Anexo 2 - Mapa da rede de computadores da empresa 83

Anexo 3 - Termo de responsabilidade – Políticas de Segurança 84

Anexo 4 - Questionário para avaliação das políticas implementadas 89

INTRODUÇÃO

Segurança da informação é um assunto bastante sério, fazendo uma pesquisa sobre, é notável o volume de conteúdo, eventos e novidades dentro da tecnologia, porém atualmente mesmo sendo muito importante ainda existem empresas e pessoas que ignoram cuidados simples que podem garantir o mínimo disso. Mesmo uma pessoa que usa seu computador apenas para acessar à internet, corre risco de perder suas informações como também empresas que guardam informações de extremo sigilo.

Atualmente vemos com mais frequência notícias de invasões e infecções aos dados de empresas devido a arquivos ou pessoas com atitudes maliciosas, várias empresas no mundo já registraram esse tipo de incidente. Países como Brasil, Portugal, Espanha, e Reino unido identificaram computadores infectados com o vírus tipo "*ransomware*" que funciona como um sequestro de dados ou do próprio equipamento bloqueando os dados até que seja feito o pagamento pelo resgate dessas informações. Com isso é cada vez mais necessário se preocupar e manter um nível adequado de segurança com as informações (O GLOBO, 2017).

A ABNT NBR ISO/IEC 27005 é uma norma técnica voltada para Gestão de Riscos da Segurança da Informação. Aplicando suas técnicas é possível identificar as falhas em uma rede de dados de pequeno, médio e grande porte, podendo fazer a identificação, estimativa e avaliação de riscos, com isso é mais fácil verificar as possíveis soluções para as vulnerabilidades encontradas, para garantir maior segurança no fluxo de dados.

Este trabalho colheu resultados e foi realizado na empresa Pneucar situada em Caratinga-MG que presta serviços automotivos. A empresa foi escolhida pois ainda não havia sido feito uma análise de segurança em seu ambiente, com isso existia a possibilidade de haver vulnerabilidades na rede de computadores, outro ponto que também diferencia este ambiente é a ausência de políticas de segurança da informação.

O objetivo geral do trabalho foi implementar políticas de segurança da informação com base em uma análise de falhas e riscos na rede de computadores a partir de diretrizes da ABNT NBR ISO/IEC 27005, com finalidade de melhorar a segurança da informação e diminuir o impacto e a incidência de falhas encontradas nesse ambiente visando também o menor custo financeiro para implantação.

A utilização da ISO é o diferencial para realização este trabalho, sua utilização não é tem finalidade de obter alguma certificação, mas a norma foi escolhida, porque tem diretrizes que seguem passos minuciosos para uma análise com maior qualidade de resultados.

No primeiro capítulo estão os estudos necessários para realizar este trabalho que relacionam a norma ABNT NBR ISO/IEC 27005, segurança da informação, redes de computadores e políticas de segurança da informação. Os demais capítulos estão distribuídos da seguinte forma:

Capítulo 2: Metodologia

A) Formular escopo de análise do ambiente.
B) Efetuar análise de falhas com base na ISO 27005.
C) Aplicar as políticas no ambiente.
D) Formular um termo de políticas de segurança em conjunto com a administração da empresa.

Capítulo 3: Resultados

E) Resultados obtidos.
F) Testes de ambiente

Para analisar os resultados foi realizado um questionário aplicado pelo próprio autor aos funcionários da empresa, dessa forma foi possível saber como as pessoas que trabalham diretamente com a rede avaliam as políticas e restrições que foram aplicadas. E também é possível encontrar os testes realizados de acordo com os bloqueios realizados na rede.

Capitulo 4: Conclusões

G) Conclusões finais

Neste capítulo está descrito as conclusões do autor sobre o trabalho finalizado juntamente com as sugestões de trabalhos futuros.

1. REFERENCIAL TEÓRICO

As seções abordadas a seguir foram base para estudo realizado e contextualizam os principais conceitos que estão envolvidos neste trabalho.

1.1 Sistemas de Gerenciamento de Segurança da Informação

Segundo a Associação Brasileira de Normas Técnicas - ABNT NBR ISO/IEC 27003 para uma empresa organização a informação é de extrema importância e por isso é necessário garantir que seja protegida. Com a segurança da informação é possível obter uma proteção com diversos tipos. Para a implantação de um SGSI, deve se justificar a sua necessidade, devem incluir os objetivos a serem realizados e definir prioridades para criar o plano inicial.

> A norma descreve o processo de especificação e projeto do SGSI desde a concepção até a elaboração dos planos de implantação. Ela descreve o processo de obter a aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI (referenciado nesta Norma como o projeto SGSI), e fornece diretrizes sobre como planejar o projeto do SGSI, resultando em um plano final para implantação do projeto do SGSI. (ABNT NBR ISO/IEC 27003:2011 Versão Corrigida:2015)

A implantação de um SGSI é de muita importância e normalmente é implementada no ambiente empresarial de forma inicial como um projeto. Todas as seções são similares, a mesma possui cinco fases que são:

a). Obtendo aprovação da direção para iniciar o projeto do SGSI (Seção 5);

b). Definindo o escopo do SGSI, limites e a política do SGSI (Seção 6);

c). Conduzindo a análise dos requisitos de segurança da informação (Seção 7);

d). Conduzindo a análise/avaliação de riscos e planejando o tratamento do risco (Seção 8);

e). Definindo o SGSI (Seção 9).

De acordo com a Norma ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação define as diretrizes para o processo de gestão de riscos de segurança da informação que explora a possibilidade de uma ameaça se aproveitar das vulnerabilidades de um ativo ou de um conjunto de ativos de um ambiente empresarial, e com isso prejudique a organização, porém vale ressaltar que se existe no ambiente um ativo vulnerável, mas não possua ameaça capaz de o explorar, então não há risco.

A norma recomenda um roteiro para suas seções, são os seguintes passos de análise:

- Ação de evitar o risco – decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.
- Comunicação do risco – troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes envolvidas.
- Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e consequências de um risco.
- Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.
- Redução do risco – ações tomadas para reduzir a probabilidade, as consequências negativas ou ambas associadas a um risco.
- Retenção do risco – aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.
- Transferência do risco – compartilhamento com uma outra entidade do ônus da perda associado a um risco

1.2 Segurança da Informação

De acordo com o artigo segurança da informação por autoria de Adrielle Fernanda, publicado em março de 2011, para se implantar um projeto de segurança da informação no ambiente corporativo é necessário estabelecer diretrizes, mecanismos de segurança, políticas e procedimentos, ferramentas de proteção e autenticação, e analisar o custo benefício de uso das mesmas. A segurança deve restringir o acesso dos funcionários apenas a conteúdos que lhe são permitidos; de forma que nenhum colaborador de setores diferentes poderá acessar uma informação que não for do seu

mesmo setor ou que não tenha nenhuma necessidade ou relação com o serviço que desempenha. A autora ainda afirma que garantir o melhor nível de segurança é fundamental.

> As ameaças à segurança podem ser de diferentes formas como incêndios, inundações, falhas de energia, sabotagem, vandalismo, roubo e outros. O uso da Internet nas organizações trouxe novas vulnerabilidades na rede interna. Se não bastassem as preocupações existentes com espionagem comercial, fraudes, erros e acidentes, agora as empresas também precisam se preocupar com os hackers, invasões, vírus e outras ameaças que penetram através desta nova porta de acesso. (FERNANDA, Adrielle. Mar 2011. Disponível em: <http://www.ice.edu.br>)

No artigo ela reforça alguns passos que devem ser concretizados para a implementação de uma política de segurança da informação:

• Riscos associados à falta de segurança;

• Benefícios;

• Custos de implementação dos mecanismos.

1.3 Análise de falhas e riscos ISO 27005

A ISO 27005 fornece as diretrizes para o gerenciamento dos riscos de segurança da informação (SI) e também dá ênfase aos conceitos aplicados na ISO 27001:2005, que é uma norma de requisitos de sistemas de gestão da SI, e também auxilia na implementação e certificação de novos sistemas de gestão.

A imagem a seguir mostra as atividades que compõem o processo de gestão de riscos de SI.

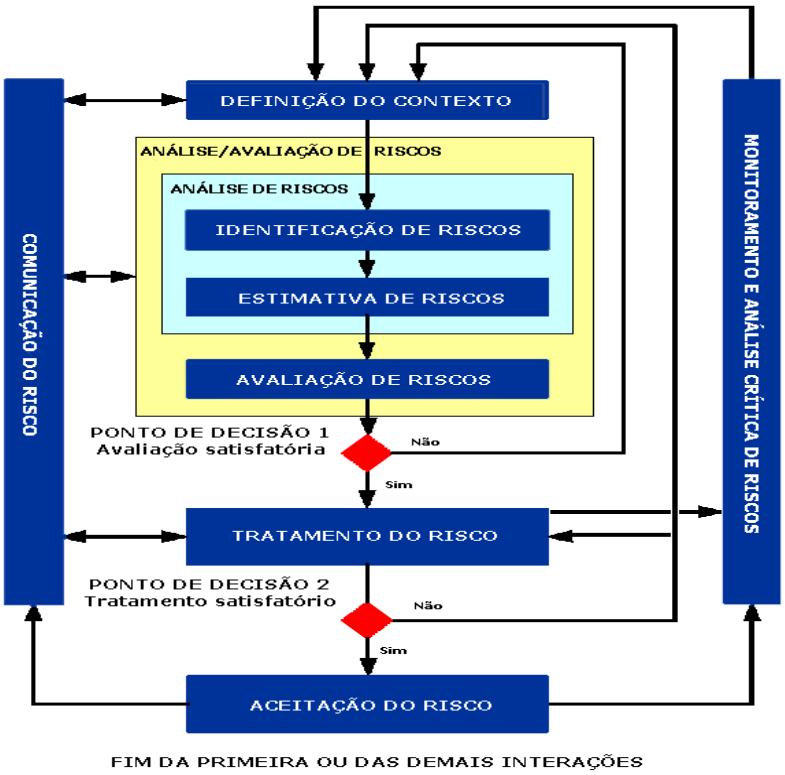


Figura 1. Gestão de riscos ISO 27005

Fonte: http://www.qsp.org.br, 2017

O material que será seguido para a análise do ambiente da empresa garantindo a conformidade com a norma ISO/IEC 27005, é mostrado a seguir:

- Definição de contexto: Definição do escopo do ambiente analisado, critério dos riscos e informações (Ativos afetados, pontos vulneráveis);
- Análise de riscos: Identificação dos riscos, estimativa e avaliação.
- Tratamento: Utiliza a ação definida na análise de riscos e é iniciado apenas se houver recursos, e se a análise for de forma satisfatória;

Serão abordadas neste projeto, apenas estas atividades restantes do processo de análise dos riscos, as demais etapas vão seguir as orientações da ISO/IEC 27005.

1.4 Definição de Escopo

O processo de análise de riscos inclui algumas decisões em termos de compreensão. O escopo é um conjunto de ativos, ameaças e vulnerabilidades que serão analisados com base na ISO. Um detalhe para iniciar um escopo em um ambiente organizacional que está sendo analisado é o tamanho do escopo definido. Pequenos escopos podem não ser eficazes por não conter todos os ativos importantes da empresa, já os escopos gigantes podem gerar processos que nunca acabam.

Para definir o escopo, será utilizado este documento que é abordado na ISO 27005, conforme é mostrado abaixo:

I – Análise da organização

Propósito principal da organização: O seu propósito pode ser definido como a razão pela qual a organização existe (sua área de atividade, seu segmento de mercado etc.)
Negócio: É necessário especificar à área de atividade da organização. Para definir o negócio de uma empresa, pode ser verificado pelas técnicas utilizadas e o know-how de seus funcionários, isso torna viável o cumprimento de sua missão.
Missão: A organização atinge seu propósito ao cumprir sua missão. Para bem identifica-la, convém que os serviços prestados e/ou produtos manufaturados sejam relacionados aos seus públicos-alvo.
Valores: Valores consistem de princípios fundamentais ou de um código de conduta bem definido, aplicados na rotina de um negócio, podem incluir os recursos humanos, as relações com agentes externos (clientes e outros), a qualidade dos produtos fornecidos ou dos serviços prestados.
Organograma: É desenhado um organograma contendo a estrutura da esquematizada da empresa demonstrando como funciona a relação dos setores. É necessário que na representação fique bem claro quem se reporta a quem, se houver, também é interessante incluir outros tipos de relacionamentos, visando que esses relacionamentos também podem participar do fluxo de informação.
Estratégia: Ela requer a expressão formalizada dos princípios que norteiam a organização. A estratégia determina a direção e o desenvolvimento necessários para que

a organização possa se beneficiar das questões em pauta e das principais mudanças sendo planejadas.

II – Restrições que afetam a organização: Demonstra as restrições que determinam o direcionamento da segurança da informação e que podem afetar sejam consideradas.

III – **Legislações e regulamentações aplicáveis à organização:** Convém que sejam identificados os requisitos de regulamentação que podem ser aplicáveis à empresa. Podem ser consistidos em leis ou decretos específicos que dizem respeito à área de atividade da organização ou regulamentos internos e externos. Englobam também contratos, acordos de natureza legal ou regulatória.

IV – **Restrições que afetam o escopo:** Ao identificar as restrições é possível enumerar aquelas que causam um impacto no escopo e determinar quais são passíveis de intervenção. Elas complementam e talvez venham a corrigir as restrições da organização discutidas mais acima.

V – **Identificação de ativos:** Para estabelecer o valor de seus ativos, uma organização precisa primeiro identifica-los (num nível de detalhamento adequado).

Para realizar este estudo, foi usado como base a ISO/IEC 27005 que possui regras para gestão de riscos de segurança da informação (GRSI). Para executar estes métodos como a proposta no projeto de pesquisa, o objetivo é analisar com base na ISO os pontos vulneráveis de segurança da informação na rede de computadores da empresa para que aconteça a criação de uma política de segurança, afim de melhorar o nível de segurança da empresa, mas não garantindo que vá impedir todos os tipos de riscos que possam ocorrer. Desta forma é uma solução para o problema de falta de regras de segurança na rede da empesa.

Neste projeto, a organização será analisada com foco no negócio e o ambiente operacional e pouco sobre os componentes tecnológicos, será analisado com maior foco a parte social, regras para os colaboradores da empresa, mas não será excluído totalmente a parte tecnológica, visando que para implantar uma política de segurança a parte tecnológica será de grande importância para realização de algumas seções. Os riscos encontrados serão classificados por categorias e níveis, e o objetivo é de indicar ao controle da empresa as características voltadas para a gerência.

1.4.1 Critérios de risco

Conforme o escopo que foi formado os objetivos da análise pode ser aplicados de forma diferente, um método para uma GRSI deve possuir pelo menos os critérios básicos como critérios de avaliação de riscos, critérios de impacto e critérios de aceitação de risco, para caracterizar e organizar estes critérios, as informações serão preenchidas nas tabelas de base para caracterização que a ISO 27005 informa.

1.4.2 Critérios de avaliação de riscos

De acordo com a ISO 27005 os critérios de avaliação de risco devem ser desenvolvidos para avaliar os riscos de segurança da informação no ambiente em questão levando em consideração alguns fatores como a importância dos processos operacionais e dos negócios, da disponibilidade, confidencialidades e da integridade.

1.4.3 Critérios de impacto

Os desenvolvimentos dos critérios de impacto são desenvolvidos de acordo com os danos ou custos que os mesmos causam para a empresa de acordo com um acontecimento que esteja relacionado com a segurança da informação. É este critério que vai determinar o tamanho do impacto ou consequências de determinado incidente também incluindo o valor de reposição do ativo danificado em relação ao tempo de parada ou até de perda das funções deste mesmo ativo.

1.4.4 Critérios de aceitação do risco

De acordo com a ISO 27005, os critérios definidos para a aceitação do risco que forem desenvolvidos sejam especificados e essa aceitação, os mesmos vão depender das políticas ou particularidades, meta e objetivos da empresa em questão, assim como os interesses das partes envolvidas. Após a aceitação do risco, se algum incidente ocorrer com relação ao mesmo, a responsabilidade é total das partes envolvidas que definiram estes critérios.

1.5 Análise e avaliação de riscos

1.5.1 Análise de riscos

Nessa fase são desenvolvidos os critérios para a avaliação dos riscos. Com base na ISO 27005, a análise de riscos demonstra que os riscos sejam identificados, descritos com mais detalhes, e se necessário priorizados. É responsabilidade da empresa selecionar um método próprio para tratar os riscos com base na meta da análise. Durante o processo de análise os ativos, ameaças, vulnerabilidades são analisados de forma mais complexa. Este estudo é para definir o nível de risco, nível de probabilidade de acontecimentos e nível de impacto do mesmo caso venha a acontecer.

1.5.2 Identificação de riscos

Nesta etapa que os ativos da organização são identificados e relacionados com as ameaças, vulnerabilidades e consequências, obedecendo o escopo que foi desenvolvido, é a fase da identificação dos riscos, assim é possível medir o impacto do mesmo após identificado.

1.5.3 Identificação dos ativos

Com base na norma da ISO 27005, para identificar um ativo é necessário que estes sejam estabelecidos dentro do escopo sugerindo que sejam classificados conforme a seguir:

•Ativos primários: informações e processos de negócio;

•Ativos de suporte e infraestrutura: *hardware*, *software*, rede, recursos humanos, instalações físicas e estrutura da organização.

1.5.4 Identificação das consequências

A identificação das consequências relaciona a mesma com a perda de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos que

podem ser danificados. A ISO 27005 propõe que as organizações identifiquem as consequências operacionais de acordo com o cenário de cada acontecimento.

1.5.5 Identificação das vulnerabilidades

Entende-se por vulnerabilidades as fragilidades que podem prejudicar de alguma forma quando são atingidas pelas ameaças à segurança de um ambiente. Nesta etapa foi identificado as vulnerabilidades que podem ocorrer na área da rede de computadores da organização. São processos e procedimentos que existiam que deixavam estas falhas no ambiente. De acordo com a ISO 27005, quando identificado uma das consequências de vulnerabilidade e não houver algo que minimize essa possibilidade, é provável que ocorra a perda de confidencialidade, de integridade e de disponibilidade de informações.

1.5.6 Estimativa de riscos

É possível realizar uma análise da estimativa caracterizando as informações obtidas como qualitativa ou quantitativa. Essa etapa consiste em 3 atividades: avaliação das consequências, avaliação da probabilidade dos incidentes e estimativas dos níveis de risco. Ao avaliar as consequências e obter o valor para o nível de impacto (NI) é levado em conta o valor necessário para substituir o ativo e a consequência caso o mesmo seja perdido e também em consideração ao tempo que o mesmo será parado.

1.5.7 Avaliação de riscos

Nessa etapa é onde será tomada a decisão sobre as ações da empresa, de acordo com as prioridades para tratar os riscos levando em conta também os critérios definidos durante o escopo do projeto. A atividade de avaliação de risco finaliza com uma lista dos riscos encontrados por prioridade de tratamento.

1.6 Redes de Computadores

Define se rede de computadores como um conjunto de máquinas autônomas que são interconectados por um meio de conexão, seja ele por cabo ou rede sem fio. As redes de computadores surgiram a partir da necessidade de que informações que estão localizadas fisicamente distantes pudessem se conectar.

É necessário entender como uma rede de computadores é gerenciada e de onde surge a necessidade de promover a segurança das informações que nela estão. Com 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.

1.7 Google Drive

O *Google Drive* é um serviço de armazenamento de arquivos em nuvem que funciona de forma online e gratuita, podendo também ser contratado o serviço de forma paga afim de aumentar o espaço de armazenamento. A versão gratuita do Drive conta com 15GB de armazenamento, além de ser totalmente compatível com as outras ferramentas do *google* como por exemplo o e-mail.

Este serviço conta com a possibilidade de armazenar arquivos de diversos tipos de extensão. Com ele também existe o aplicativo de backup e sincronização, que será tratado neste trabalho. A ferramenta sincroniza automaticamente com a nuvem as informações guardadas em um computador ou pasta em específico. Tem funcionamento para outras plataformas de sistema operacional como *Windows, Android, IOS* e também por acesso em página da web. Aqui será mostrado algumas das vantagens do *google* Drive em relação aos outros serviços de armazenamento em nuvem.

- Clássico design dos serviços Google
- Interface intuitiva

- Possibilidade de compartilhamento e colaboração
- Organização em pastas
- Disponibiliza documentos para serem usados *off-line*

1.8 Kaspersky Antivírus

É um software anti-malware e firewall desenvolvido pela Kaspersky lab, uma empresa que atua como desenvolvedora de software e também é fabricante e vendedora de equipamentos para redes de computadores.

O produto desta empresa que é utilizado neste trabalho é o Kaspersky Internet Security que possui os componentes de proteção de seu outro produto o Kaspersky Anti-Virus junto com um serviço de *firewall*. Foi eleito a melhor solução com capacidades de auto-defesa pela Anti-Malware Test Lab.

> O Kaspersky® Internet Security previne o roubo de informação confidencial como passwords, números de contas bancárias e cartões de crédito) do seu computador. Este software detecta também mensagens de "*phishing*" e desautoriza qualquer seguimento de "*links*" que conduzam a sites de "*phishing*", também impossibilita que "*scripts*" perigosos possam ser lançados em sites visitados pelo utilizador, e bloqueia igualmente janelas "*pop-up*" e de publicidade. (Disponível em: <https://www.kaspersky.com>)

2. METODOLOGIA

2.1 OBJETO DE ESTUDO

O estudo de caso foi realizado com uma análise das falhas e riscos, utilizando como metodologia de exploração os passos descritos na ABN NBR ISO/IEC 27005, em uma empresa que atua no ramo automotivo que está situada na região de Caratinga – MG. A empresa foi escolhida para a aplicação deste trabalho ainda não havia sido realizado uma análise de vulnerabilidades no seu ambiente.

Situada na Av. Presidente Tancredo Neves no bairro Zacarias a Pneucar é uma empresa especializada no ramo de reforma e venda de pneus e prestadora de serviços de suspensão, freios, alinhamento e balanceamento de automóveis e caminhões. A Pneucar iniciou suas atividades no ano de 1980 e até hoje é uma empresa que presta serviços com muita qualidade para a população de Caratinga e região.

A Pneucar possui uma parceria com a empresa de tecnologia também situada na cidade de Caratinga-MG, essa empresa é a desenvolvedora do software de controle gerencial e fiscal (PPPR) e emissor de NF-e e geração de arquivo emissão para NFS-e e também é provedora de um dos links de internet que a empresa possui.

Atualmente o sistema de controle gerencial funciona de modo cliente servidor, os arquivos do sistema ficam hospedados na máquina cliente, mas o banco de dados está armazenado em um servidor específico que trabalha com sistema operacional Linux. O sistema, porém, ainda está em constante evolução, pois vão surgindo novas demandas sendo necessário adaptar para atender da melhor forma possível.

O sistema possui controles de usuário por níveis, também tem uma característica muito importante para a empesa que é o registro de *log's*. Essa funcionalidade foi fundamento muito importante para estabelecer parte das políticas de segurança implantadas na empresa.

O trabalho limita-se a analisar apenas a rede de computadores e seus ativos, vai incluir algumas ações que funcionários podem tomar de acordo com os parâmetros estabelecidos na norma ISO 27005, a norma especifica que para realizar um escopo de análise não é viável que seja definido um escopo muito grande, pois assim a análise gera processos que podem ser intermináveis, como se for montado um escopo muito pequeno

pode não gerar uma análise muito informativa. Dessa forma a análise cita, equipamentos de rede ou ativos físicos, ativos de informação, e ativos de software.

Após este levantamento de informações realizados na empresa, foi possível definir uma política de segurança da informação adaptada com as particularidades da empresa, mas com intenção de informar aos funcionários as mudanças e demonstrar que boas práticas no trabalho também podem garantir a segurança das informações no seu local de trabalho.

2.2 AMBIENTE DE ESTUDO

Com a análise de vulnerabilidades na empesa, foi possível fazer um levantamento das áreas onde pode-se aplicar novas regras e práticas para minimizar o impacto e a incidência dos problemas e com isso foi possível definir um grau de importância para cada situação. Esta etapa foi seguida com base nas práticas para identificação, estimativa e avaliação dos riscos descritas na ISO 27005.

Identificando por níveis cada tipo de risco, foi possível analisar uma média do tempo de inatividade nos serviços da empresa, caso venha a acontecer uma falha do tipo definido. Assim essas falhas foram classificadas desde o nível mais crítico para o menos crítico. Dessa forma com a participação da direção da empresa foi possível analisar e implementar práticas que estão presentes nas políticas de segurança que foram implantadas com intuído de evitar a reatividade aos problemas que surgirem, assegurando que a empresa poderá trabalhar com uma maior possibilidade de forma proativa.

Após as falhas identificadas, foram classificadas por níveis cada uma, assim conseguiu-se definir dentro dos parâmetros e particularidades da empresa se um risco é ou não aceitável, e informando o porquê de sua aceitação. Dentro das políticas de segurança foi possível informar como tratar as falhas existentes e acrescentar maneiras como minimizar esses impactos. Com isso foi necessário definir com a administração da empresa o que poderia deixar como aceitável. Por exemplo, o proprietário definiu que alguns funcionários não deveriam ter acesso a internet bloqueado ou previamente monitorado por uma ferramenta de firewall.

2.3 ANÁLISE DE FALHAS E RISCOS

Visando analisar com os métodos sugeridos pela ISO 27005, foi executado este estudo de caso com o ambiente da empresa Pneucar Pneus Caratinga. A empresa é composta de 30 funcionários, e atua no ramo automotivo, prestando serviços como reforma e revenda de pneus além de serviços mecânicos. Na parte de informática, a empresa conta com mais de 20 computadores operando sistemas de informática e de automação responsáveis pela parte de controle de estoque, faturamento entre outros.

Devido a particularidades da empresa, está análise irá visar somente a área de redes de computadores que irá incluir seus computadores, acesso à internet não orientados e monitorados, servidores e áreas sem restrições.

2.3.1 Definição de contexto

Passo 1 - Definir escopo do ambiente

Escopo do Ambiente

Informações da empresa

Empresa particular: Empresa Privada

Localidade: A Pneucar está situada no Bairro Zacarias da cidade de Caratinga, leste do estado de Minas Gerais

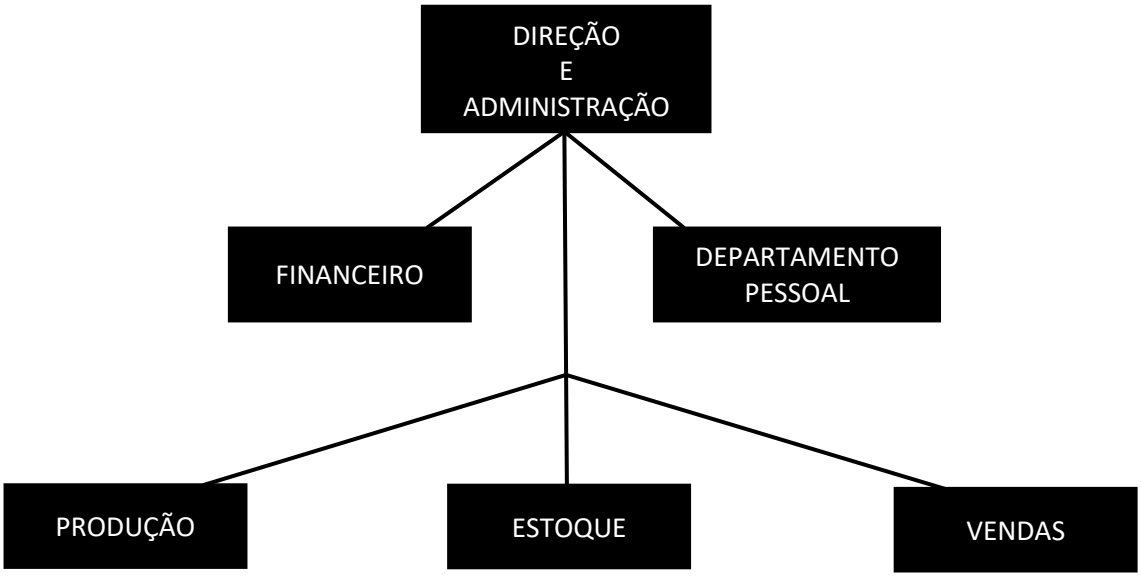
Missão: É uma empresa que possui alta qualificação no ramo de reforma e venda de Pneus, que atualmente presta serviços a outras empresas entregando produtos com a qualidade que seus clientes esperam procurando satisfaze-los da melhor forma possível.

Estratégia: Ser na região e no mercado de prestação de serviços automotivos uma empresa referência em qualidade, satisfação e ótimo atendimento aos clientes.

Valores:

- Compromisso com o cliente e seus colaboradores.
- Oferecer qualidade nos produtos e serviços prestados
- Valorização aos parceiros da empresa

Organograma:



Organograma: Organização de setores da empresa, quem reporta a quem

Fonte: O próprio autor

A empresa conta com um setor específico de direção e administração, onde os funcionários de cada setor devem reportar-se as pessoas que compõem este setor, vale lembrar que nesse setor também inclui o dono da empresa, todas as situações devem ser passadas por ele antes de ser tomada alguma decisão.

Limite de escopo: A análise feita na empresa estará limitada apenas a ativos de informações como ativos físicos, de software e de informação. Por questões de privacidade nessa análise não será citado pessoas com informações como ativo da empresa e para manter o foco na área de redes não caberá nesta análise a inclusão de ativos de serviços como falhas de faltas de energia, danos estruturais da empresa.

Restrições que afetam a organização: É uma restrição da empresa para que determinados setores não tenham nenhum tipo de acesso à internet e que também não exista nenhum tipo de bloqueio de internet em computadores de outros setores. Essas restrições foram esclarecidas diretamente com a direção da empresa, para efetuar essa análise foi necessário verificar as particularidades do ambiente.

Restrições que afetam o escopo: É uma particularidade de a empresa não haver peças de reposição de equipamentos como computadores, servidores, hardwares e dispositivos de rede reservas como roteadores.

Identificação de ativos: Para estabelecer o valor de seus ativos, uma organização precisa primeiro identifica-los (num nível de detalhamento adequado).

Ativos de informação: A empresa possui banco de dados e arquivos em servidor, documentações em papel e em arquivos digitais com informações importantes da empresa.

Ativos de software: A empresa possui um sistema integrado, denominado PPPR – Pacote Personalizado Prodata Retaguarda, que contém todas as informações de controle de estoque, controle fiscal (NFe e CF), compra e venda de produtos, informações de funcionários, fornecedores e clientes.

Ativos físicos: Existem na empresa dois servidores um para banco de dados e outro para arquivos, 20 computadores para uso dos funcionários, roteadores, switches e hubs e dispositivos de armazenamento externo.

2.3.2 Definição de critérios para avaliação de risco

Passo 2 - Definir Critérios de avaliação de risco

As tabelas utilizadas, são de referência da própria ISO proposta. Nas tabelas de classificação de riscos as informações são inseridas conforme a conformidade das informações da empresa para com a análise realizada.

Critério para avaliação de risco

Nessa tabela será informada por nível a gravidade dos riscos. Riscos graves são classificados como riscos que afetam a integridade, disponibilidade e autenticidade das informações e também que vão afetar no mal-uso de informações que afetam os envolvidos da empresa ou que possa gerar dano à imagem da empresa.

Critério de Impacto

CRITÉRIO	BAIXA	MÉDIA	ALTA
Valor de reposição do ativo	Ativos de baixo valor (Periféricos e acessórios)	Ativos com valor financeiro considerado médio e que podem ser substituídos por outros com um pouco mais de prazo de espera. (Computador)	Ativo de grande valor e de difícil reposição ou de grande demora para ser reestabelecido em sua normalidade. (Servidor de arquivos ou BD)
Consequência para o negócio relacionado a perda do ativo	Mínimo de dano possível, não causa de perda de informação.	Processos serão afetados caso ocorra a falha total do ativo, causará perda de eficiência no processo.	Podendo gerar paralização total ou parcial nos processos dependentes do sistema ou de funcionamento adequado da rede.

Tabela 1. Critério de Impacto

Critério para aceitação de risco

Nível de risco	Descrição	Aceitabilidade	Observações
Alto (15-25)	Perda de dados que possa causar a paralização nos processos da empresa ou causar dano à sua imagem.	Requer que o ativo seja corrigido imediatamente, não é aceitável riscos do tipo.	Nesse caso pode se incluir a falha de um servidor, que necessita de reposição imediata.
Médio (4-12)	Processos que podem perder sua eficiência.	Necessita de correção rápida, porém pode não causar danos graves a empresa, mas não aceitável.	Pode se incluir um roteador que dá acesso à internet para clientes, ativo que não irá causar dano grave a empresa caso venha a falhar.
Baixo (1-4)	Baixo nível de efeito.	Risco aceitável	Inclui também como risco aceitável a escolha da direção da empresa de não criar bloqueio de internet ao setor que foi permitido o uso, não existem regras de travas nem bloqueios de sites.

Tabela 2. Critério para aceitação de risco

2.3.3 Análise dos riscos identificados

Passo 3 – Efetuar análise dos riscos identificados

Análise dos riscos

A tabela a seguir mostra como é determinado o nível de impacto.

Valor de reposição	Consequência para a empresa em relação a perda do ativo	Nível de impacto
Baixo	Baixo	1
	Médio	2
	Alto	3
Médio	Baixo	2
	Médio	3
	Alto	4
Alto	Baixo	3
	Médio	4
	Alto	5

Tabela 3. Nível de impacto

2.3.4 Análise de probabilidade de riscos

Passo 4 – Analisar a probabilidade das falhas

Análise da probabilidade de incidente

Critério	Baixo	Médio	Alto
Probabilidade	Ameaças de rara frequência, média de 5 a 10 anos.	Ameaças de média frequência, acontecimento com média de 1vez por semestre	Ameaças que acontecem frequentemente.
Facilidade da exploração de vulnerabilidade	Risco de difícil exploração. É necessária maior demanda de tempo e conhecimento técnico e específico para ser explorado e resolvido	Risco com descoberta recente. Necessita de conhecimento técnico para exploração.	Risco facilmente explorado. Pode não haver demanda de conhecimento técnico.

Tabela 4. Critério de probabilidade de incidente

Análise do nível de probabilidade de incidente

Probabilidade de ameaça	Facilidade de exploração	NP
Baixo	Baixo	1
	Médio	2
	Alto	3
Médio	Baixo	2
	Médio	3
	Alto	4
Alto	Baixo	3
	Médio	4
	Alto	5

Tabela 5. Classificação do nível de probabilidade de incidente

2.3.5 Classificação por nível de risco

Passo 5 – Análise e classificação por nível de risco

Nível de Risco

Para obter o nível de risco é necessário fazer um cálculo, multiplica o valor do nível de impacto pelo nível de probabilidade. Nível baixo (1-4), Nível médio (4-15), e de Nível alto (15-25).

Análise de risco

ANÁLISE DE RISCOS							
Identificação de riscos					**Estimativa de riscos**		
Ordem	**Ativo**	**Ameaça**	**Vulnerabilidade**	**Impacto**	**NP**	**NI**	**NR**
1	PPPR	Indisponibilidade dos dados do sistema	Parada inesperada do servidor	Perda de integridade e disponibilidade de uso do sistema em toda empresa.	4	4	16
2	PPPR	Falha nos backups	Backup não conferido ou feito corretamente	Perda de confidencialidade, integridade e disponibilidade. Em caso de perda total do servidor os dados do último backup até o dia do incidente serão	4	5	20

				perdidos			
3	PPPR	Perda de conexão à internet	Queda nos 2 serviços de internet	Perda de disponibilidade de informação. Impossibilidade de emissão de NF-e e NFS-e.	3	2	6
4	PPPR	Falha na segurança do acesso	Uso indevido de senha	Perda de confidencialidade integridade e disponibilidade. Comprometimento dos processos realizados. Uso indevido de senha de um colega de trabalho.	3	3	9
5	Servidor de arquivos	Indisponibilidade	Parada do servidor	Indisponibilidade total de acesso a arquivos da empresa	3	4	12
6	Servidor de arquivos	Falha nos backups	Backup não conferido ou feito corretamente	Em caso de perda total do servidor os dados do último backup até o dia do incidente serão perdidos	4	5	20
7	Estação de trabalho	Falha do dispositivo	Defeito em peça ou falha do sistema operacional.	Indisponibilidade dos serviços realizados.	3	3	9
8	Estação de trabalho	Infecção por vírus	Acesso a conteúdo não seguro ou dispositivo infectado.	Perda de integridade, confiabilidade e disponibilidade. O computador infectado pode espalhar o vírus pela rede infectando outros computadores.	2	4	8
9	Estação de trabalho	Perda total do dispositivo	Defeito irreparável, perda de peças ou o HD.	Perda de integridade, confiabilidade e disponibilidade. Se houver informações gravadas neste computador e não houver backup, os dados não serão	3	4	12

				restaurados. Serviço realizado pela estação será parado até ser providenciado um computador reserva.			
10	Estação de trabalho	Sem bloqueio a sites com conteúdos maliciosos	Acesso não monitorado à internet	Este acesso pode acarretar em problemas de infecção. Perda de confiabilidade e integridade.	3	5	15
11	Roteador	Acesso sem autorização a rede.	Roteador configurado no mesmo endereçamento da rede dos computadores da empresa.	Um dispositivo de um funcionário ou cliente que possa estar infectado com vírus se conecta à rede podendo espalhar para as outras máquinas	2	5	10
12	Roteador	Acesso sem autorização a rede,	Roteador sem alteração de senha padrão de configuração.	Um usuário mal-intencionado pode se conectar e modificar as configurações do roteador causando perda de disponibilidade e confiabilidade.	2	5	10
13	HUB e Switch	Perda do dispositivo	Hub ou Switch queimado	Perda de integridade, confiabilidade e disponibilidade das informações. Os computadores conectados na rede a partir desse aparelho perdem o acesso à rede e aos servidores.	2	4	8
14	Rede	Conexão de outro computador, notebook não autorizado na rede	Usuário conecta um computador ou notebook a rede fazendo acesso não monitorado.	Perda de integridade, confiabilidade e disponibilidade das informações. O usuário pode acessar informações sem autorização ou espalhar um vírus na	2	5	10

				rede de forma intencional.			
15	Mikrotik	Perda do dispositivo	Mikrotik queimado.	O dispositivo é o gateway da rede, caso ele venha a queimar os computadores perdem conexão com a rede.	1	5	5

Tabela 6. Análise e classificação dos riscos

Tabela para critério de avaliação de risco

Ordem	Cenário	NR	Perda de 4 ativos de informação	Perda de 3 ativos de informação	Perda de 2 ativos de informação	Perda de 1 ativos de informação	Prioridade do risco
2	Backup não conferido ou feito corretamente	20				X	1
6	Backup não conferido ou feito corretamente	20				X	2
1	Parada inesperada do servidor	16	X				3
10	Acesso não monitorado à internet	15	X				4
5	Indisponibilidade	12	X				5
9	Perda total do dispositivo	12	X				6
11	Acesso sem autorização a rede.	10		X			7
12	Acesso sem	10		X			8

	autorização a rede.						
14	Conexão de outro computador, notebook não autorizado na rede	10	X				9
4	Falha na segurança do acesso	9				X	10
7	Falha do dispositivo	9				X	11
8	Infecção por vírus	8		X			12
13	Perda do dispositivo	8			X		13
3	Perda de conexão à internet	6			X		15
15	Perda do dispositivo	5	X				15

Tabela 7. Critério para avaliação do risco

2.3.6 Tabela de riscos por prioridade

Passo 6 – Criação da tabela de riscos

Tabela de riscos

Ordem de prioridade

Nº	Ativo	Risco
1	PPPR	Parada inesperada do servidor
2	PPPR	Backup não conferido ou feito corretamente
3	Serv. Arquivos	Backup não conferido ou feito corretamente

4	Serv. Arquivos	Parada inesperada do servidor
5	Estação de trabalho	Acesso não monitorado à internet
6	Estação de trabalho	Defeito irreparável, perda de peças ou o HD.
7	Roteador	Acesso sem autorização a rede,
8	Roteador	Roteador sem alteração de senha padrão de configuração.
9	Rede	Conexão de outro computador, notebook não autorizado na rede
10	PPPR	Falha na segurança do acesso
11	Estação de trabalho	Defeito em peça ou falha do sistema operacional.
12	Estação de trabalho	Infecção por vírus
13	HUB e Switch	Perda do dispositivo
14	PPPR	Perda de conexão à internet
15	Mikrotik	Perda do dispositivo

Tabela 8. Riscos por prioridade

Concluindo essa análise, temos uma relação dos riscos por prioridade de acordo com a tabela de informação da ISO. Os riscos que foram encontrados por essa avaliação mostram os pontos vulneráveis na empresa que podem acarretar em falhas, lentidão, perda total ou parcial de informações e de desempenho nos processos. Com essa lista conseguimos analisar e dentro das condições atuais da empresa e juntamente com as particularidades foi possível montar um projeto de implantação de políticas de segurança para minimizar a incidência de pelo menos parte desses riscos, garantindo maior segurança ao ambiente.

Para isso não foram implementadas ferramentas como uma GPO para controlar as máquinas e limitar acessos, firewall para bloquear portas de acesso, por motivo que a empresa não poderia ceder um computador para implantar outro servidor, e não poderia disponibilizar um valor financeiro para a aplicação destes.

As políticas implantadas visaram o baixo custo para manter a segurança da empresa. Pois um dos objetivos deste trabalho é minimizar os impactos e as incidências de riscos com baixo custo financeiro. Boas práticas, regras e punições adequadas podem melhorar a segurança dos dados de uma empresa, pois segurança não interfere apenas em tecnologia, mas ela é garantida através de pessoas, boas práticas e a tecnologia trabalhando em harmonia.

2.3.7 Início da implantação das políticas

Passo 7 – Iniciar implantação das políticas de segurança

Após realizada a análise com os padrões da norma ABNT, essas informações foram repassadas a direção da empresa, e com isso foi possível elaborar as políticas de segurança aplicadas na empresa. As políticas foram aplicadas obedecendo algumas restrições e particularidades da empresa. Como a empresa não poderia arcar financeiramente no momento com novos dispositivos, ou servidores para outras implantações de ferramentas de segurança, este trabalho teve foco em promover a segurança da rede de computadores com baixo custo financeiro, e visando a responsabilidade que os funcionários precisam ter com as informações da empresa.

Para isso foi elaborado um termo de políticas de segurança, este termo foi passado para os funcionários, eles leram os termos e assinaram concordando com as informações contidas neste. A elaboração do termo foi com base nas restrições que a direção da empresa queria implementar e com informações para o funcionário diante as regras e restrições que cada setor tem em particular.

2.4 IMPLANTAÇÃO DAS POLÍTICAS DE SEGURANÇA

Após feita a análise de riscos com base na ISO 27005, para melhorar a segurança do ambiente e diminuir a incidência de ocorrer falhas na rede, foi implantado políticas de segurança com auxílio da direção da empresa, que foi fundamento chave para gerar o termo passado aos funcionários. Com a norma estabelecida, os funcionários leram os termos e assinaram uma vez que concordaram com as políticas adotadas pela empresa para melhorar a segurança do ambiente. Agora como termo implantado, a empresa repassa essas regras a todos os funcionários novos que são contratados, eles devem ler e assinar concordando com os termos.

A rede de computadores trabalha com a topologia cascata, que é possível observar com o mapa da rede que se encontra em anexo neste trabalho (Anexo 2), uma topologia que não é uma das melhores topologias para fluxo de dados pois ela possui diversos *hub's* que são dispositivos concentradores de rede que se encarrega receber e transmitir os dados através da rede aos dispositivos que estão ligados a partir dele. Porém como existem

vários hubs na empresa, caso algum desses aparelhos tenha algum defeito, apenas os dispositivos ligados a ele perderão sinal, de modo que não haverá falha em toda a rede da empresa.

A estrutura física da rede não foi modificada porque para alterar sua topologia, também é necessária uma alteração na estrutura física da empresa para manter a conformidade com um novo tipo de topologia, como por exemplo uma topologia estrela, que é uma das mais utilizadas atualmente e que pode funcionar tendo apenas um único ponto centralizador que distribui informações para todos os dispositivos da rede.

A empresa tem projeto de reformas que pode mudar alguns setores de local, com isso será necessário efetuar uma mudança na rede de computadores, além de um investimento para novos equipamentos como *switch* que tem frequência de velocidade /100/1000 mbps.

2.4.1 Políticas de uso da internet

Para a formulação dessas normas, a direção da empresa optou por bloquear totalmente o acesso à internet dos setores de venda, e dos setores de produção, setor responsável pela reforma de pneus. Foi determinado assim pois segundo a direção esses setores não tem necessidade de acessar internet para realizar suas funções. Para concretizar essa configuração foi utilizada a ferramenta *mikrotik* que já existia na empresa com a funcionalidade de balanceamento de internet. Para isso foi bloqueado os IPs e MAC das placas de rede para não efetuarem acesso à internet.

Para melhorar o nível de segurança referente ao endereçamento das máquinas foi optado por “amarrar” o endereço de IP que a máquina recebe juntamente com a MAC (*Média Acess Control*) que é o endereço físico do dispositivo que já está vinculado à sua interface de comunicação na rede de computadores. A seguir a imagem do painel de configuração.

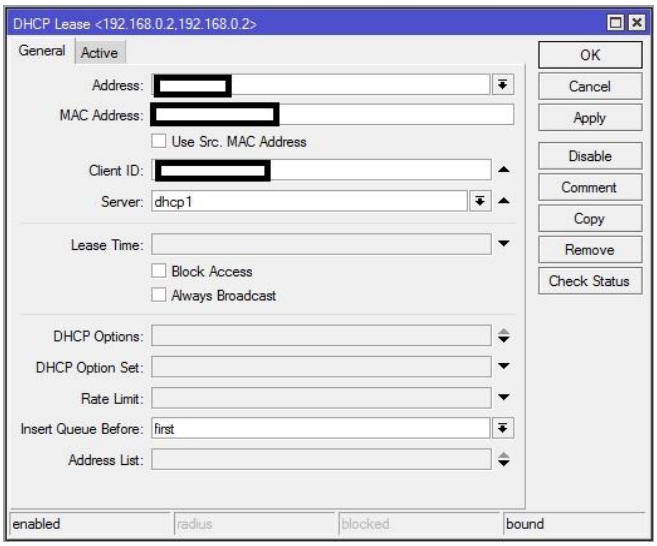


Figura 2. Amarração IP e MAC

Fonte: O próprio autor

Essa configuração é realizada quando se tem o servidor DHCP (*Dynamic Host Configuration Protocol*) que se trata de um serviço que distribui de forma dinâmica endereços IP, máscara de sub-rede, gateway para os terminais da rede, ou os computadores e dispositivos nela conectados. Dessa forma o *mikrotik* possui essa função permitindo inserir o endereço físico do terminal e configurar com ele juntamente o endereço de IP concedido apenas para aquele computador, a figura a seguir mostra isso.

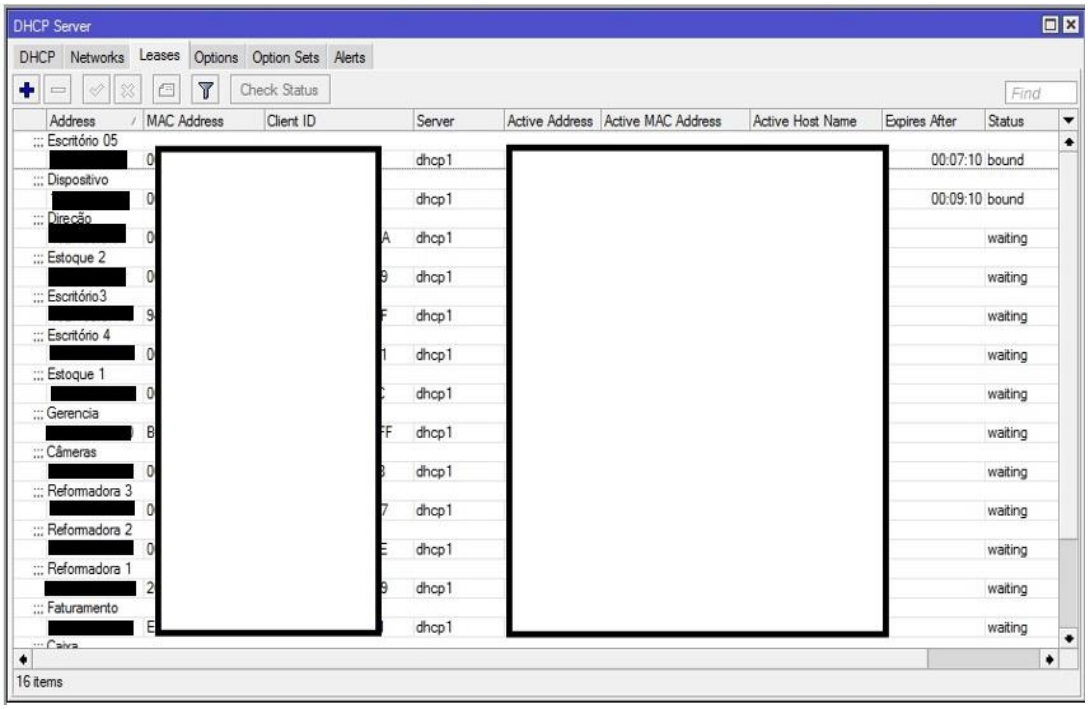


Figura 3. Configuração IP e MAC

Fonte: O próprio autor

Este método garante maior segurança pois os computadores que tem restrição de internet, mesmo que formatados, tendo seu sistema operacional trocado entre outros, ele continuará recebendo o mesmo endereço na rede todas as vezes que for conectar.

As informações de IP, MAC e ID dos dispositivos estão encobertos por motivo de segurança. Na imagem acima podemos ver o painel com as configurações já aplicadas, mostra os computadores que estão conectados no momento e os que não estão. Dessa forma toda vez que o dispositivo iniciar a conexão ele receberá apenas o IP para ele designado.

Para realizar essa configuração foi coletado as informações de MAC de todas as máquinas da rede, criado uma relação de IP, Setor e nome de dispositivo, entre eles estão computadores e roteadores. A finalidade dessa aplicação é manter organização dos endereços da rede, a segurança e minimizar evitar conflitos de IP.

2.4.2 Limitação de banda de internet

Com o *mikrotik* foi feito o balanceamento de banda dos demais computadores que tem acesso à internet autorizada. Com essa aplicação foi possível limitar a velocidade de acesso à internet dos computadores que tem esse acesso, ou seja o objetivo é, se um funcionário tiver a necessidade de fazer algum download ou upload de um arquivo muito grande, essa ação não vai prejudicar os demais usuários que precisam da internet.

A configuração foi realizada da seguinte forma, é adicionado ao *mikrotik* uma regra que chamada de *Queue*. É adicionado o número do IP do computador e assim o nome da máquina ou qual setor a mesma está. Assim onde temos *Max limit* definimos a quantidade de download ou upload que determinado computador terá disponível.

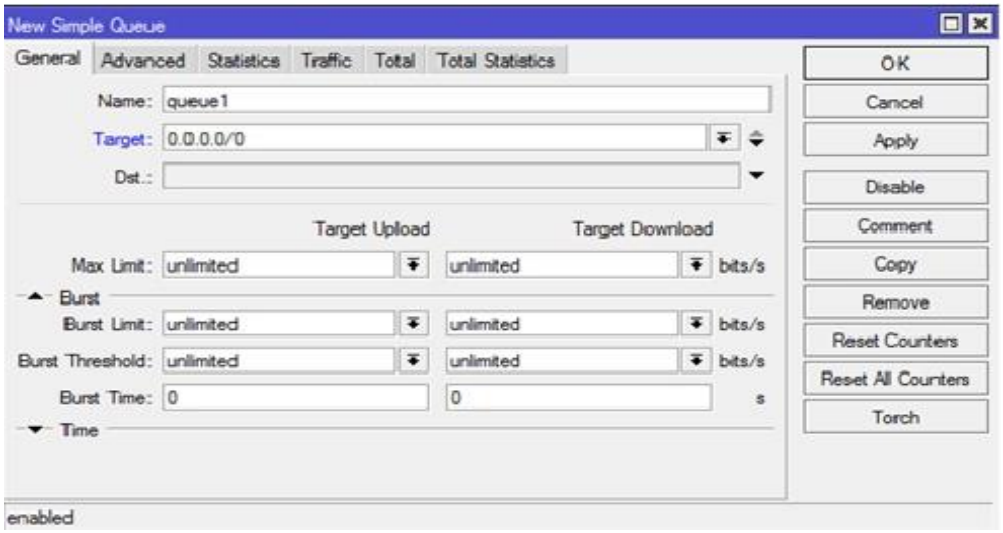


Figura 4. Configuração limite de banda de internet

Fonte: O próprio autor

Na figura a seguir temos o a relação das regras de limite em funcionamento onde é possível ver quanto cada máquina está consumindo de internet no momento exato.

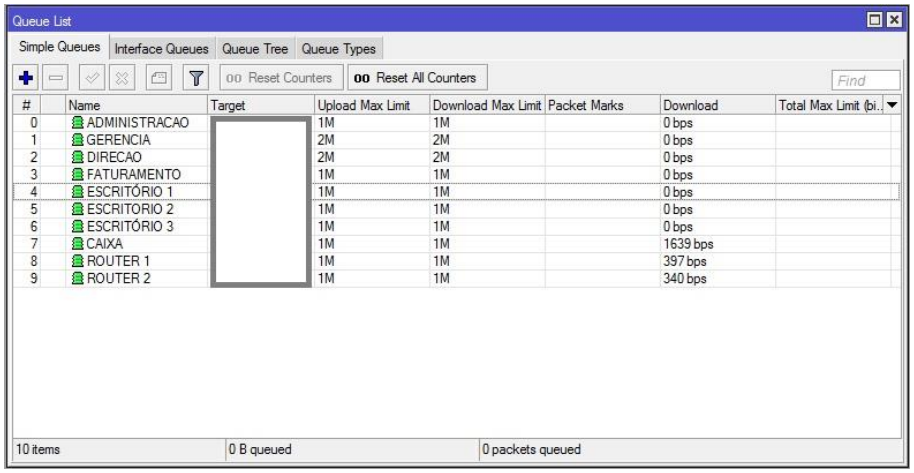


Figura 5. Relação de limite de internet por máquina

Fonte: O próprio autor

Esta regra também foi aplicada para os roteadores, um está situado na loja onde é de acesso dos clientes, outro está situado no escritório para acesso interno apenas de funcionários autorizados. A regra evita que um cliente realize download ou upload consumindo a quantidade excessiva de internet prejudicando os serviços da empresa. Essas regras de limitação foram aplicadas dessa maneira com auxílio da direção da

empresa e durante seu funcionamento tem atendido muito bem as necessidades dos funcionários e de forma alguma atrapalhou o trabalho deles.

2.4.3 Políticas de Senha

Os funcionários foram orientados a nunca passar sua senha de uso do sistema de informática para ninguém, incluindo desde os colegas de trabalho até pessoas de convívio pessoal que não tem ligação da empresa. Uma senha segura é uma senha intransferível. Para garantir a segurança de cada um, foi informado que os usuários são responsáveis pelas ações realizadas nos sistemas, para verificar isso os sistemas possuem ferramenta de log que grava no banco de dados do sistema de informática as ações de cada um dentro do sistema como mostram as imagens a seguir.

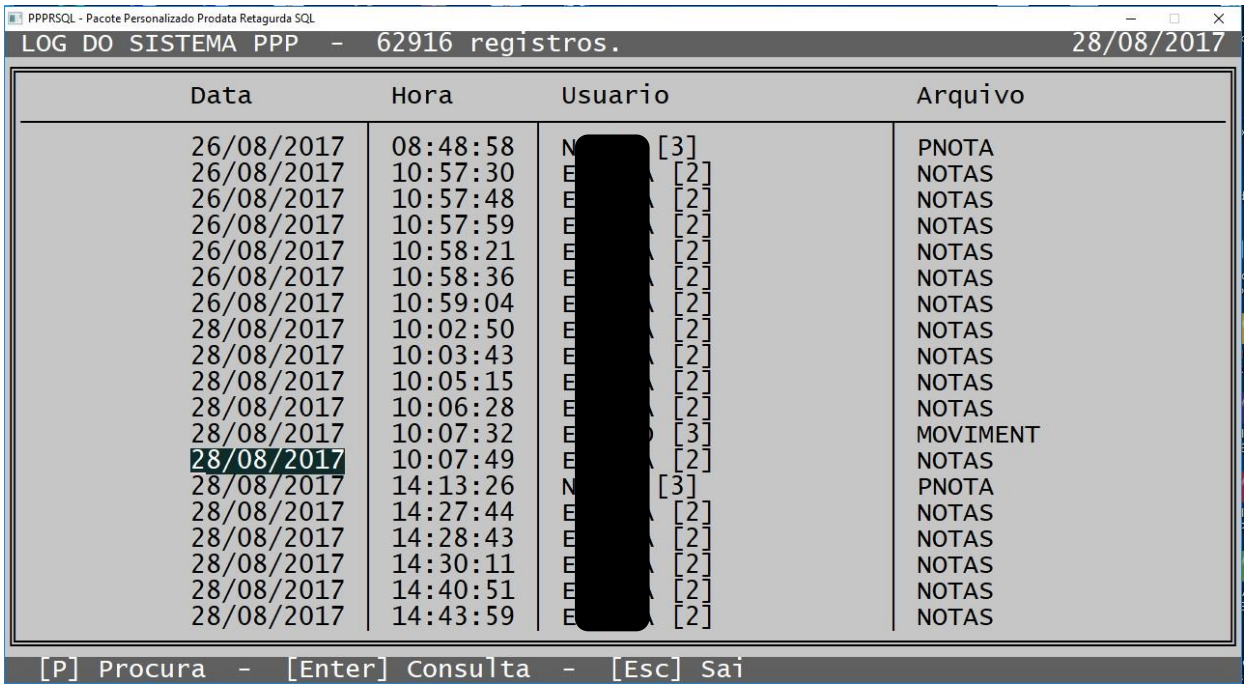


Figura 6. Sistema PPPR

Fonte: O próprio autor

A imagem acima mostra a lista com o registro de log do sistema informando quando ocorreu a modificação, a hora registrada e quem foi o usuário que executou a ação, em frente ao nome do usuário o número indica o nível de acesso que esse usuário tem dentro do sistema e a frente a coluna do arquivo que o usuário acessou dentro do sistema.

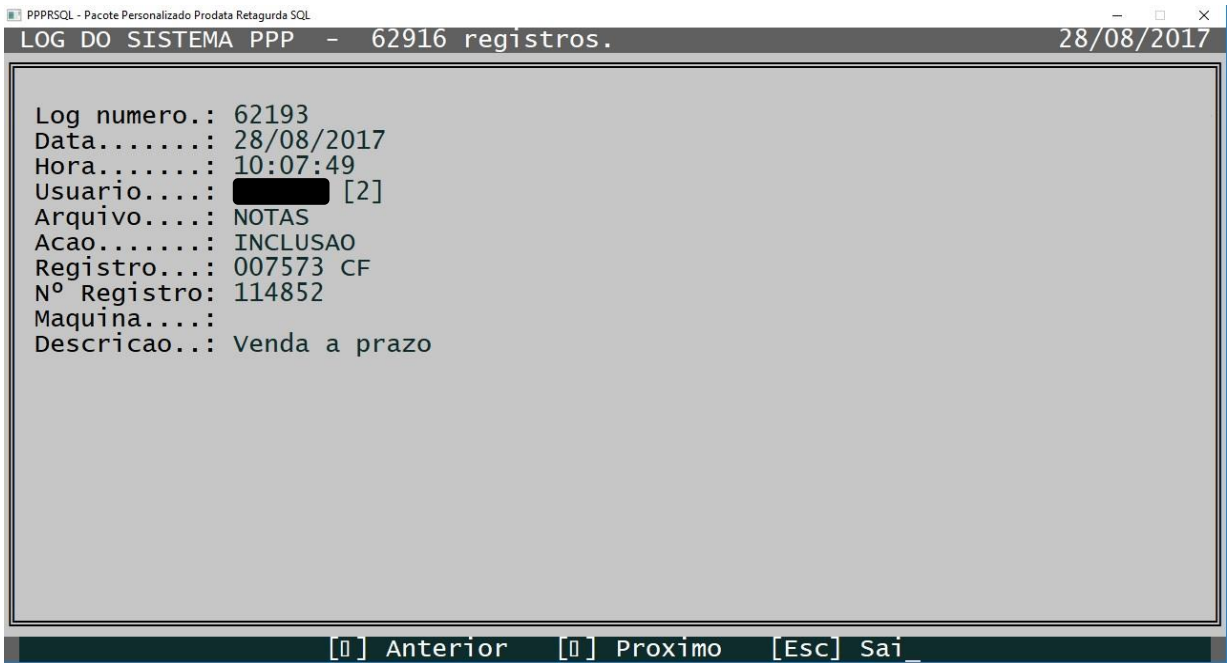


Figura 7. Log sistema PPPR

Fonte: O próprio autor

Essa imagem traz com mais detalhes a informação que o funcionário incluiu ou alterou no sistema.

Por questões de privacidade com a exibição de nomes dos funcionários os campos onde aparecem seus nomes foram estão cobertos, mas não impedindo o entendimento da funcionalidade do sistema para coleta de informação.

2.4.4 Políticas de segurança com e-mail

Outra orientação nas políticas implantadas foram as boas práticas para uso de e-mail dentro da empresa. Essa orientação se aplica apenas aqueles que tem acesso à internet e necessitam da ferramenta. Práticas como sempre verificar se o endereço de quem enviou o e-mail é conhecido, verificar o assunto do e-mail, e caso o mesmo tenha arquivos em anexo, não executar o anexo caso seja de alguma extensão como .exe, .bat, .html. Caso o funcionário tenha alguma dúvida sobre o arquivo em anexo ou o endereço que enviou este e-mail, ele deve verificar com os colegas se alguém está esperando algum e-mail, caso ainda exista dúvidas ele deve ignorar ou entrar em contato com a equipe de TI para uma análise melhor apurada. Uma observação que foi feita dentro desta política é que o funcionário não deve utilizar o e-mail da empresa para fins pessoais, além da

senha do mesmo ser intransferível, os funcionários que tem acesso devem manter a mesma em sigilo.

2.4.5 Políticas de uso do computador de trabalho

Foi criada está instrução para os funcionários da empresa. Cada computador possui configurações que permitem a análise das ações realizadas e que identificam este terminal na rede da empresa. No caso do escritório cada utilizador tem seu próprio computador para realizar suas funções, sendo assim cada um se responsabiliza pelas ações executadas no seu computador.

Os funcionários não devem instalar nenhum programa/*software* que não seja autorizado pela direção ou pela equipe de TI. Devem evitar transferir para seu computador de trabalho arquivos como músicas, fotos pessoais, filmes e vídeos entre outros, a equipe técnica não se responsabiliza por estes tipos de informações e orienta que não tenha esses tipos de arquivos no mesmo na mídia de transferência não sabe se existe algum tipo de vírus ou *malware*. A estação de trabalho só deve ser utilizada para exercer suas funções de trabalho na empresa e jamais para uso pessoal, é preferível que no computador exista apenas dados de uso da empresa, essas informações devem ser preferencialmente armazenadas no servidor.

Pendrives, celular, mp3 entre outros entre outros dispositivos de armazenamento USB são muito práticos para transferir arquivos, más por muitas vezes virem de origem desconhecida, podem se tornar um problema pois podem ocasionar com a infecção de vírus no computador e podendo espalhar este mesmo em toda rede, porém na rede de computadores da Pneucar não são todas as máquinas tem necessidade de ter informações trocadas por este tipo de dispositivo. Afim de minimizar a incidência de riscos de infecção por vírus como o que existia na análise de falha que foi realizada foi realizado um bloqueio específico para isso com os computadores dos setores de produção, loja e estoque. Atualmente os computadores tem as entradas USB bloqueadas para o acesso de dispositivos desse tipo.

Para realizar esse bloqueio primeiramente foi adicionado a cada computador um usuário administrador com todos os privilégios de modificações e um usuário padrão que será usado pelos funcionários para realizar seu trabalho, com isso os funcionários ficam limitados a realizar ações como instalação de programas e alterações de configurações

dos computadores pois sempre que houver a tentativa de realizar alguma configuração a senha de administrador será solicitada. Quem tem conhecimento dessa senha é a equipe de TI e a direção da empresa, mas sempre for solicitado algum suporte, reparo ou manutenção que necessite dessa senha a equipe de TI que será encarregada de realizar.

Após a criação do usuário administrador foi feito em cada computador a seguinte configuração, acessando o editor de registro do Windows, procuramos pela seguinte entrada de informações:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR

O diretório onde é possível encontrar este registro está com destaque como mostra a figura a seguir:

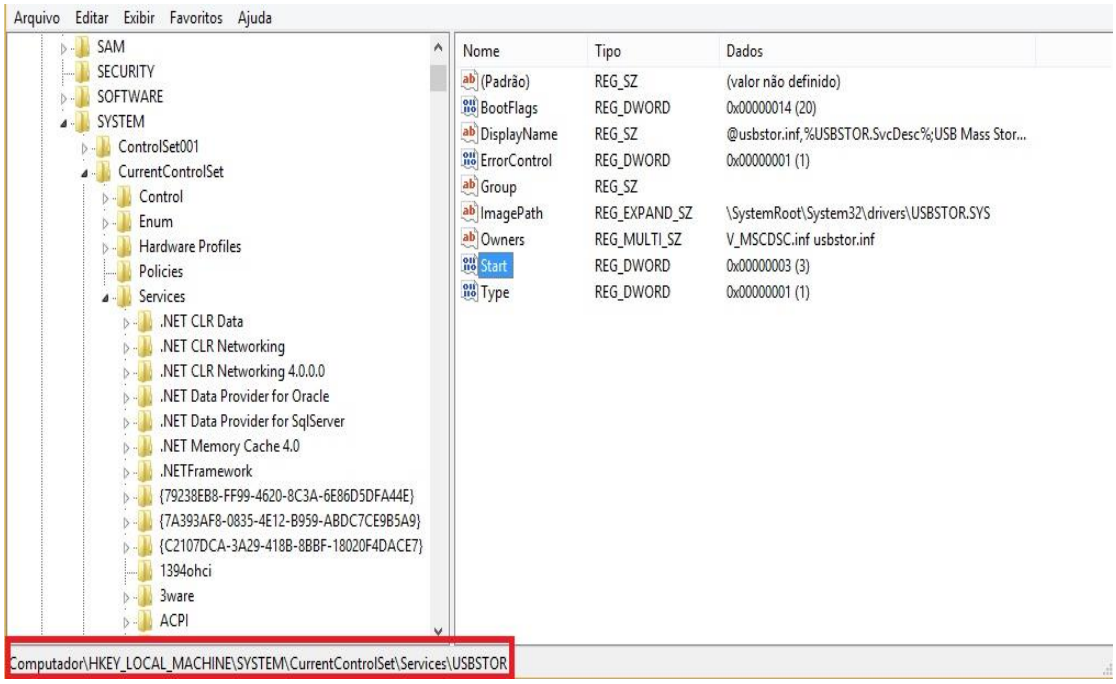


Figura 8. Editor de registro do Windows

Fonte: O próprio autor

No registro selecionado com o nome start, foi alterado a informação contida nele. Para fazer essa modificação inserimos no registro o número 4 e aplicamos a alteração como mostra a figura seguinte:

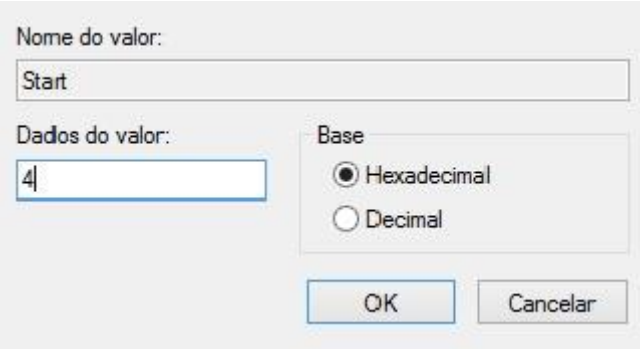


Figura 9. Alteração de registro do Windows

Fonte: O próprio autor

Logo após essa alteração, os dispositivos de armazenamento USB ficaram bloqueados, porém este processo não desabilita mouse ou teclado USB, periféricos como esses funcionam normalmente. Caso for necessário habilitar essa função de acesso a mídias de armazenamento USB seria necessário voltar a configuração como estava ao invés de 4 somente voltar para 3.

A aplicação do usuário administrador nos computadores é justamente para que alterações como essas sejam impossibilitadas de alteração pelos funcionários. Somente será possível modificar esse registro se a pessoa tiver poder da senha de usuário administrador.

2.4.6 Políticas de acesso à rede wireless

Ao iniciar esse trabalho, a empresa solicitou que fosse adicionado um roteador na parte da loja fornecendo uma rede *wi-fi* disponível para os clientes e para os funcionários caso venha a ser necessário ser utilizada por eles. Existe outro roteador que fornece acesso a outra rede *wi-fi* para os funcionários do escritório. Para garantir a segurança da rede interna da empresa, foi realizada uma configuração em ambos os roteadores de modo que, um celular, notebook ou outro dispositivo ao conectar na rede *wirelles* não consegue fazer nenhum acesso a mesma rede em que estão os computadores da empresa. Essa regra foi adotada para que não exista conflitos de informação, acesso não autorizados ou a danificação de dispositivos da empresa.

No painel de configurações do aparelho roteador tem a funcionalidade para modificar o endereço de rede que será distribuído a partir dele, então os endereçamentos foram trocados para que a faixa de IP estabelecida pelo roteador seja diferente da faixa

dos computadores da empresa. Essa funcionalidade foi testada com a ferramenta *ping*. É um comando que ao ser executado verifica se existe conexão em nível de IP com outro dispositivo da rede. Essa ferramenta funciona enviando mensagens de um computador e verifica se o outro computador recebeu essa resposta retornando para o usuário uma mensagem que houve o recebimento dessa informação. O *ping* é o principal comando utilizado para verificar e solucionar problemas de conectividade, alcance e resolução de nomes.

Os resultados dos testes informaram que não foi possível conectar a nenhum dos servidores, ou máquinas cliente da rede de computadores da empresa, e mesmo dentro do Windows não foi possível identificar nenhum outro dispositivo da rede interna como mostra a imagem a seguir.

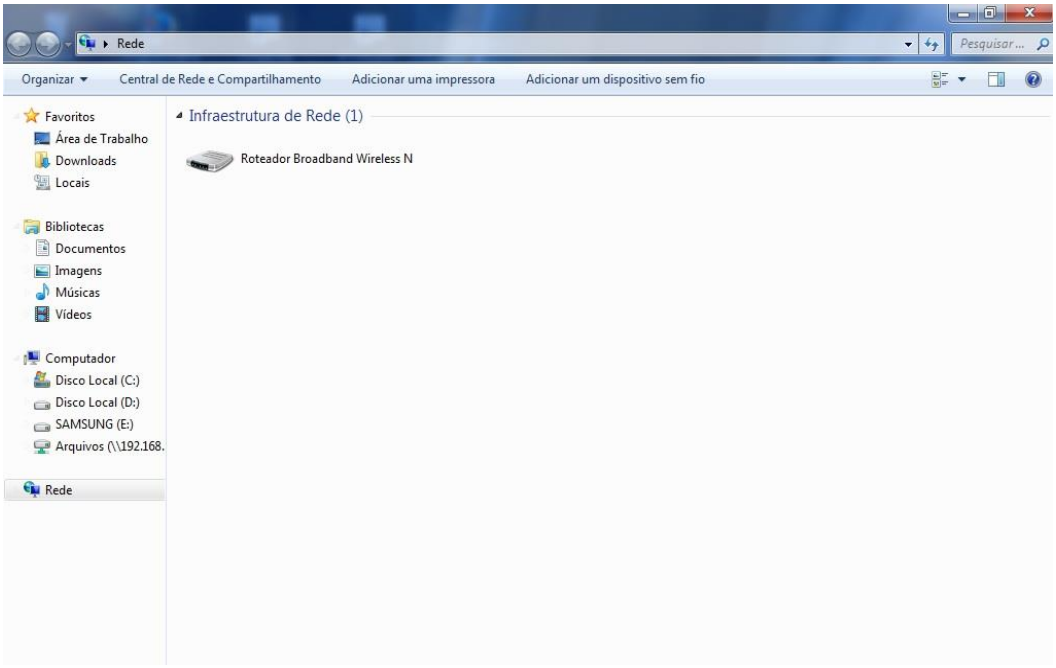


Figura 10. Conexões com a rede de computadores

Fonte: O próprio autor

Nenhum outro dispositivo da rede aparece com a conexão, assim é possível evitar possíveis invasões as máquinas da empresa melhorando o nível da segurança.

Nos termos das políticas de segurança que está em anexo neste trabalho, está descrito as restrições de uso da rede wi-fi aos funcionários, como a quem está destinada e restringindo o acesso dos mesmos apenas com autorização.

2.4.7 Políticas com antivírus

A empresa utiliza como ferramenta antivírus o software *kaspersky internet security*. Essa ferramenta tem se mostrado muito eficiente para manter a segurança dos computadores por conter funcionalidades como controle parental, proteção a *webcam*, um serviço de firewall muito bom além de ser um dos antivírus que consome menos recursos do CPU (Fonte: Kaspersky blog). Por se tratar de um software pago, está instalado apenas nas maquinas com acesso à internet da empresa, e com todas suas funcionalidades ativadas. A figura a seguir mostra o antivírus e seus módulos de execução:

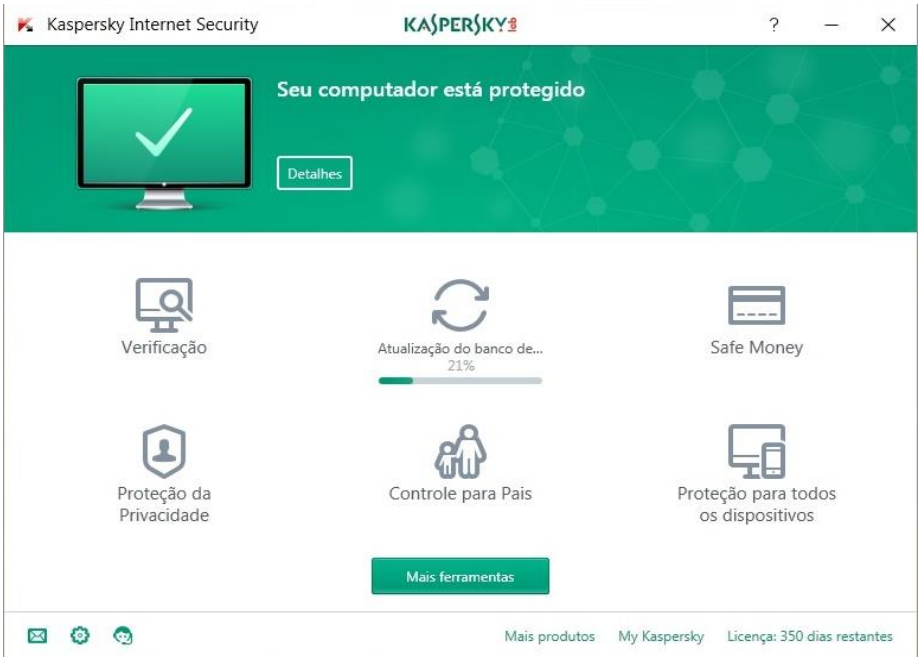


Figura 11. Antivírus Kaspersky

Fonte: O próprio autor

Além de possuir um firewall muito bom, também conta com extensões para o navegador que influencia positivamente no acesso a sites sejam eles de origem duvidosa ou não e também possui uma outra ferramenta que é o *Kaspersky Safe Money*, ferramenta que possui níveis de segurança para proteger transações online com bancos, cartões de crédito e compras pela internet. Para as transações bancárias a ferramenta *Safe Money* auxilia na proteção da digitação das senhas. Onde existe o teclado virtual, que é muito utilizado em serviços internet banking o antivírus efetua a proteção e exibe uma mensagem para que o usuário saiba que existe essa verificação antes de digitar sua senha, afim de melhorar a segurança dos dados.

Vale ressaltar que o antivírus *Kaspersky* efetua bloqueios de conexão as máquinas da rede de modo que, se o usuário definir que não quer deixar seu computador acessível para os outros da rede, o antivírus bloqueia totalmente este tipo de acesso. A figura a seguir mostra o painel onde pode observar com mais detalhes as ferramentas do software e onde é possível modificar ou alterar configurações.

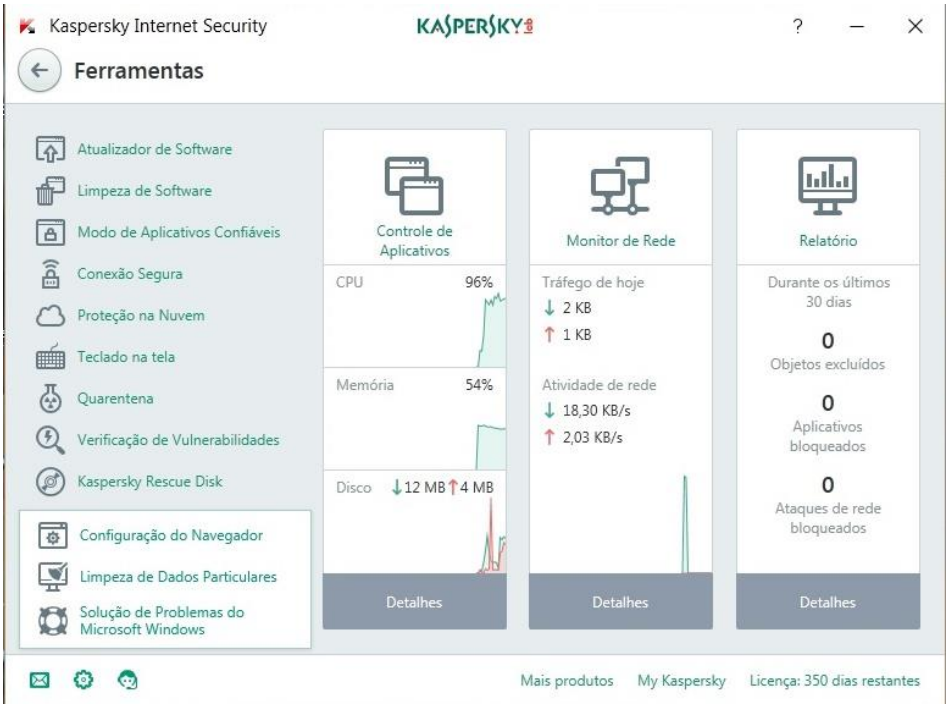


Figura 12. Ferramentas do Antivírus Kaspersky

Fonte: O próprio autor

Nos termos das políticas de segurança (Anexo 3) estão algumas dicas para os funcionários de como eles devem verificar as ações desse *software*, os mesmos devem periodicamente verificar atualizações para o seu antivírus, periodicamente efetuar uma verificação no seu computador, alguns usuários optaram por configurar automaticamente esta funcionalidade de verificação para o horário em que não estão presentes na empresa e em um dia da semana que não dependem totalmente do computador para realizar seus trabalhos devido a possível lentidão durante esse processo. Essa configuração pode ser observada na figura a seguir:

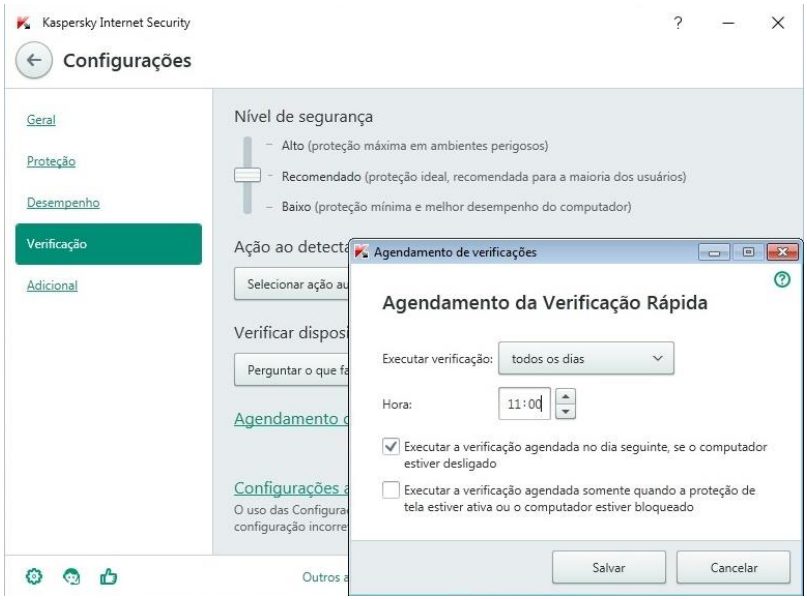


Figura 13. Configuração de verificação do Antivírus Kaspersky

Fonte: O próprio autor

O agendamento de verificação pode ser configurado para ser realizado todos os dias ou periodicamente com intervalo de dois até sete dias. Os funcionários estão orientados a sempre que surgir dúvidas ou falhas durante este procedimento, a entrar em contato com a equipe de TI, para que a equipe se encarregue de verificar e resolver a situação.

2.4.8 Políticas de backup

Os backups do sistema de informática sempre foram um assunto de muita preocupação dentro da empresa. A direção sempre se preocupou com o fato dos sistemas terem backups redundantes afim de garantir maior segurança. Já os arquivos dos computadores pessoais dos funcionários ficam armazenados em um servidor onde somente os funcionários autorizados tem acesso a esses dados. Para garantir maior segurança muitos poucos arquivos são salvos nos computadores dos usuários, e caso aconteça algum defeito em um desses computadores o usuário corre mínimos riscos de perder informações porque os arquivos que cada um utiliza em seu computador estão salvos no servidor.

O servidor de arquivos e de banco de dados possuem um *firewall* próprio para que não ocorra incidência de vírus ou acessos não permitidos, esta funcionalidade foi configurada pela equipe de TI durante a instalação e configuração do sistema operacional dos servidores, além de configurar que os servidores não tenham nenhum tipo de acesso externo, pois não existe a necessidade que os servidores comuniquem com nenhuma rede fora da empresa ou com a internet.

Para realizar o backup do banco de dados dos sistemas a equipe de TI desenvolveu um software que facilita muito a realização dos backups. Este sistema é o ProBKP, por se tratar de um banco de dados em SQL o software é responsável por executar um comando de *dump* que funciona compactando os arquivos do banco de dados em apenas um e salvando o arquivo em uma pasta específica do computador ou outro armazenamento. A figura a seguir mostra a imagem do sistema.

Figura 14. Sistema de backup ProBKP

Fonte: O próprio autor

Este sistema é prático para os usuários porque quando já está configurado necessita apenas de um clique no botão efetuar backup e o realiza automaticamente sem nenhuma interferência do usuário. O software também não necessita de um banco de dados, é executado na própria máquina cliente, e apenas configurado realiza os backups que sempre são conferidos pela equipe da empresa e pela equipe de TI. A imagem a seguir mostra a configuração deste sistema.

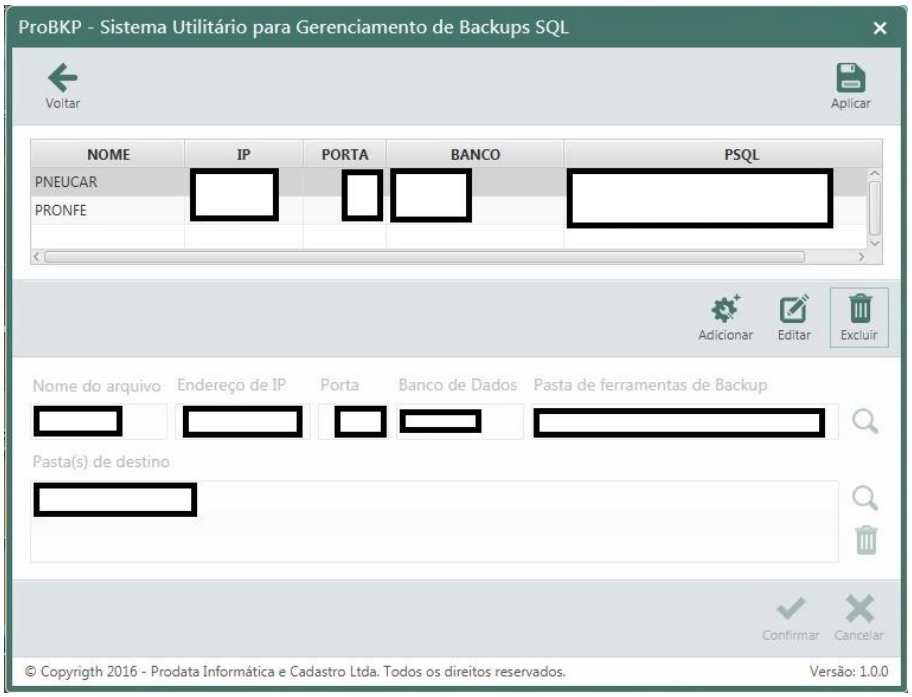


Figura 15. Configuração do Sistema de backup ProBKP

Fonte: O próprio autor

Preenchendo as configurações de IP do servidor, porta, nome do banco de dados, selecionando as pastas onde ficaram as ferramentas de *dump* e a de armazenamento do arquivo, conclui a etapa de continuação e depois de salvar o backup já pode ser realizado.

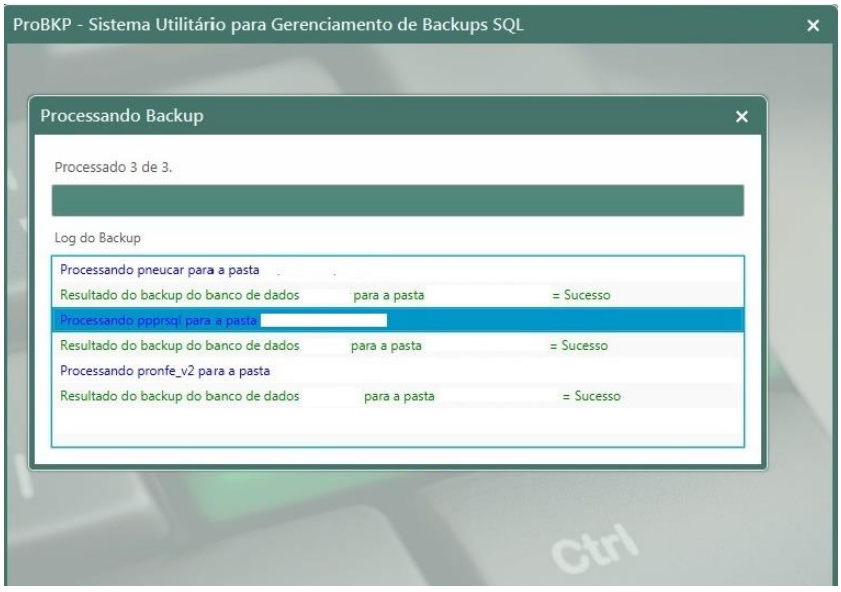


Figura 16. Resultado dos backups do Sistema ProBKP

Fonte: O próprio autor

Durante o andamento do backup o sistema mostra uma barra de progresso para que o usuário acompanhe esse procedimento. Assim que finalizado retorna uma mensagem mostrando que o processo concluiu como mostra a figura anterior. As informações como nome do banco de dados e pasta de armazenamento das figuras do sistema não estão amostra por motivo de segurança.

Após a realização dos backups, estes arquivos são salvos de 3 maneiras diferentes. Primeiro eles são salvos na máquina cliente, e logo após o funcionário responsável por executar o backup faz uma cópia desses arquivos para mídias de armazenamento. A empresa conta com um *pendrive* para cada dia da semana que for realizado o backup. Essas mídias são de exclusividade dos backups dos sistemas, e jamais utilizadas para outro tipo de armazenamento. Somente a direção da empresa, a equipe de TI e este funcionário responsável pelos backups tem acesso a estes dispositivos, os mesmos ficam guardados na empresa longe do conhecimento de outros funcionários e somente são utilizados durante o processo de backup. A figura a seguir mostra as mídias de armazenamento.

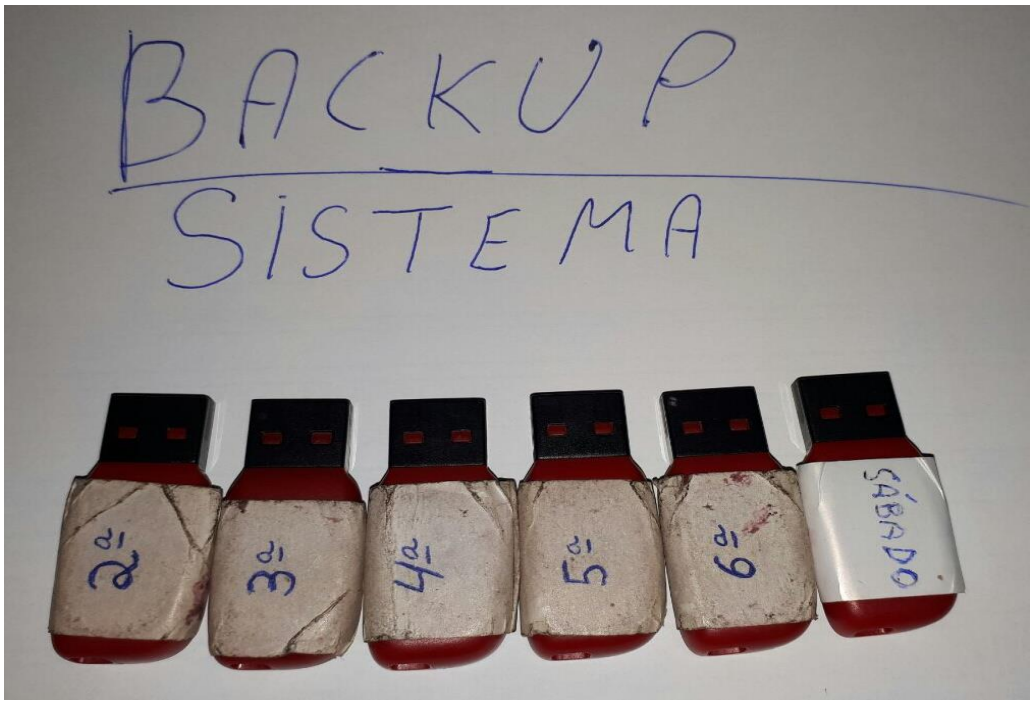


Figura 17. Pendrives para armazenamento dos backups do sistema

Fonte: O próprio autor

Cada mídia tem 4GB de armazenamento, espaço suficiente para salvar os arquivos do backup do sistema, pois os arquivos não passam de 100 MB de tamanho. Quando um *pendrive* está cheio, o arquivo de backup mais antigo é substituído pelo mais recente. Assim os backups antigos são sempre sobrepostos pelos mais novos, pois o sistema ProBKP armazena o backup com a data do dia. Por exemplo, se no dia 10/01/2017 foi feito o backup, este arquivo será substituído somente pelo backup do dia 10/02/2017, caso aconteça de as datas não coincidirem o arquivo permanece e assim que houver um backup realizado na data de número igual, ocorre a substituição, até porque não é necessário o backup antigo em caso de ocorrer algum problema.

O backup estando salvo no computador e nos *pendrives*, também foi implementado uma ferramenta para armazenamento de backup automático e externo da empresa. Para isso foi utilizado a ferramenta *Google Drive* que demonstrou confiabilidade, praticidade e segurança para armazenamento dos arquivos, além de ser uma ferramenta gratuita, possuir também a ferramenta de e-mail e por ter um armazenamento de 15GB. Espaço muito apropriado para o armazenamento dos backups porque o tamanho dos arquivos não excede esse limite de espaço.

A ferramenta conta com um software de sincronização que automaticamente efetua o upload do arquivo para a plataforma do *Google Drive*. Este software foi instalado e configurado no computador do responsável pelo backup. O mesmo também conta com um marcador de progresso que informa sempre que os arquivos estão sendo copiados para a plataforma. O Sistema está configurado para sincronizar a pasta onde o ProBKP armazena seus arquivos de backup, sendo assim, todos os dias quando ocorre um backup novo, o sistema realiza o *upload* para a plataforma como mostra a figura a seguir.

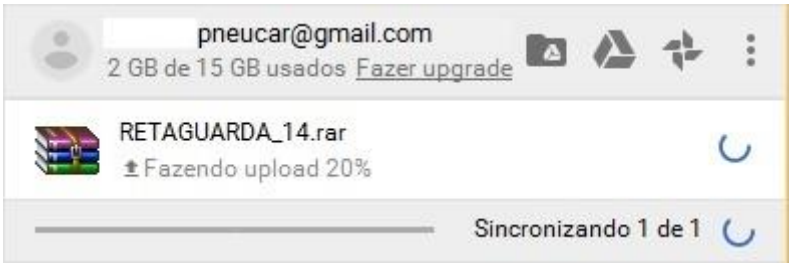


Figura 18. Upload do arquivo de backup

Fonte: O próprio autor

Automaticamente o upload é feito e se um arquivo com o mesmo nome é adicionado, ele é substituído para não deixar muito cheio o espaço, assim os backups antigos sempre serão substituídos pelos mais recentes.

A figura a seguir mostra que mesmo com todos os arquivos de backup de mais de um mês, vemos que o espaço gratuito do *Google Drive* é suficiente para armazenar os arquivos e garantir a segurança de forma externa da empresa.

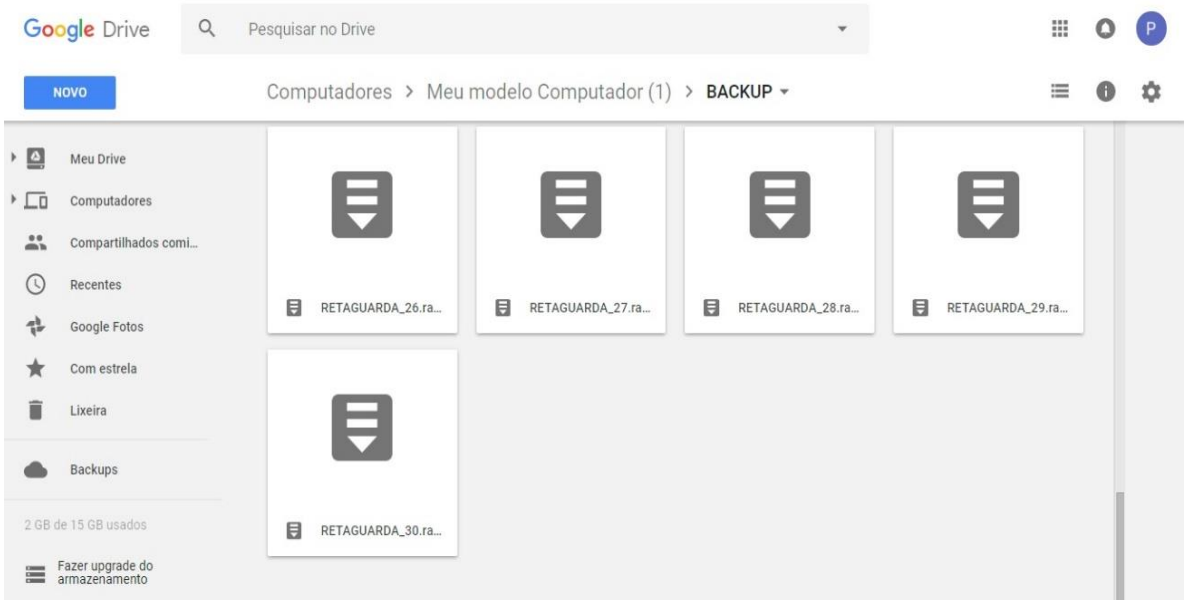


Figura 19. Painel do Google Drive

Fonte: O próprio autor

Com este método os arquivos podem ser conferidos pela direção da empresa e também pela equipe de TI. Caso venha a ocorrer uma falha no processo ou aconteça a ausência de um arquivo novo de backup, a equipe de TI consegue saber e pode entrar em contato para averiguar porque o backup diário não foi realizado.

3. ANÁLISE DOS RESULTADOS

Este capítulo mostra a análise dos resultados que foram atingidos com o andamento deste trabalho. Primeiro será tratado os pontos em que as políticas de segurança entraram em conformidade com o resultado da análise de falhas feitas com base na ABNT NBR ISSO/IEC 27005. Dessa forma será classificado como as políticas melhoraram a segurança.

Foram realizados alguns testes para verificar se as políticas realmente estavam com bom funcionamento e sendo executadas corretamente. Será tratado sobre o termo que foi criado e repassado aos funcionários, que também foram muito importantes para a execução desse trabalho, pois a segurança não depende apenas de aspectos tecnológicos, a segurança também trata ambiente, pessoas e a tecnologia, se esses pontos estiverem em harmonia, é possível garantir um nível maior de segurança da informação.

Após o termo elaborado e repassado aos funcionários, foi aplicado também um questionário, para que fosse possível avaliar a opinião de cada um sobre as mudanças e regras aplicadas na empresa, assim foi possível conhecer como cada um avalia as mudanças e o que acha que pode ou não ser melhorado.

3.1 Análise de falhas e riscos com base na ABNT NBR ISO/IEC 27005

A análise de falhas realizada na empresa Pneucar, mostrou de forma mais organizada, as vulnerabilidades que existiam na rede de computadores. A norma ISO 27005 foi utilizada para promover melhor confiabilidade e por ser um padrão nacional de normas garantiu resultados melhores. Antes não existia um plano de ação caso viessem a acontecer falhas, era necessário identificar onde está o problema e tentar resolver o mais rápido possível. Hoje tendo em mãos riscos classificados em níveis, é possível ter uma visão maior de solução, com essas informações que foi possível elaborar um plano de ação, que gerou restrições na rede de computadores e também um termo de segurança que foi repassado aos colaboradores.

As restrições aplicadas diminuem consideravelmente a incidência e o impacto caso venha a ocorrer uma falha. Hoje o risco de ocorrer uma infecção por vírus é menor, pois menos computadores tem acesso a conteúdos maliciosos, e também os computadores

que podem ser infectados estão protegidos de forma adequada afim de evitar que um arquivo malicioso passe despercebido e venha a atrapalhar os serviços ou até espalhar pela rede de computadores.

Atualmente os funcionários da empresa estão cientes de suas responsabilidades com as informações da empresa, também tem ciência de que atitudes maliciosas podem gerar transtornos, prejuízos ou até o desligamento da empresa dependendo da ocorrência. Restrições aos usuários podem melhorar muito a segurança, pois um usuário só acessa aquilo que lhe é permitido, assim garante a confiabilidade, integridade e disponibilidade das informações.

Com a análise de falhas, as políticas de segurança puderam melhorar muito a segurança do ambiente, porém ainda existem adaptações que podem e devem ser realizadas para melhorar muito a segurança. Como este trabalho teve o foco de aplicar políticas de segurança a nível de regras aos usuários e visando o baixo custo, algumas ferramentas não puderam ser implementadas, ferramentas essas que podem garantir de uma forma mais completa a segurança da empresa.

3.1.1 Conformidade com a ISO

As diretrizes da ISO 27005 tem como foco a exploração de vulnerabilidades. Com isso devido a questões particulares da empresa algumas determinações nas falhas encontradas na análise não podem ser satisfeitas, como a reposição de ativos danificados por exemplo.

No momento a empresa não possuir máquinas servidores de reserva, nem um dispositivo HD (*hard drive*) que armazena todos os arquivos do servidor como cópia ou espelhamento, que é uma funcionalidade capaz de criar em outro HD uma cópia completa dos dados e arquivos do computador onde está instalado.

Mas a empresa não ignorou o problema. Está ciente de que é necessário manter uma válvula de escape caso venha a ocorrer qualquer tipo de falha ou parada inesperada de um ou dos dois servidores. Para isso a empresa vai investir futuramente em dispositivos HD que possam ser configurados como espelhamento. Esse processo também não pode ser implantado no momento porque não é possível parar os serviços dos servidores, e mesmo que existisse essa possibilidade, parar no momento atual e inserir um novo periférico nessas máquinas poderia acarretar em problemas de identificação de hardware,

que poderia ocasionar uma perda total dos arquivos ou até das configurações ocasionando maior tempo de parada dos serviços.

Existem ferramentas que trabalham com diretivas de grupo, muito conhecidas pela sigla GPO. É uma funcionalidade existente em servidores Windows e Linux que garante de uma forma mais eficiente e segura limitações impostas para os usuários e também melhor verificação de logs das ações de cada um no computador. Porém para implementar uma funcionalidade como essa é necessário investir em uma máquina servidor que fará com que todos as máquinas cliente façam requisições a esse servidor. No momento não é possível adquirir dispositivos como um novo servidor. Mas a empresa é ciente que existe essa funcionalidade e quando for possível pode optar por implantar essa ferramenta.

Ainda tratando da reposição de ativos, a empresa possui dispositivos como *hub's* e máquinas cliente reserva. É importante ressaltar que as configurações desses computadores determinados como reserva, são mínimas e não poderiam ser convertidas para uso de um servidor por exemplo pois não tem capacidade de processamento nem memória suficiente para isso.

Mas como já existe um projeto de mudança estrutural na empresa, a direção tem interesse em realizar também uma mudança na rede de computadores devido à necessidade de mudar a localidade de alguns setores dentro da empresa. Assim ser a possível modificar a topologia da empresa evitando o máximo de cascatas possível afim de melhorar a identificação de problemas que possam ocorrer com conexões na rede.

O dispositivo *mikrotik* já existia na empresa com a funcionalidade de criar balanceamento de internet, acionando o outro provedor quando um estiver em queda. Seu acesso e uso também é de prioridade do setor de internet da empresa de TI, algumas das regras nele aplicadas foram possíveis por autorização e instrução do setor a utilizar o dispositivo, mas o mikrotik não é o foco para implementar as políticas de segurança. Por esse motivo isso a ferramenta não foi mais explorada para realizar as políticas, detalhe que este trabalho não tem como foco explorar as funcionalidades de uma ou mais ferramentas específicas afim de garantir a segurança da empresa e sim explorar os recursos que nela já existem.

3.2 Sobre as políticas de segurança

Com finalidade de melhorar a segurança do ambiente, foi formulado o termo de segurança da informação no qual os funcionários têm conhecimento das regras que a empresa aderiu. Para formular este termo foi realizado uma reunião com o presidente da empresa e outros funcionários que fazem parte da administração para adaptarmos os termos as necessidades de acordo com a viabilidade de implementação em cada setor, pois se uma regra atrapalhar o serviço de um funcionário não é uma regra válida e precisaria ser revisada.

É importante ressaltar que a administração da empresa entendeu que políticas de segurança, são revisadas periodicamente, pois mudanças e necessidades vão surgindo, sendo da própria empresa, de um setor ou funcionário específico, com isso as políticas vão sendo revisadas, e sempre que necessário podem ser alteradas.

Afim de atender as vulnerabilidades da empresa, com intuito de minimizar incidências e impactos, o documento foi elaborado e repassado para o presidente da empresa juntamente com os funcionários da administração foi avaliado e autorizado. O documento passou por duas revisões incluindo as políticas com rede *wi-fi* e regras de utilização do antivírus.

O documento final foi autorizado e começou a ser repassado aos funcionários da empresa a partir do dia 16 de outubro de 2017, e logo após houve uma conversa com parte dos funcionários para fazer uma explicação e demonstração dos termos. Assim que os funcionários estavam cientes dos termos foi concluída a divulgação das normas. Este documento encontra-se em anexo neste trabalho. (Anexo 3)

3.3 Responsabilidade dos envolvidos

Nos termos das políticas de segurança aplicados na Pneucar, está descrito para o entendimento dos funcionários, da gerencia e da equipe de TI as informações sobre a responsabilidades que ambos devem ter com as informações da empresa. Estas informações estão no tópico de introdução no termo que foi repassado aos funcionários. (Anexo 3)

3.4 Testes das políticas de segurança

Os testes realizados na empresa foram para avaliação do funcionamento das regras aplicadas na rede de computadores. Primeiramente foi passado em máquina por máquina para verificar se as modificações estavam surtindo efeito. O teste foi realizado durante o mês de outubro, os computadores que sofreram modificações foram verificados nesse período para verificar se aconteceu alguma modificação neste período e se algum computador perdeu configurações.

Para evitar a incidência da utilização de engenharia pessoal para coleta de dados da empresa, foi explicado aos funcionários e também está descrito no termo de políticas de segurança instruções de como se portar com informações da empresa para evitar que pessoas sem nenhum tipo de ligação com a empresa tenham esse tipo de acesso as informações.

> Em posse de determinadas informações, um invasor pode planejar métodos de invasão utilizando palavras chaves coletadas. Essas palavras chaves podem ser utilizadas em métodos específicos para a descobrir de nomes de usuários ou senhas (GIAVAROTO; SANTOS, 2013).

Também foi utilizado uma ferramenta para verificar se o dispositivo gateway da rede está totalmente desprotegido. Como neste dispositivo não existe nenhum tipo de redirecionamento nem necessidade de outros acessos portas de acesso padrão foram bloqueadas para evitar este tipo de exposição. Vale lembrar que para a segurança dos servidores, na rede de computadores eles estão atrás deste dispositivo gateway da rede e também protegidos com um firewall próprio do sistema operacional de cada um e também sem nenhum tipo de conexão com a internet.

3.4.1 Ping

A ferramenta *ping* foi testada em um computador com sistema operacional *windows* que estava conectado nas redes dos roteadores da empresa. O objetivo de uso dessa ferramenta é tentar identificar *hosts* ou computadores na rede dos computadores da empresa. A figura a seguir mostra o resultado do teste usando a ferramenta.

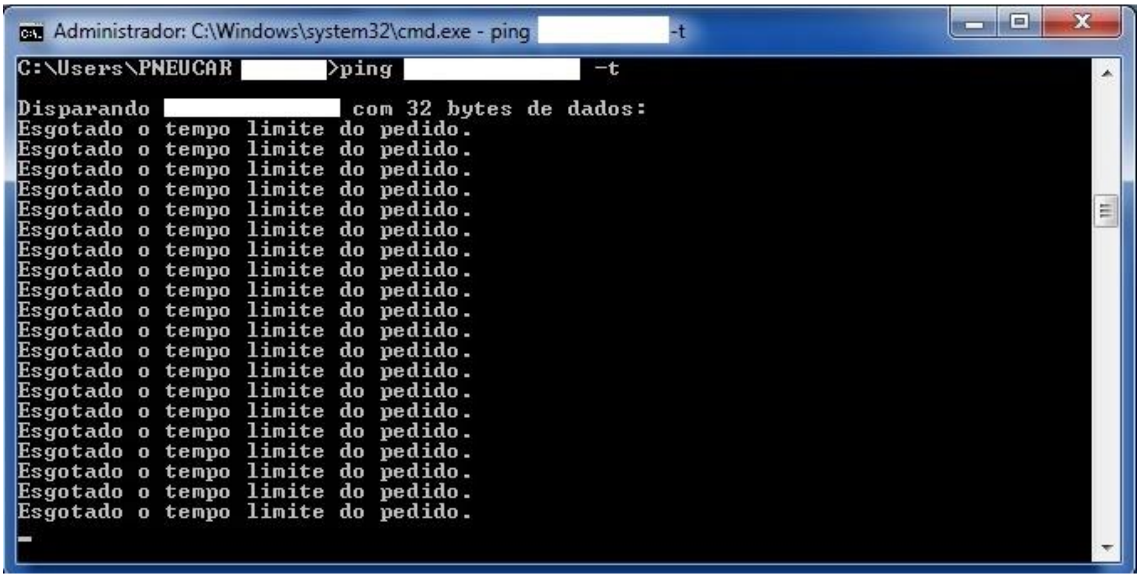


Figura 20. Execução do ping

Fonte: O próprio autor

Foi acrescentado ao comando um parâmetro de execução denominado –t que serve para que o comando seja repetido várias vezes até que seja interrompido manualmente. É possível notar na figura acima que não houve nenhum tipo de resposta computador servidor. Dessa forma não foi possível identificar nem acessar a rede interna da empresa a partir das redes wireless.

3.4.2 Bloqueios nos computadores de trabalho

Esta funcionalidade foi testada manualmente, indo em todos os computadores bloqueados de acessar a internet, de utilizar mídias USB ou realizar instalações de programas e alterar configurações como por exemplo editar registros do Windows ou alterar um endereço de IP. Foi feito os testes em dias diferentes e horários também para averiguar seu funcionamento. O bloqueio de internet não está apenas no computador, mas o bloqueio de mídias de armazenamento por USB e de modificações sem privilégios administrador foram feitas em todos os computadores.

Sendo assim cada computador quando necessita ser substituído ou quando vai para manutenção e é necessária formatação, quando volta para a empresa o mesmo é configurado da mesma forma, bloqueando acessos a *pendrives*, criando o usuário administrador e acesso à internet.

3.5 Questionário de segurança da informação

A opinião dos funcionários foi muito relevante para verificar a usabilidade das mudanças aplicadas na empresa. Para avaliar suas opiniões foi elaborado um questionário e repassado a todos os colaboradores para que pudessem ler atentamente e expressar o que acham sobre as mudanças, a qualidade dos serviços e o estado atual do ambiente da empresa. É um ponto muito importante que os funcionários terem avaliado isso pois eles também tiveram muita importância para realizar este trabalho.

O questionário foi dividido em duas partes, uma para avaliar o grau de satisfação e a opinião dos funcionários sobre as mudanças aplicadas e as políticas de segurança. Durante os 4 dias que o questionário esteve disponível para avaliação, 19 funcionários preencheram e responderam as informações contidas no questionário em anexo neste trabalho (Anexo 4). Os demais que não responderam, foi devido à ausência por período de férias, licença ou por realizarem trabalho externo com muito pouco contato presencial na empresa.

A segunda parte foi para avaliar como as políticas de segurança influenciaram na realização dos seus serviços, e como acham que deve ser a responsabilidade de todos com relação a segurança das informações da empresa. Os resultados foram avaliados em forma de gráfico para melhor demonstração.

Primeira questão avaliada foi como eles avaliam as políticas de segurança.

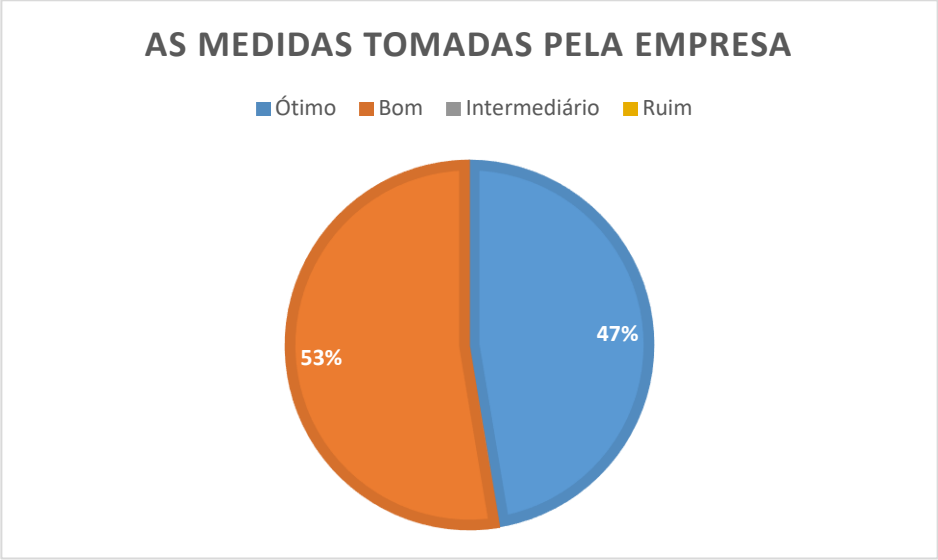


Gráfico 1. Medidas de segurança tomadas pela empresa

Fonte: Próprio autor

O objetivo desta questão foi avaliar se as medidas que a empresa tomou para aplicar as políticas de segurança teve boa aceitação referente as melhorias que trouxe para a empresa. Observando o gráfico 1 é possível identificar que 47% dos colaboradores definiram as medidas como ótimo e 53% definiram que são medidas boas.

A segunda questão são os bloqueios de mídia e acesso à internet na empresa.

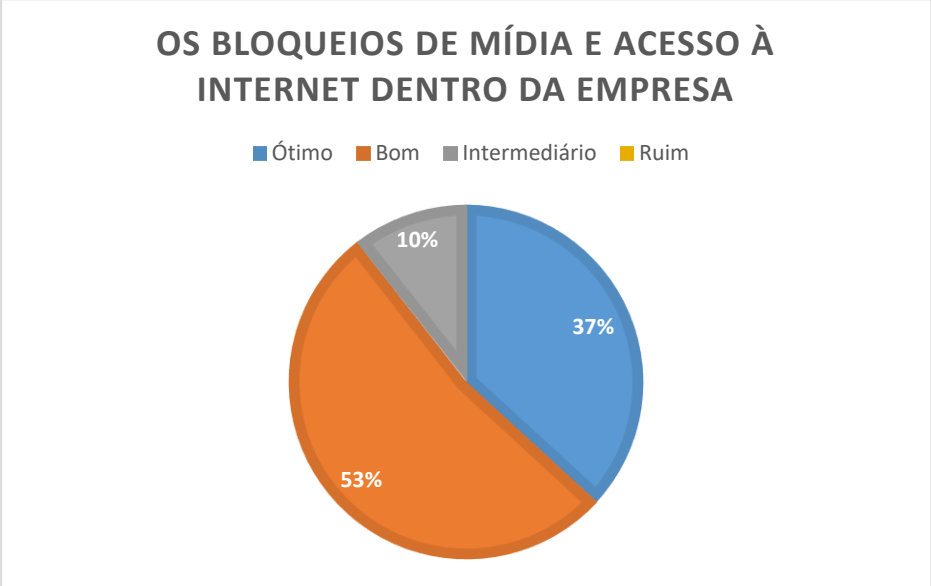


Gráfico 2. Bloqueios de mídias e acesso à internet

Fonte: Próprio autor

O objetivo dessa questão é verificar se os bloqueios que foram realizados dentro da empresa foram bem aceitos, e se os funcionários concordaram que foram regras para melhorar a segurança da informação de toda a empresa. Segundo o gráfico 2 podemos observar que 53% dos funcionários definiram os bloqueios como bom e 37% definiram como ótimo e 10% apenas, definiram como intermediário, com esse resultado foi possível atingir a um bom nível de aceitação dessas restrições.

A terceira questão abordada foi a qualidade atual da rede de computadores.

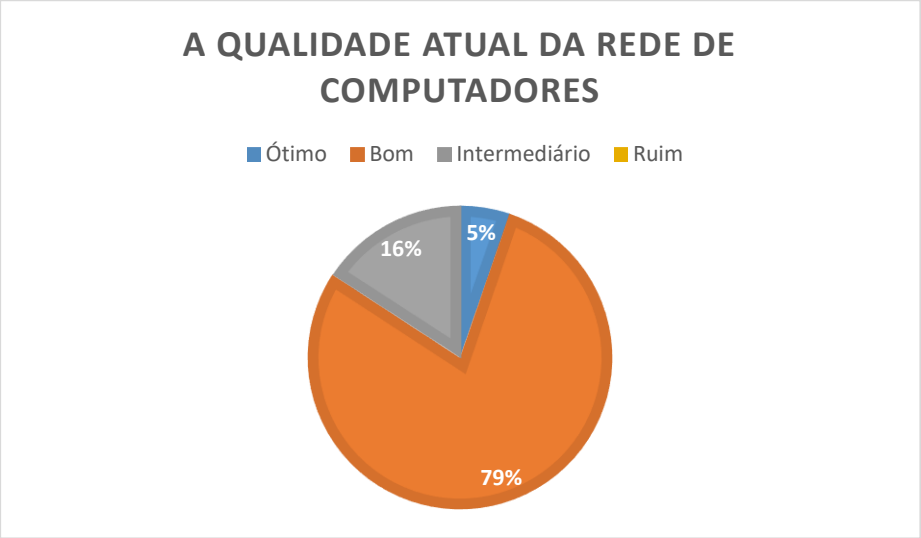


Gráfico 3. Qualidade atual da rede de computadores

Fonte: Próprio autor

Essa questão teve como objetivo analisar o que os funcionários acham da qualidade da rede de computadores da empresa. Mesmo não tendo sofrido mudanças é bom avaliar a satisfação dos usuários com a rede da empresa. No gráfico 3 é possível verificar que 79% dos funcionários avaliaram a qualidade da rede como boa, 16% definiram como intermediária e 5% definiram como ótima. Por esses resultados pode-se avaliar que é aceitável uma modificação na rede.

A quarta questão é sobre as regras aplicadas a rede *wi-fi*.

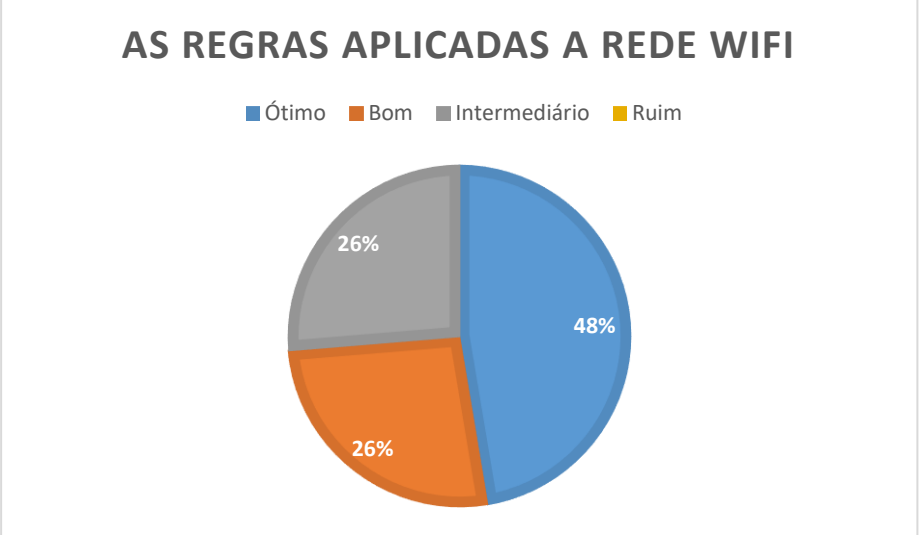


Gráfico 4. Regras aplicadas a rede *wi-fi*

Fonte: Próprio autor

No gráfico quatro podemos observar que 48% dos funcionários definiu como ótimo as regras aplicadas na rede *wi-fi*, 26% definiram como bom e 26% definiram como intermediário. Essa questão foi aplicada para verificar como os funcionários opinaram sobre as regras de uso que a empresa aplicou sobre a rede *wi-fi*. Assim a grande maioria teve uma concordância maior com as regras de uso.

A quinta questão trata sobre o reestabelecimento dos serviços quando surge falhas.

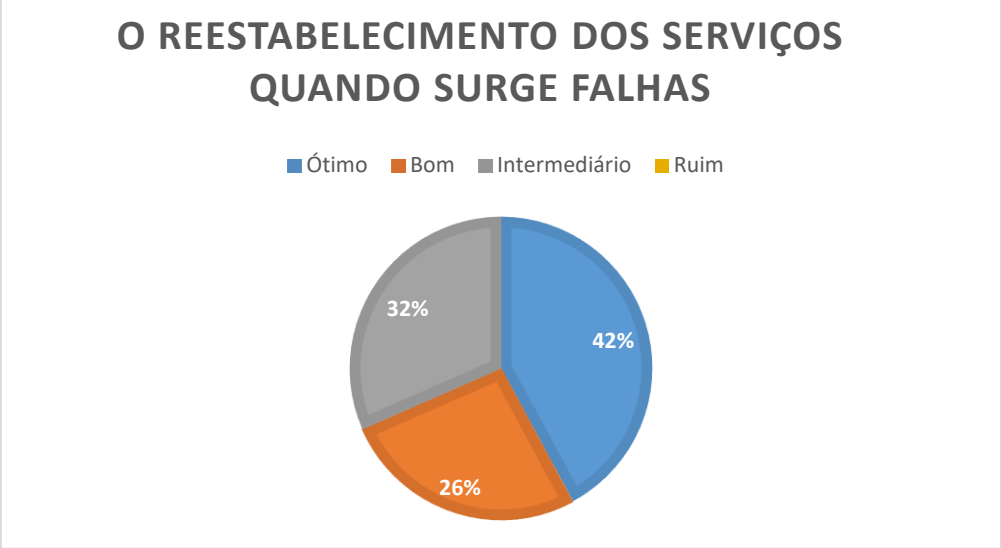


Gráfico 5. Reestabelecimento dos serviços

Fonte: Próprio autor

Essa questão avalia a opinião dos funcionários sobre o restabelecimento dos serviços quando surge alguma falha ou imprevisto que venha a atrapalhar os serviços da empresa. A maioria definiu como ótima totalizando 42%, os demais foram 26% que definiram como bom e 32% como intermediário, sendo assim o reestabelecimento dos serviços são reestabelecidos de forma satisfatória para a maioria, mas de acordo com os resultados este quesito é passível de melhorias.

A sexta questão trata o grau de usabilidade das políticas para que os funcionários realizem seu trabalho.

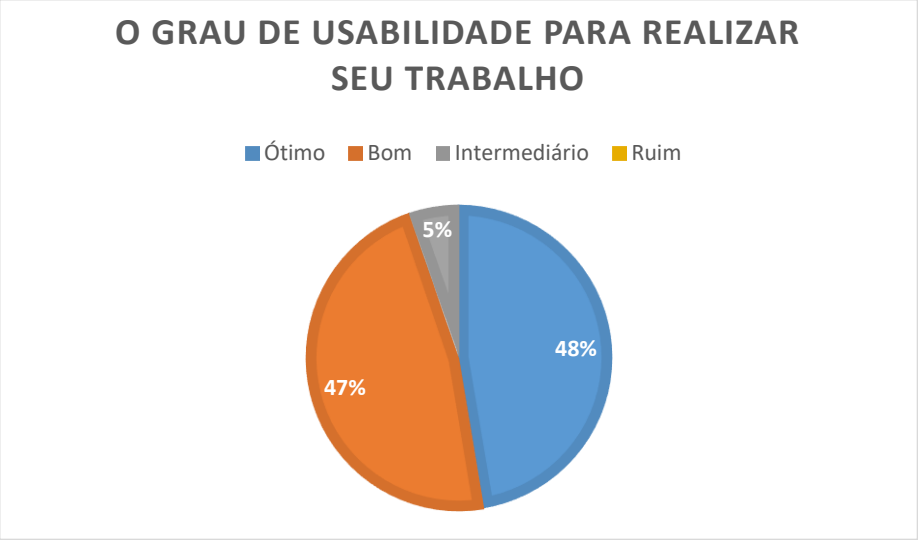


Gráfico 6. Usabilidade das políticas para realizar o trabalho

Fonte: Próprio autor

Esta questão é para avaliar a facilidade com que os funcionários podem realizar seus trabalhos com o emprego das políticas de segurança na empresa. 48% dos funcionários definiram como ótimo, 47% como bom e 5% como intermediário. Dessa forma é possível avaliar que os colaboradores não tiveram dificuldades para realizar seus serviços, mas ainda existe uma minoria que encontrou dificuldades.

A sétima questão trata a viabilidade das políticas na empresa.

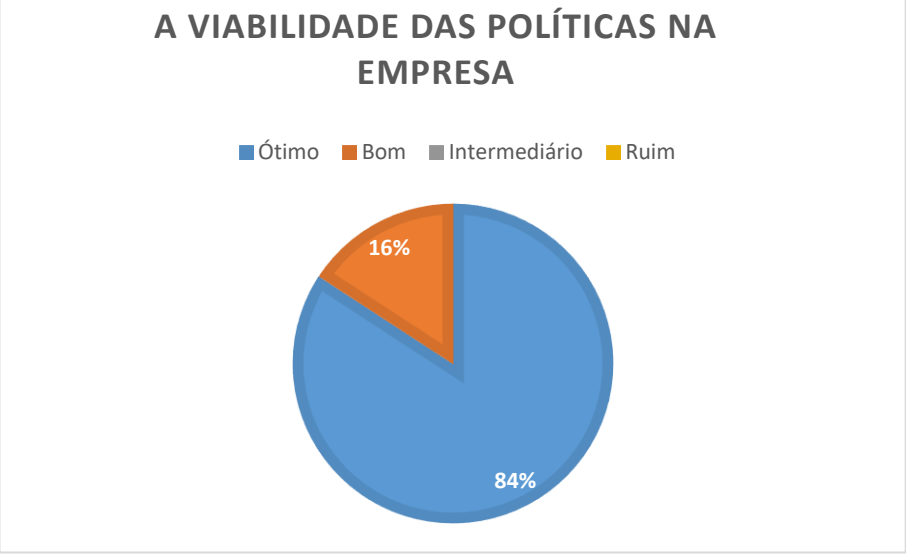


Gráfico 7. Viabilidade das políticas de segurança na empresa

Fonte: Próprio autor

Essa questão trata como os funcionários avaliam a viabilidade técnica das políticas de segurança, ou seja, se as regras obedecem às características a respeito dos serviços que são realizados na empresa, e se atende as condições que a empresa se encontra e também não é prejudicial aos próprios funcionários. 84% dos funcionários definiram como ótimo a viabilidade das políticas, já outros 16% definiram como bom. Assim pode-se classificar como políticas de segurança viáveis para a empresa.

A oitava questão trata o acesso aos sistemas que o funcionário utiliza.

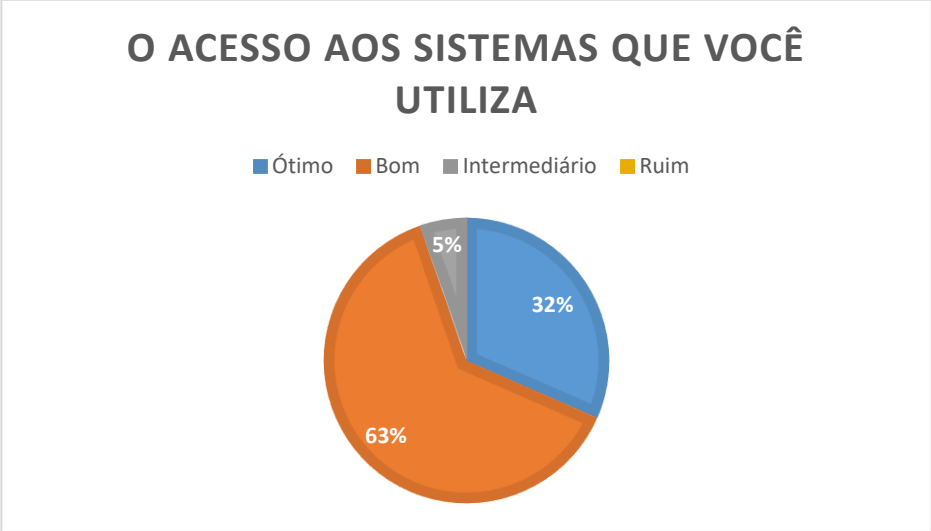


Gráfico 8. O acesso aos sistemas que utiliza.

Fonte: Próprio autor

Esta questão analisou se houve melhoria na execução dos sistemas que são utilizados em rede pelos funcionários. De acordo com o Gráfico 8 é possível analisar que 32% dos funcionários consideram que o acesso aos sistemas é ótimo, 63% consideram que o acesso é bom e 5% consideram que o acesso é intermediário. Dessa forma é possível assegurar que os funcionários não obtiveram dificuldades para acessar os sistemas e realizar seu trabalho.

A questão nove aborda a necessidade de mudanças na rede de computadores.

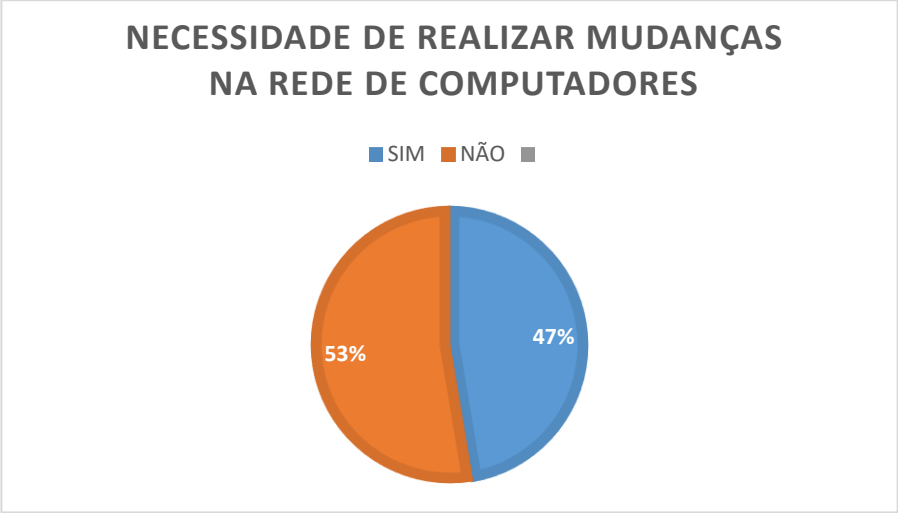


Gráfico 9. Necessidade que a empresa efetua mudanças na rede de computadores

Fonte: Próprio autor

Esta questão trata a opinião dos funcionários quanto a necessidade de modificar a rede de computadores da empresa. Segundo o gráfico 9 é possível considerar que 53% dos funcionários acham que não precisa efetuar mudanças e 47% acham que é necessário. Mais da metade está conformada com a estrutura de rede que trabalham.

A décima questão trata se a empresa deveria investir mais em segurança.

Gráfico 10. Necessidade de investimento em segurança da informação

Fonte: Próprio autor

Esta questão aborda a opinião dos funcionários se a empresa necessita de investir mais em segurança da informação. Segundo o gráfico 10 é possível considerar que 53%

dos funcionários avaliam que sim, a empresa deve investir mais enquanto 47% acreditam que não é necessário. Ou seja, a maioria acredita que é bom efetuar mudanças e investir mais na segurança da empresa, afinal segurança para a empresa também significa segurança para os funcionários.

A décima primeira questão verifica se as políticas prejudicaram os serviços.

Gráfico 11. As políticas prejudicaram os serviços

Fonte: Próprio autor

Segundo o gráfico 11 podemos notar que 100% dos funcionários avaliaram que as políticas de segurança não prejudicaram os serviços que eles realizam na empresa.

A segunda parte do questionário trata sobre a importância e a responsabilidade dos funcionários com a segurança da informação na empresa.

A décima segunda questão trata o grau de importância para a segurança da informação para a empresa.

Gráfico 12. Importância da segurança da informação para a empresa

Fonte: Próprio autor

Segundo o gráfico 12 é possível considerar que 100% dos funcionários acreditam que a segurança da informação é importante para a empresa. As informações que são repassadas para os funcionários sobre boas práticas de segurança são relevantes e fazem os mesmos terem melhor entendimento do assunto.

A décima terceira questão trata a necessidade de melhorias na segurança das informações.

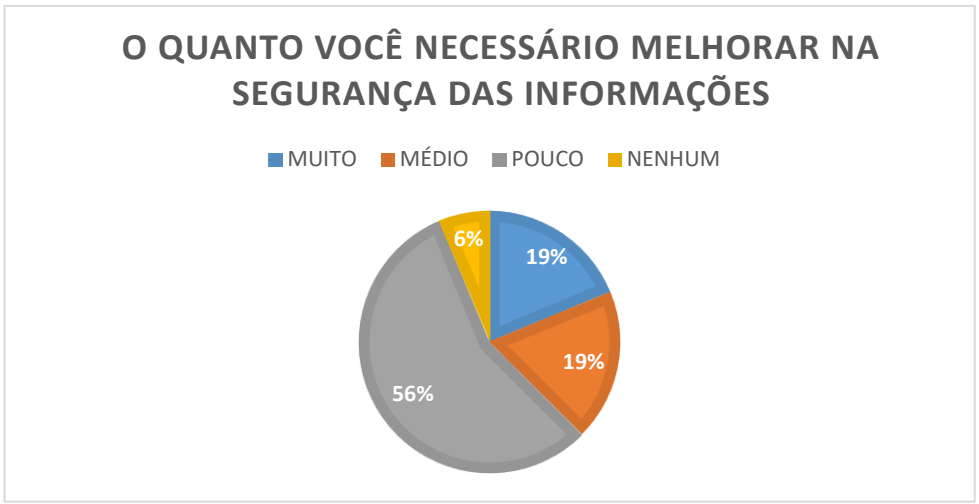


Gráfico 13. Necessidade de melhorar em segurança da informação

Fonte: Próprio autor

Segundo o gráfico 13, 56% dos funcionários avaliaram que a empresa precisa melhorar pouco na questão segurança da informação, enquanto 19% dos funcionários definiram a necessidade de melhoria como médio, 19% como muito, enquanto 5% dos funcionários definiram que a empresa não precisa melhorar em relação a segurança da informação.

A questão quatorze trata a importância das informações e orientações que devem ser repassadas sobre a segurança da informação

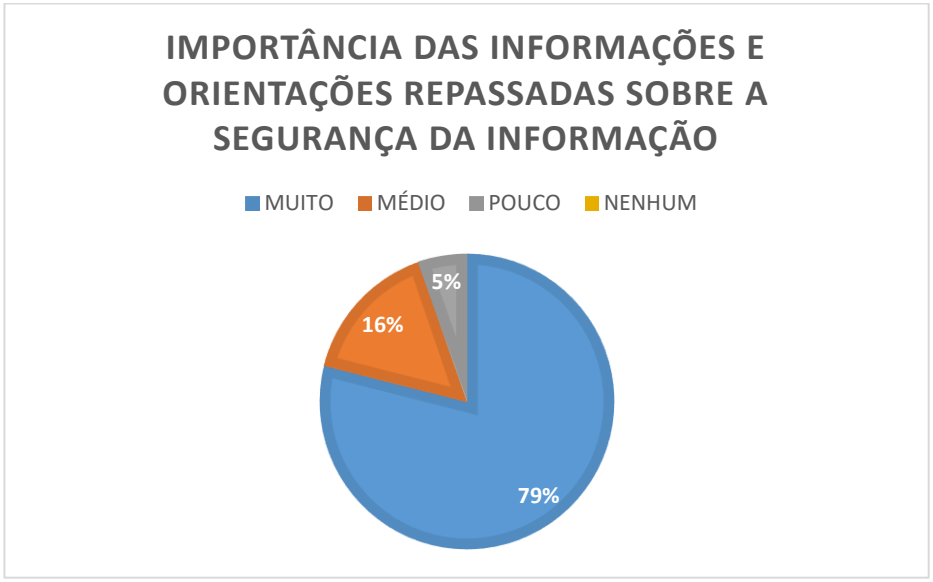


Gráfico 14. A importância das informações e orientações sobre segurança da informação

Fonte: Próprio autor

Pode-se notar observando o gráfico 14 que 79% dos funcionários definiram como muito importante o repasse de informações e orientações sobre segurança da informação, enquanto 16% definiram como média e 5% deram pouca importância para essas informações.

A questão quinze avalia a responsabilidade que todos devem ter para manter a segurança das informações da empresa

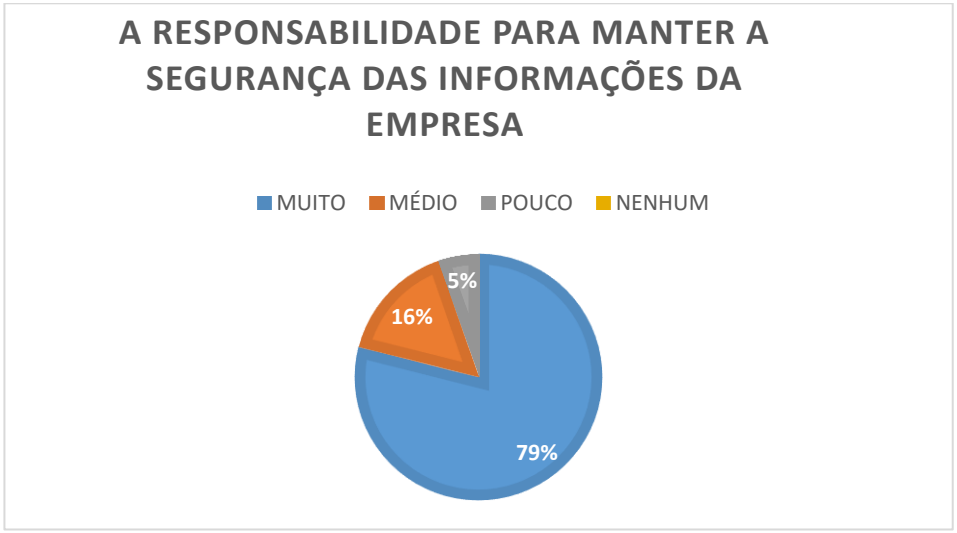


Gráfico 15. Responsabilidade para manter a segurança das informações da empresa

Fonte: Próprio autor

Observando o gráfico quinze é possível avaliar que 79% dos funcionários definiram como muito importante as suas responsabilidades para manter a segurança das informações na empresa, enquanto 16% definiram como média importância e 5% como pouca importância.

A questão dezesseis trata a responsabilidade que todos devem ter para manter a segurança das suas próprias informações dentro da empresa

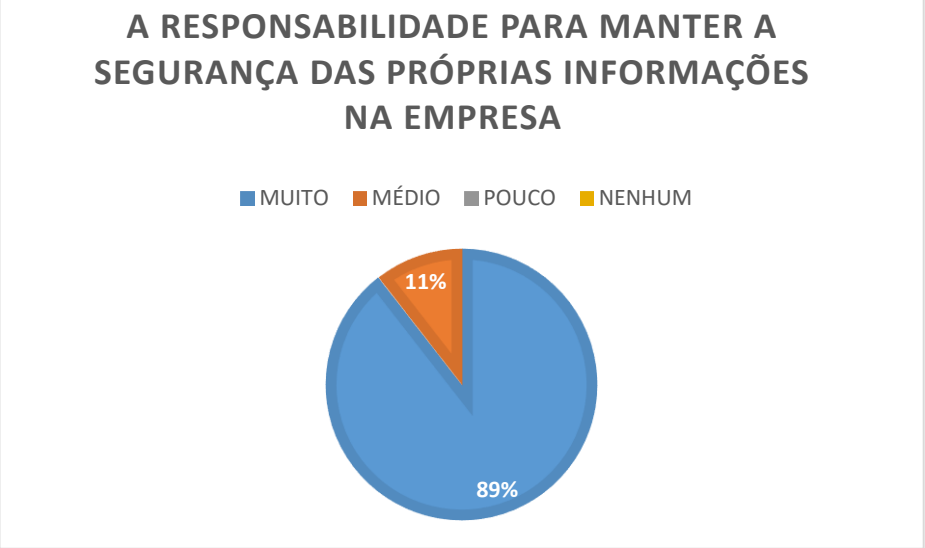


Gráfico 16. Responsabilidade para manter a segurança das próprias informações na empresa

Fonte: Próprio autor

Segundo o gráfico dezesseis é possível avaliar que 89% dos funcionários definiram como muito importante as suas responsabilidades para manter a segurança das próprias informações na empresa, enquanto 11% definiram como média importância. Um exemplo deste tipo de informação é a integridade de suas informações pessoais e de uso dentro da empresa como senhas pessoais, *logins* de usuário entre outros, com finalidade de até evitar vulnerabilidades como engenharia pessoal.

A questão 17 mostra como os funcionários avaliaram a qualidade dos serviços prestados referentes a segurança da informação.

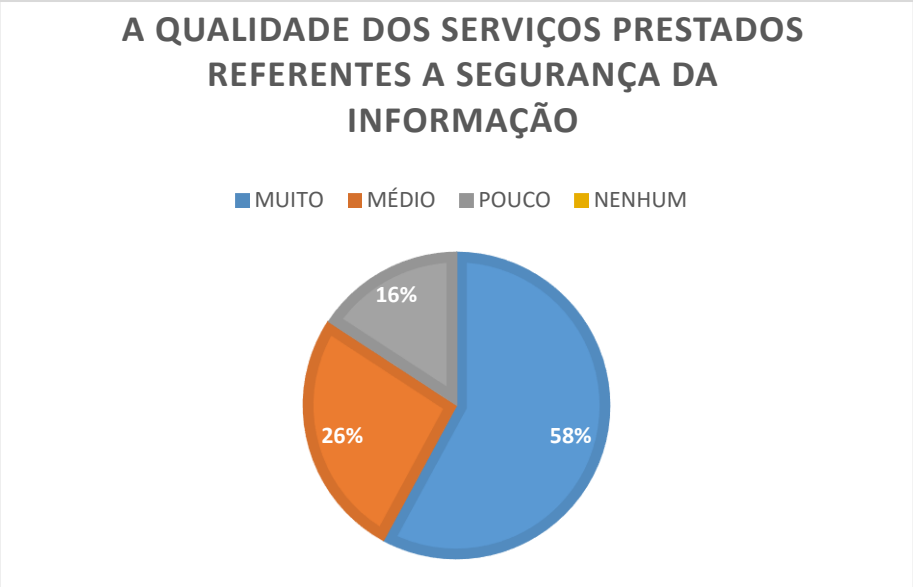


Gráfico 17. Qualidade dos serviços prestados

Fonte: Próprio autor

Segundo o gráfico dezessete, a qualidade dos serviços prestados foi classificada em 58% como muito boa, 26% como média e 16% como pouco satisfatória para os funcionários. Assim podemos concluir que a maioria está satisfeita com a prestação de serviços da equipe de TI na empresa. Essas pessoas que estão pouco satisfeitas são um ponto que pode ser analisado e verificar por quais motivos seu nível de satisfação com os serviços não está como a maioria.

4. CONCLUSÕES

O objetivo deste trabalho foi melhorar a segurança da informação na rede de computadores da empresa Pneucar visando baixo custo financeiro, aplicando regras a nível de usuário como termo de políticas de segurança, utilizando os recursos que a empresa podia disponibilizar efetuando inicialmente uma análise de falhas e riscos com base nas melhores práticas propostas pela NBR ISO/IEC 27005.

A ISO não trata métodos e práticas para aplicar a segurança da informação, a norma trás em suas diretrizes métodos de documentação, análise e gestão de falhas e riscos. Os passos para analisar o ambiente, verificar os pontos vulneráveis e o que podia ocasionar problemas para a empresa, foi justamente ponto chave para que medidas pudessem ser tomadas e as políticas serem implantadas. A ISO utilizada neste trabalho não tem diretrizes que indicam que o ambiente deve possuir métodos como firewall, bloqueios para evitar invasão e etc., mas suas diretrizes têm tabelas de informação muito bem definidas para classificar com melhor qualidade as falhas que o ambiente possui.

Para alcançar um nível de segurança melhor que o atual, foi feito a análise de falhas e riscos de segurança da informação, explorando o ambiente da empresa, indo em todos os setores, efetuando mapeamento da rede de computadores, e analisando todos os componentes e ativos na rede de computadores. A finalidade da análise foi colher falhas e pontos vulneráveis na rede de computadores, tendo estes resultados documentados foi possível elaborar um plano de ação, onde deu origem as políticas de segurança da empresa.

A melhoria na segurança foi alcançada podendo observar os testes realizados e a opinião dos usuários com o questionário de segurança, pois as restrições aplicadas com intuito de melhorar o ambiente, não prejudicou os serviços dos funcionários além de melhorar o nível de segurança, onde não existia regras nem termos de responsabilidade, hoje a empresa está organizada nesse ponto. Assim é possível notar eficiência da nova aplicação feita no ambiente de estudo. Fica evidente melhoria no ambiente empresarial referente a segurança da informação podendo ser observado nos gráficos de análise dos questionários.

Com isso é possível concluir que organizando bem as restrições de uma empresa, adaptando-se e instruindo os funcionários a seguir regras de segurança sem interferir de

forma negativa na execução de seus trabalhos, é possível proporcionar a segurança da informação que muitas empresas desejam no seu ambiente.

Este trabalho foi realizado com intuito de também contribuir com outros trabalhos realizados com foco na segurança da informação em redes de computadores. Esse trabalho é importante mostrar a necessidade do conhecimento das técnicas de normalizações padrão ISO e sendo possível melhorar a segurança da informação de um ambiente, com simples regras de segurança que aplicadas aos colaboradores do ambiente podem garantir a segurança e evitar diversas possibilidades de riscos.

Este estudo não teve objetivo de mostrar a melhor maneira de promover segurança da informação, mas agrega bastante valor pois é mais uma forma eficiente de mostrar que boas práticas, regras bem definidas e restrições necessárias em redes de computadores podem ser muito importantes para melhorar a segurança do ambiente. Porém é necessário sempre visar as melhores práticas possíveis para promover a segurança do ambiente. Por isso para uma análise mais qualitativa, foi utilizado a ABNT NBR ISO/IEC 27005 que possui ótimas práticas de documentação e avaliação de vulnerabilidades em redes.

Finalizando, este trabalho, mostra a importância de ter políticas de segurança em ambientes empresariais, mantendo a organização da empresa, e visando a segurança dos dados, e que nem sempre é necessário realizar gastos extremos com equipamentos de segurança que podem ser muito caros. Obtendo regras bem definidas, restrições desejáveis e com a contribuição dos colaboradores e da direção da empresa é possível manter um ambiente mais seguro. A participação de todos os envolvidos da empresa é que são os responsáveis pelo êxito deste trabalho.

4.1 Trabalhos Futuros

Este trabalho trata um estudo de caso onde foram analisados a estrutura de processos e de um ambiente empresarial, com isso o autor teve a liberdade de colher informações para a realização deste trabalho

Com isso o estudo de segurança da informação pode ser ampliado visando outros pontos que também afetam a segurança da informação e também a aplicação de ferramentas que podem garantir a segurança, como por exemplo o estudo de uma ferramenta de diretivas de grupo (GPO) para promover a segurança da informação de uma rede de computadores afim de atender as diretrizes da ABNT NBR ISO/IEC 27001 que

possui mais diretrizes e pontos de verificação do que a norma utilizada neste trabalho.

Outro ponto que pode ser pesquisado é a utilização de ferramentas Linux afim de promover a segurança da informação, com base nos padrões NBR ISO/IEC 27001, que é uma técnica de normalização com mais diretrizes e foco em diversos ambientes desde log de acessos a bloqueios afim de evitar invasões.

Por último, também a ser estudado é a implementação um plano de ação para a reposição de ativos utilizando métodos ágeis, ferramentas que podem sanar as falhas de ativos de informação.

REFERÊNCIAS

ABNT. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582> Acesso em: 27 abr. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2011**, Tecnologia da informação — Técnicas de segurança — Gestão de riscos de Segurança da Informação.

CUNHA, André. **O Valor das informações para empresas e a importância da segurança da informação**. Disponível em: <https://pt.slideshare.net/acunha_sp/o-valor-das-informaes-para-as-empresas-e-a-importancia-da-seguranca-da-informacao> Acesso em: 20 abr. 2017.

EQUIPE TARGET. **A Gestão da Segurança da Informação em uma Empresa.** Disponível em: <https://www.target.com.br/produtos/materias-tecnicas/2011/11/17/2382/nbr-iso-iec-27003-as-diretrizes-para-a-implantacao-de-um-sistema-de-gestao-de-seguranca-da-informacao> Acesso em: 21 abr. 2017.

FERNANDA, Adrielle. **SEGURANÇA DA INFORMAÇÃO.** 14 Mar 2011. Disponível em: http://www.ice.edu.br

FONSECA, Fernando. **ISO/IEC 27005 Exemplificada.** Disponível em: <ftp://ftp.registro.br/pub/gts/gts15/02-ISO-27005-exemplificada.pdf> Acesso em: 21 abr. 2017.

FONTES, Edison **Gestão de Riscos de SI – Norma 27005:2008** Disponível em: <http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/889> Acesso em: 21 abr. 2017.

LIMA, Gustavo Norma ABNT NBR ISO/IEC 27003:2011. **Disponível em:<http://blog.corujadeti.com.br/norma-abnt-nbr-isoiec-270032011/> Acesso em: 21 abr. 2017.**

LUIS, Ewertton **O CONTEXTO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO. <**http://www.atenas.edu.br> Acesso em: 22 abr. 2017.

PWC. **Pesquisa Global de Segurança da Informação**. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13.pdf >. Acesso em: 21 set. 2017.

SEGINFO. Quais são os Melhores Livros de Monitoramento de Redes. Disponível em: <https://seginfo.com.br/2015/12/21/6-passos-para-evitar-vazamento-de-dados-na-sua-empresa-2/> Acesso em: 22 ago. 2017**.**

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.

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

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

ANEXOS

Anexo 1 - Autorização da empresa para aplicação do trabalho.

PNEUCAR

Av. Presidente Tancredo Neves, 2.233/2.255
B. Zacarias - CEP: 35.300-102 - Caratinga - MG
Tel.: (33) 3329-5555 - Fax: (33) 3321-6677

AUTORIZAÇÃO PARA IMPLEMENTAÇÃO DE TCC

Eu, Gladson Ramalho de Oliveira, presidente da empresa PNEUCAR PNEUS CARATINGA – LTDA, autorizo o aluno Warlisson Costa de Oliveira a utilizar o nome e as dependências desta empresa com a finalidade de implementar o seu trabalho de conclusão de curso aplicado na rede de computadores com foco na área de segurança da informação.

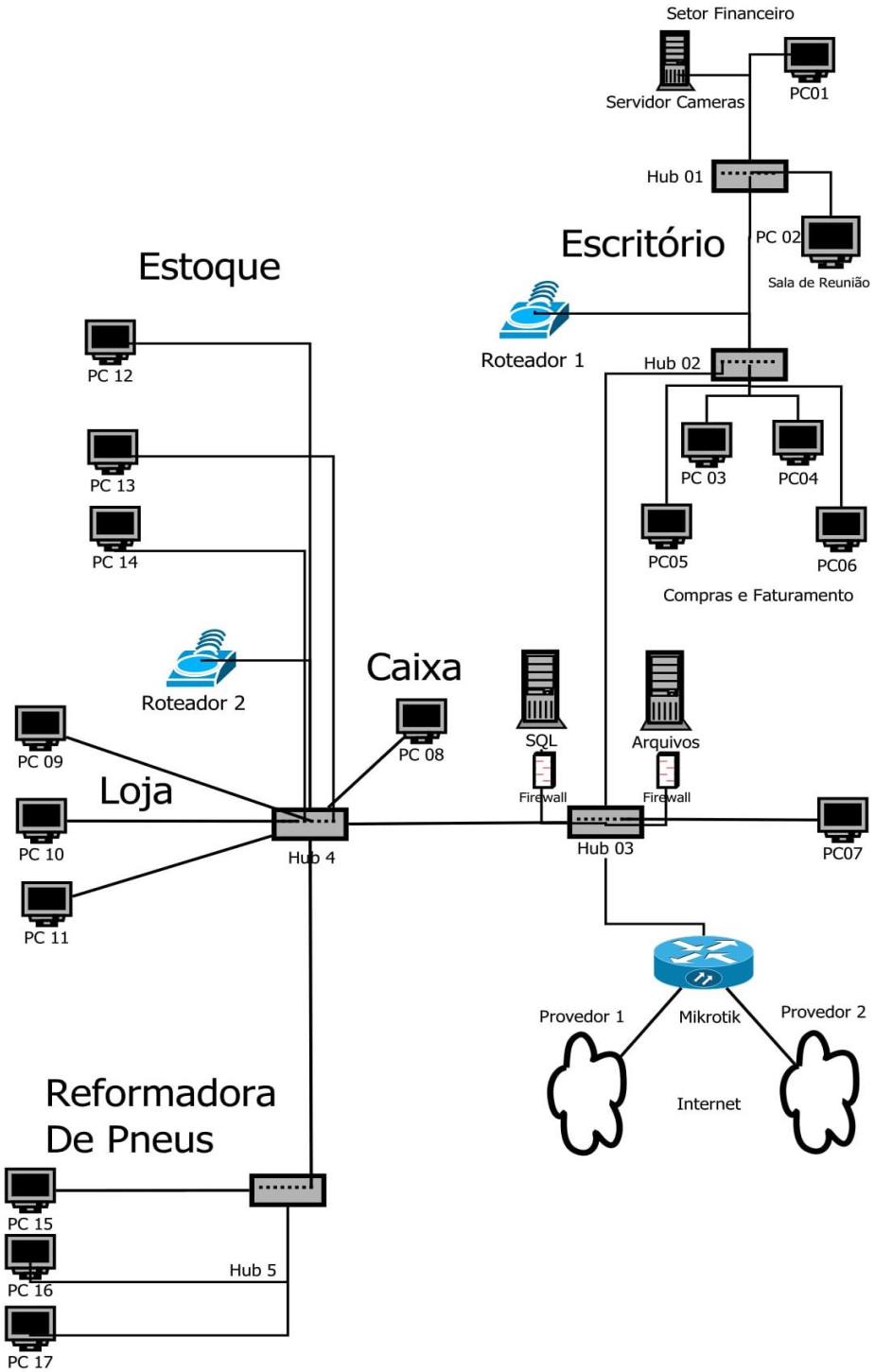
Caratinga, 30 de junho de 2017

Gladson Ramalho de Oliveira
Presidente da empresa

PNEUS NOVOS, SERVIÇOS DE REFORMAS, SUSPENSÃO, FREIOS, ALINHAMENTO E BALANCEAMENTO DE AUTOMÓVEIS E CAMINHÕES

PNEUCAR - PNEUS CARATINGA LTDA
C.N.P.J.: 21.523.543/0001-63 - Insc. Est.: 134.314.096-0087

Anexo 2 - Mapa da rede de computadores da empresa



Anexo 3 - Termo de responsabilidade – Políticas de Segurança

Políticas de Segurança

Empresa: PNEUCAR PNEUS CARATINGA LTDA

Políticas introduzidas para garantir melhor forma de segurança e monitoramento das informações que são utilizadas e disponíveis na rede de computadores da empesa, visando estações de trabalho, sistemas de informática entre outros.

1. Introdução

A segurança é um assunto muito importante a ser tratado em qualquer ambiente. Preocupando-se com isso, a Pneucar apresenta este documento com um conjunto de normas, instruções e procedimentos para melhorar a segurança das informações do ambiente de trabalho. A empresa tem como intuito minimizar a incidência de falhas que podem afetar nos processos e na segurança dos dados da empresa.

Princípios

- A informação produzida ou recebida como resultado de sua atividade profissional pertence PNEUCAR.
- A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.

A empresa e a política de segurança

Todas as normas aqui estabelecidas deveram ser seguidas à risca por todos os envolvidos com nossos serviços. Ao receber essa cópia da Política de Segurança, você como funcionários, parceiros ou prestadores de serviços, aceita comprometer-se com todos os tópicos que são informados aqui, e fica ciente que informações como e-mails e sites visitados na internet podem estar sendo monitorados. Os envolvidos para o desenvolvimento deste documento encontram-se a disposição para sanar dúvidas que surgirem.

Objetivo

Esta política de segurança da informação aplica-se a todos colaboradores da empresa afim de definir responsabilidades e orientar a conduta de todos, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações da PNEUCAR

2. Autenticação

Os sistemas que a empresa trabalha são autenticados por um código de usuário e por uma senha. Crie suas senhas de forma que seja possível lembrar facilmente da mesma, uma sugestão é criar combinações com dados como datas, nomes entre outros. Tente criar sua senha de forma responsável e obedecendo a política de senhas.

2.1 Política de senhas

- Uma senha só será segura se a mesma for intransferível

- Sua senha não deve ser passada a outro funcionário ou nem mesmo para os membros da equipe de segurança. Caso venha a desconfiar que sua senha foi descoberta por outro funcionário, ou tenha à esquecido, entre em contato com a gerência do seu setor para providenciar rapidamente a alteração da mesma.
- Facilite sua senha criando padrões de relação para lembrar sua senha com mais facilidade.

- Os sistemas de informática possuem um sistema de logs, ou seja, é possível analisar qualquer ação realizada e quem foi o usuário que fez essas ações, com isso, qualquer ação executada com seu usuário e senha será de toda responsabilidade, para não ocorrer problemas com isso, mantenha o mais secreto possível a mesma.

3. Política de segurança com e-mail

- Antes de abrir um e-mail, analise se o remetente é de fonte conhecida ou confiável, ou até mesmo se já esperava um e-mail deste endereço eletrônico.

- Atenção com todos os e-mails que venham com assuntos desconhecidos ou suspeitos. Um exemplo disso são e-mails com assuntos com conotação sexual, informações em inglês entre outros.

- Não abra e-mails com arquivos anexo com extensões como .exe, .bat, .html, caso venha a desconfiar do anexo, entre em contato com a equipe de TI para verificar estes arquivos.

- Não utilize o e-mail corporativo para uso pessoal, o mesmo só deve ser utilizado para assuntos da empresa.

- Senha do e-mail também deve seguir os mesmos padrões da política de senhas. No caso de e-mail corporativo, não transfira a senha deste para funcionários de outros setores ou até mesmo pessoas de fora da empresa.

4.Política de acesso à internet.

A empresa possui um dispositivo que limita a banda de navegação a internet por máquinas. Neste caso, somente as máquinas do escritório e o computador do caixa que possuem acesso à internet. A demais máquina tem seu acesso totalmente bloqueado, uma vez que por decisão da direção da empresa, os demais setores não têm necessidade acesso à internet para realizar suas devidas funções.

- O uso recreativo da internet não deverá ocorrer no horário de trabalho.

- Utilize a internet apenas para navegar em sites.

- Sites com conteúdo pornográfico, jogos, bate-papo entre outros relacionados a entretenimento será monitorado e bloqueado.

- É proibido fazer downloads de arquivos muito grandes, ou de ferramentas que vão forçar o download de arquivos como Utorrent e entre outros.

- É proibido o uso de ferramentas de mensagem que não sejam autorizados pela empresa. As Ferramentas autorizadas atualmente na empresa é o Telegram e o Whatsapp em casos totalmente específicos.

5.Política de acesso à rede Wirelles.

A empresa possui rede wi-fi disponível para os clientes e para os funcionários caso venha a ser necessário ser utilizada. Um dispositivo fornece acesso aos funcionários do escritório em uso de trabalho e outra para a loja com finalidade de atender preferencialmente os clientes. Ambas as redes não fazem acesso a mesma rede que estão os computadores da empresa. Essa regra foi adotada para que não exista conflitos de informação, acesso não autorizados ou a danificação de dispositivos da empresa.

- A regra de não acesso à internet em determinados setores da empresa também é a mesma para a rede wi-fi.

- Caso exista algum dispositivo não autorizado acessando a rede wi-fi o mesmo terá o acesso bloqueado.

- É proibido o uso de aparelhos pessoais na empresa e conecta-los a rede wi-fi (Notebook, smartphone, tablete entre outros), conexões deste tipo podem acontecer somente com supervisão e autorização da direção.

- A rede wi-fi é destinada exclusivamente para os clientes, pode ser utilizada por funcionários caso o mesmo não esteja em horário de trabalho.

6.Política de uso do computador de trabalho.

- Cada computador possui configurações que permitem a análise das ações realizadas e que identificam este terminal na rede da empresa. No caso do escritório cada utilizador tem seu próprio computador para realizar suas funções, sendo assim cada um se responsabiliza pelas ações executadas no seu computador.

- Não instale nenhum programa/*software* que não seja autorizado pela direção ou pela equipe de TI.

- Evite transferir para seu computador de trabalho arquivos como músicas, fotos pessoais, filmes e vídeos entre outros, a equipe técnica não se responsabiliza por estes tipos de informações e orienta que não tenha esses tipos de arquivos no mesmo na mídia de transferência não sabe se existe algum tipo de vírus ou *malware*.

- Utilize seu computador apenas para uso pessoal, garanta que no seu computador exista apenas dados de uso da empresa, essas informações devem ser preferencialmente armazenadas no servidor.

- Procure efetuar periodicamente backup dos seus arquivos de trabalho. Caso não saiba como realizar este procedimento entre em contato com a equipe de TI.

7. Vírus, *malwares* e arquivos maliciosos

Para os computadores com acesso à internet.

- Procure verificar atualizações para o seu antivírus periodicamente. Qualquer dúvida ou falha que ocorrer durante o procedimento, a equipe de TI se encarregará de verificar e resolver sempre que necessário.

- Informe a equipe de TI caso a licença de uso do antivírus esteja expirando e serão tomadas as medidas para renovação.

- Periodicamente coloque seu antivírus para analisar todos os arquivos do seu computador. Durante esse processo o antivírus pode deixar o computador lento, então preferencialmente inicie essa atividade pouco antes de iniciar o seu horário de almoço para que a lentidão que possa ocorrer não atrapalhe o andamento do seu trabalho. Caso retorne a empresa e a análise ainda não foi concluída pause o procedimento e deixe dar continuidade em outra oportunidade. Em caso de dúvida comunique a equipe de TI para verificar a situação.

Para todos os computadores da empresa.

- Para garantir a segurança do ambiente empresarial os computadores dos setores da produção, estoque e loja são bloqueados para uso de mídias USB como *pendrive*, mp3, celular entre outros.

- Não traga dispositivos de armazenamento como, *pendrives*, cd ou dvd e etc que venham de fora da empresa a menos que seja necessário o uso. Mesmo que haja necessidade de utilizar tal dispositivo, entre em contato com a gerência da empresa ou diretamente com a equipe técnica para o dispositivo possa ser verificado antes do uso e para efetuar a liberação da sua máquina para utilizar o mesmo.

- Caso presencie situações suspeitas de mal funcionamento do computador ou do sistema, entre em contato com a equipe de TI, para que seu computador possa ser verificado e se houver presença de algum vírus ou arquivo malicioso, o mesmo seja identificado e eliminado o mais rápido possível.

- Tenha suspeita com sites ou arquivos onde você clica e não exibe nenhuma informação na tela.

8. O não cumprimento dessa política

O colaborador que não vier a cumprir com essas políticas estará sujeito a medidas administrativas que viram a ser tomadas de acordo com a gravidade da ocorrência, uma

vez que dependendo do nível de tal gravidade poderá acarretar no desligamento do funcionário.

9 . Segurança para nosso trabalho.

Uma informação só será segura se a mesma também for disponível e autentica as partes que necessitam dela. Para buscar melhor esta segurança para todas as partes envolvidas na empresa este documento foi desenvolvido. Contamos com a sua colaboração e a de todos os membros da empesa para que possamos manter nosso ambiente de trabalho o mais seguro possível e que possamos nos tornar cada vez mais uma empresa que presta serviços em excelência para nossos clientes. Caso houver alguma dúvida ou sugestão para estas informações, entre em contato com a gerência ou direção da empesa, podendo entrar em contato direto com a equipe de TI.

Equipe de TI

Prodata Informática e Cadastro LTDA
Telefone: (33) 3322-6363
E-mail: prodatafinanceiro@gmail.com
Contato: Warlisson, Eduardo ou Silveira

Presidente da empresa

Gladson Ramalho de Oliveira
E-mail: gladsonramalho@oi.com.br
Ramal: 56

Li e concordo com as regras de trabalho as informações citadas acima.

_____

Assinatura do colaborador

Anexo 4 - Questionário para avaliação das políticas implementadas

Questionário de Trabalho de Conclusão de Curso - Políticas de segurança da informação.

Nome:
Setor:
Cargo:
Escolaridade:

Sobre as políticas de segurança aplicadas na empresa, como você avalia:

As medidas tomadas pela empresa?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

Os bloqueios de mídias e acesso à internet dentro da empresa?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

A qualidade da atual rede de computadores?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

As regras aplicadas a rede *wi-fi*?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

O reestabelecimento do serviço quando surge falhas?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

O grau de usabilidade para realizar seu trabalho?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

A viabilidade das políticas aplicadas na empresa?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

O acesso aos sistemas que você utiliza?				
ÓTIMO ( )	BOM ( )	INTERMEDIÁRIO ( )	RUIM ( )	PÉSSIMO ( )

Acha necessário que a empresa efetue mudanças na rede de computadores?	
SIM ( )	NÃO ( )

Acha que a empresa deveria investir mais em segurança?	
SIM ( )	NÃO ( )

Acha que as políticas de segurança prejudicaram os serviços?	
SIM ( )	NÃO ( )

Sobre a importância e a responsabilidade com a segurança da informação:

Como você define:	Muito	Pouco	Médio	Nenhum
O grau de importância você define para a segurança da informação na empresa?				
O quanto você acha que a empresa precisa melhorar em segurança das informações?				
O grau de importância das informações e orientações repassadas sobre a segurança da informação?				
A responsabilidade que todos devem ter para manter a segurança das informações da empresa?				
A reponsabilidade que todos devem ter para manter a segurança das suas próprias informações na empresa?				
A qualidade dos serviços que são prestados referentes segurança da informação?				

Se for do seu interesse, deixe sua opinião sobre as políticas de segurança da empresa, e sugestões de melhorias: