UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

FELIPE SCHLOSER ZARPELON
MATHEUS INOCENCIO DOS SANTOS

# IMPLEMENTAÇÃO DE FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO EM PEQUENAS EMPRESAS

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2018

FELIPE SCHLOSER ZARPELON
MATHEUS INOCENCIO DOS SANTOS

# IMPLEMENTAÇÃO DE FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO EM PEQUENAS EMPRESAS

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica – DAELN – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

**Orientador**: Prof. M.Sc. Christian C. S. Mendes

CURITIBA
2018

**TERMO DE APROVAÇÃO**

FELIPE SCHLOSER ZARPELON
MATHEUS INOCENCIO DOS SANTOS

**IMPLEMENTAÇÃO DE FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO EM PEQUENAS EMPRESAS**

Este trabalho de conclusão de curso foi apresentado no dia 23 de novembro de 2018, como requisito parcial para obtenção do título de **Tecnólogo em Sistemas de Telecomunicações**, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Profa. Dra. Tânia Lucia Monteiro
Coordenadora de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. M.Sc. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

**BANCA EXAMINADORA**

_____
Prof. M.Sc. Fabiano S. de Carvalho
DAINF - UTFPR

_____
Prof. Dr. Luis Carlos Vieira
DAELN - UTFPR

_____
Prof. M.Sc. Christian C. S. Mendes
Orientador – UTFPR

- O termo de aprovação assinado encontra-se na Coordenação do curso.

## RESUMO

ZARPELON, Felipe Schloser. DOS SANTOS, Matheus Inocencio. **Implementação de ferramentas de segurança da informação em pequenas empresas**. 2018. 74 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

O presente trabalho de conclusão de curso apresenta um estudo de caso que aborda a segurança da informação em pequenas empresas. Mapeia os principais serviços de Tecnologia da Informação utilizados e identifica as falhas presentes no ambiente de rede, bem como falhas físicas que podem ser cruciais para um ataque cibernético. Elabora um manual de boas práticas a serem seguidas pelos colaboradores e sugere ferramentas para melhorar a segurança de rede da empresa com base nas normas ABNT ISO/IEC 27001, ABNT ISO/IEC 27002 e ABNT ISO/IEC 27005.



**Palavras-chave:** Gestão de segurança da informação. Prevenção de falhas. *Firewall. Malware.*

## ABSTRACT

ZARPELON, Felipe Schloser. DOS SANTOS, Matheus Inocencio. **Implementation of small business information security tools**. 2018. 74 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The present work of course completion presents a case study that addresses the information security in small companies. It maps the main Information Technology services used and identifies the flaws present in the network environment as well as physical flaws that can be crucial to a cyber attack. Develops a manual of good practices to be followed by employees and suggests tools to improve the company's network security based on ABNT ISO/IEC 27001, ABNT ISO/IEC 27002 and ABNT ISO/IEC 27005 standards.



**Keywords:** Information security management. Preventing failures. Firewall. Malware.

## LISTA DE FIGURAS

## LISTA DE QUADROS

**SUMÁRIO**

# 1. INTRODUÇÃO

## 1.1. DELIMITAÇÃO DO TEMA

Na atualidade, tudo está conectado na rede e, consequentemente, na Internet. Por esse motivo a segurança de redes e segurança dos dados é de extrema importância para manter em sigilo as informações de cada pessoa, empresa, projetos, produtos e toda e qualquer outra informação.

O presente estudo foi feito na empresa Teleinfra Serviços em Teleinformática e Infraestrutura Ltda., a qual possui um servidor com várias aplicações e muitos dados de extrema importância para a organização. Tendo em vista a grande quantidade de dados e a forma como ele é tratado hoje na empresa, os sócios-administradores notaram que se acontecesse algum tipo de problema (perda de dados, *malware,* etc.) eles acabariam por sofrer perda de documentos, projetos e até mesmo dados financeiros da empresa.

Este estudo de caso visa sugerir ferramentas e mecanismos para a segurança de informações de pequenas empresas, que não possuem alta verba disponível para investir na segurança, e acabam por se tornar alvos visados. Com a sugestão destas ferramentas, os autores esperam poder implantar as soluções e obter um resultado satisfatório em relação à segurança da rede da organização escolhida.

## 1.2. OBJETIVOS

### 1.2.1. Objetivo Geral

Demonstrar formas de prevenção de falhas, ataques, perda de dados, entre outros, e sugerir soluções para os problemas de segurança da informação em empresas, com o menor investimento possível.

### 1.2.2. Objetivos Específicos

- Mapear os serviços de tecnologia e informações existentes na empresa;
- Identificar as falhas e os principais pontos a serem melhorados, com base na norma ABNT ISO/IEC 27005;
- Sugerir melhorias no sistema da empresa, baseado nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002;
- Efetuar testes de ferramentas e softwares de segurança e monitoramento.
- Elaborar um manual de boas práticas relacionada à segurança de informação, para empresas, baseado nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002.

## **1.3.** JUSTIFICATIVA

Atualmente muitas empresas armazenam seus dados e aplicações em servidores, estando eles na própria empresa ou fora dela. Organizações maiores destinam verbas pesadas para o setor de Tecnologia da Informação, para que os responsáveis implantem ferramentas que minimizem ou até mesmo acabem com a possibilidade da empresa ser invadida, porém, mesmo com todo este investimento, elas acabam por ser fraudadas. Em pequenas empresas, este investimento é quase nulo, e muitas delas, ao sofrerem um ataque, podem até fechar as portas, devido ao grande impacto que uma perda de dados pode acarretar em seus negócios.

# 2. REVISÃO DE LITERATURA

A revisão de literatura descrita a seguir será baseada em artigos, normas, revistas científicas, trabalhos acadêmicos e livros relacionados à segurança de informações e segurança de redes empresariais, desde a segurança física até conceitos sobre informação e comunicação, softwares e ferramentas diversas.

## 2.1. SEGURANÇA DA INFORMAÇÃO

A área de Tecnologia da Informação (TI) faz parte de praticamente toda organização na atualidade, mas nem toda empresa será capaz de montar e manter uma equipe para suprir as necessidades de processos, inclusive na área de segurança. (BATISTA, 2015).

O objetivo principal da segurança da informação é garantir a segurança dos dados, partindo do princípio da tríade de segurança, que engloba a confidencialidade, integridade e disponibilidade dos dados.

> A informação passou a ser um ativo cada vez mais valorizado pelas organizações e governos, onde prevalece o uso da tecnologia da informação fazendo com que os dados e o conhecimento sejam disseminados numa rapidez jamais imaginada, sendo assim indispensável para as empresas o investimento em Segurança da Informação. Manter a esta significa preservar sua confiabilidade, integridade e disponibilidade. (SARAIVA, 2012).

Hoje em dia as informações das organizações são colocadas à mercê de muitas ameaças, roubos de informações, vazamentos e outros problemas. Pensando nisso, a Política de Segurança de informação serve como base para o estabelecimento de normas e procedimentos que garantam a segurança de tais informações, e também ajuda a especificar as responsabilidades inerentes a segurança dentro da empresa. (SANTOS, 2010).

> Normalmente a implementação de uma política de segurança é considerada a parte mais complexa. Sua criação envolve muitas variáveis, como: ambiente de rede, organização, tecnologia e pessoas. Contudo, a execução da implementação é avaliada como a maior dificuldade desse processo de política de segurança, pois leva um pouco de tempo para que as pessoas entendam e cumpram as designações. (SARAIVA, 2012).

Falar em segurança de redes é quase que sinônimo de falar em *Firewalls*, como

diz o livro Análise de Tráfego em Redes TCP/IP “Firewall é todo o esforço físico e lógico utilizado para prover segurança a uma rede de computadores” (MOTA FILHO, 2013). *Firewalls* são sistemas (*softwares*, ferramentas) básicos utilizados na segurança de redes e informações corporativas, portanto, implementado por todos os profissionais da área de tecnologia, porém não pode ser o único mecanismo a ser usado e explorado.

## 2.2. CONCEITOS GERAIS SOBRE SEGURANÇA

Como em toda a área de TI, existem conceitos básicos sobre tecnologia e segurança, que são de grande ajuda para o entendimento e desenvolvimento do estudo.

Dentre os conceitos, podemos separar os que estão relacionados a equipamentos, outros que são relacionados a *softwares*, e ainda outros que remetem às boas práticas que devem ser utilizadas, seguidas, implementadas.

Todas as empresas, nos tempos atuais, estão sujeitas a ataques e, consequentemente, a perda de dados primordiais para sua sobrevivência no mercado. Portanto, as corporações devem estar em constante preocupação e atualização a respeito de sua segurança, incluindo o ambiente físico, os funcionários e também dos dados e sistemas. Deve-se identificar e analisar todas as vulnerabilidades contidas no ambiente local físico e lógico, a fim de sanar todas as ameaças e ataques.

Ao pensar em segurança da empresa no quesito das informações e da rede, os gestores e diretores, no geral, não tinham uma visão de que deve ser bem definida e confiável a segurança dos dados, somente um *firewall* resolvia. O avanço tecnológico e as notícias sobre ataques cibernéticos atuais, como os ataques de roubo de dados e indisponibilidade de serviços mostraram que todos devem se atentar ainda mais às questões relacionadas à segurança. Entretanto, necessita investimento de tempo e dinheiro para a implementação de ferramentas e boas práticas de segurança, pois não é da noite para o dia que se consegue estabelecer um nível aceitável e estável, pois tudo deve ser estudado, colocado em ambiente de teste para homologação e, após isso, ativar em ambiente de produção. Além disso, o *hardware* e os *softwares* que são utilizados para manter o ambiente seguro, em sua maioria, não são de baixo

investimento, fazendo com que organizações de pequeno e até médio porte não se atentem para essa área.

Também podemos notar que o avanço tecnológico é constante, com muitas mudanças e atualizações, novas técnicas, tecnologias e metodologias para efetivamente fazer acontecer. Então, sejam avanços e pesquisas da iniciativa privada ou até de iniciativa pública, e também os famosos Códigos Abertos (*Open Source*) onde temos a pesquisa e colaboração de vários usuários em fóruns e ambientes de desenvolvimento, tudo está ligado para a melhoria contínua dos sistemas e, consequentemente, da segurança destes sistemas e informações.

## 2.3. NORMAS E PROCEDIMENTOS

No campo de segurança de informação, existe a norma ABNT NBR ISO/IEC 27001. Ela tem como principal objetivo especificar requisitos para o estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI). (ABNT, 2006).

A norma NBR ISO/IEC 27002 estabelece diretrizes e princípios gerais para iniciar, manter e melhorar a gestão de segurança da informação em organizações, além de servir como um guia para desenvolver procedimentos de segurança da informação e práticas eficientes de gestão de segurança. (ABNT, 2005).

A NBR ISO/IEC 27002 define 3 (três) elementos essenciais para o processo de gestão de riscos:

- Ativo: qualquer coisa que tenha valor para a empresa;
- Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano a um sistema ou organização;
- Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. (ABNT, 2005).

Segundo a norma NBR ISO/IEC 27005, uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da empresa em relação aos requisitos de segurança da informação. Convém que esta abordagem seja adequada ao ambiente da empresa e que os esforços de segurança

lidem com os riscos de maneira eficaz e em tempo certo. Ainda de acordo com a norma, é importante definir o entendimento de riscos de segurança da informação:

> Riscos de segurança da informação: Possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. É medido em função da combinação da probabilidade de um evento e de sua consequência. (ABNT, 2011).

Para a norma NBR ISO/IEC 27005 a gestão de segurança da informação deve contribuir para:

- Identificação de riscos;
- Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los. (ABNT, 2011).

### 2.3.1. Processo de Gestão de Riscos

De acordo com a NBR ISO/IEC 27005, o processo de gestão de riscos de segurança da informação consiste na definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, continuação do risco e do monitoramento e análise crítica de riscos. (ABNT, 2011).

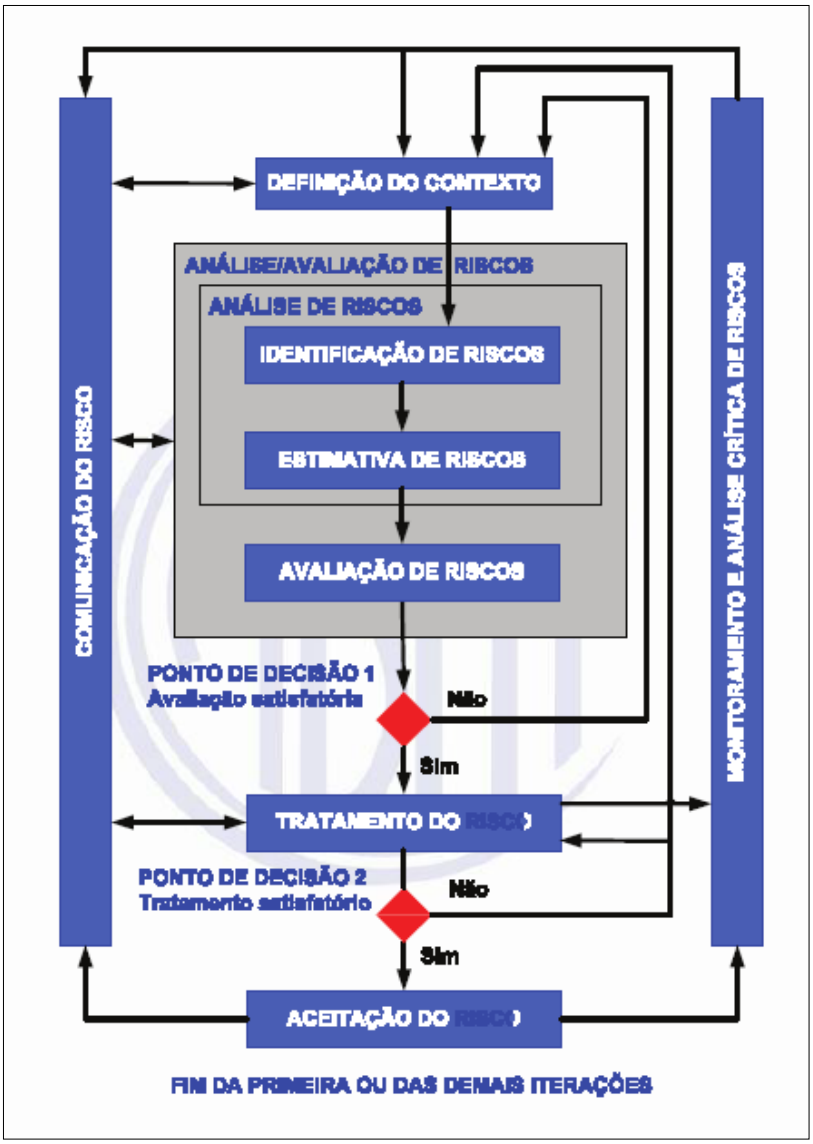



**Figura 1 - Processo de gestão de riscos de segurança da informação**
**Fonte: NBR ISO/IEC 27005/2011**

## 3. METODOLOGIA

De acordo com Konzen (2013), as atividade das organizações estão frequentemente a mercê de riscos, portanto, as empresas devem gerenciar os mesmos identificando-os e analisando-os, para um futuro tratamento do risco. Ainda segundo Konzen, na literatura, encontram-se metodologias para a identificação e análise dos riscos, mas a maioria delas não se relaciona com a norma NBR ISO/IEC 27005/2011 e isso faz com que as organizações acabem escolhendo um processo ineficiente.

Neste sentido o presente estudo trata-se de um levantamento empírico, usando as metodologias contidas na norma ABNT NBR ISO/IEC 27005/2011 para estabelecer a gestão de riscos de segurança da informação da organização estudada.

Para tal estudo, inicialmente foi mapeada toda a estrutura de rede da empresa Teleinfra Serviços em Teleinformática e Infraestrutura Ltda., incluindo seus principais serviços, ativos de rede, segurança, e até a infraestrutura do local onde se encontram os equipamentos. Foi realizada também uma análise das informações, a qual foi importante, para determinar a importância, e como elas serão tratadas pelos dispositivos de segurança que foram propostos pelo estudo.

Em seguida, analisaram-se as falhas existentes na rede atual, a partir delas, foi elaborado um plano de ação para corrigi-las, por meio das soluções sugeridas pelo presente estudo.

Realizadas as etapas anteriores, foram feitos alguns testes, para verificar a atual condição de defesa dos serviços da organização. Estes testes serviram de base para detectar as vulnerabilidades atuais e ajudar a planejar a ferramenta de defesa adequada.

A partir da conclusão destas etapas, os dados coletados nas mesmas foram analisados pela equipe, juntamente com o professor orientador, e foram oferecidas diversas soluções aos diretores da empresa, os quais analisaram e optaram pela opção que mais agradou tanto financeiramente, quanto em questão da confidencialidade de seus dados. Estas ferramentas já existem no mercado de tecnologia, porém ainda não utilizadas pela empresa envolvida neste estudo. Escolhidas as ferramentas, iniciou-se o processo de implantação das mesmas, que foram monitoradas pelo orientador,

juntamente com a equipe do presente estudo.

Após a realização da implementação das ferramentas identificadas por meio do levantamento inicial, foram replicados os mesmos testes efetuados no início do estudo, para compararmos os dados e cruzá-los para mensurar a melhora de segurança dos dados da organização. Após os testes, os resultados foram apresentados à diretoria da empresa para mostrar a eficácia das ferramentas propostas pelos autores do estudo em conjunto com o orientador.

## 3.1. A EMPRESA

A empresa Teleinfra Serviços em Teleinformática e Infraestrutura foi fundada em 01 de maio de 1996, atua na área de Telecomunicações, prestando serviços de Infraestrutura, Instalação e Ativação de Sistemas Via Satélite e Rádio Acesso, dispondo de mão de obra qualificada e equipamentos da mais alta tecnologia, em todo território nacional. Seus principais serviços são:

- Site Survey para Implantação de Sistemas de Telecomunicações;
- Projeto de Instalação de Sistema Satélite e Terrestre;
- Execução de Infraestrutura para Implantação de Sistemas Satélite e Terrestre;
- Instalação de Sistemas Satélites (TV/RO, VSAT e SCPC);
- Instalação de Sistemas de Rádio Acesso;
- Teste de Propagação e Prospecção;
- Dimensionamento de Enlaces;
- Instalação de Modem Óptico e GPRS;
- Instalação de Wireless e VOIP;
- Instalação de Router CISCO, HP e Huawei;
- Comissionamento (Sistema VSAT);
- Teste Mandatório (Sistema SCPC);
- Manutenção Preventiva;
- Manutenção Corretiva (TV/RO, VSAT, SCPC e RÁDIO);

### 3.1.1. Principais Clientes

EMBRATEL (Curitiba/PR) – desde ano 2000
Implantação Sistema Rádio Acesso, Satélite e Ativação de Dados:
Quantidade de instalações (Satélite): Aproximadamente 250 estações
Quantidade de instalações (Rádio Acesso): aproximadamente 200 enlaces
Localidades: PR, SC e RS.

ALCATEL TELECOMUNICAÇÕES (Rio de Janeiro/RJ) – desde ano 1998
Implantação Sistema Satélite
Quantidade de instalações (Satélite): aproximadamente 100 estações
Localidades: diversas (nível Brasil)

BT BRASIL LTDA. (Hortolândia/SP) – desde ano 1996
Implantação Sistema Rádio e Satélite
Quantidade de instalações (Satélite): Aproximadamente 1.200 estações
Localidades: diversas (Nível Brasil)

DEPV (Rio de Janeiro/RJ) – desde ano 2000
Manutenção Sistema Satélite
Quantidade de Manutenções (Satélite): 50 estações
Localidades: diversas (nível Brasil)

FTC – FERROVIA TEREZA CRISTINA (Tubarão/SC) – desde ano 2003
Implantação Sistema Rádio Acesso
Quantidade de instalações (Rádio Acesso): 10 enlaces

RAYTHEON BRASIL (Manaus/AM) – desde ano 2003
Manutenção Sistema Satélite
Quantidade de Manutenções (Satélite): 35 estações

Localidades: diversas (nível Brasil)

BBN ENGENHARIA (Curitiba/PR) – desde ano 2002
Testes de prospecção
Quantidade: aproximadamente 700 testes
Localidades: RJ, SP e Região Sul.

ITAUTEC (São Paulo/SP) – desde ano 2004
Implantação Sistema Satélite
Localidades: PR e SC

GILAT DO BRASIL (Rio de Janeiro/RJ) – desde ano 2009
Implantação Sistema Satélite
Localidades: diversas (nível Brasil)

### 3.1.2. Missão

Ser um diferencial entre as melhores empresas na Prestação de Serviços de Telecomunicações, fornecer mão de obra qualificada, superar as expectativas de nossos clientes, manter um ambiente agradável e trabalhar com comprometimento, humildade, transparência e seriedade.

### 3.1.3. Visão

Ser uma empresa de excelência na prestação de serviços, acompanhando as novas tecnologias e proporcionando maior confiabilidade, transparência e competência.

## 3.2. MAPEAMENTO DAS PRINCIPAIS AMEAÇAS E VULNERABILIDADES

Em um primeiro momento, foram mapeados os principais ativos da empresa

quando se trata de segurança da informação. Para cada um deles, tomando como base a norma NBR ISO/IEC 27005 e a norma NBR ISO/IEC 27001, identificou-se a ameaça a que este ativo esta sujeito a ter e logo após, as vulnerabilidades inerentes a estas ameaças, como mostra o Quadro 1:

**Quadro 1 - Análise das Ameaças e Vulnerabilidades existentes**

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Sala de Equipamentos (CPD) | Incêndio | 1 - Climatização não é adequada;<br>2- Solução para combate a Incêndios ineficaz;<br>3- Falta de Monitoramento de Temperatura. |
| | Acesso não autorizado | 1 - Ausência de restrição física (tranca ou biometria);<br>2 - Ausência de controle de Presença no Local;<br>3 - Ausência de monitoramento Físico;<br>4- Acesso irrestrito aos ativos. |
| | Invasão | 1 - Ausência de monitoramento de acesso remoto;<br>2 – Ausência de controle através de ferramentas; |
| | | 3 - Ausência de restrição de acesso através de políticas e ausência de ponto de estrangulamento;<br>4- Ausência de Antivírus; |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Sala de Equipamentos (CPD) | Invasão | 5- Ausência de monitoramento Físico;<br>6- *Softwares* desatualizados/obsoletos;<br>7- Má configuração dos equipamentos;<br>8- Atribuição errônea de direitos de acesso. |
| | Falha dos equipamentos | 1 - Falta de *Hardware* backup;<br>2 - Falta de monitoramento do ambiente;<br>3 - Falta de Manutenção Preventiva;<br>4- Inexistência de um plano de continuidade;<br>5- *Softwares* desatualizados/obsoletos;<br>6- Má Configuração dos equipamentos;<br>7- Equipamentos sensíveis à variação de tensão. |
| | Falta de energia | 1 - *No-break* com problemas;<br>2 - Falta de Monitoramento de carga;<br>3 - Ausência de gerador;<br>4 - Equipamentos sensíveis à variação de tensão. |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Sala de Equipamentos (CPD) | Comprometimento dos dados | 1 - Ausência de *Backup*;<br>2 - Falta de política de *backup*;<br>3 - Ausência de backup externo.<br>4 - Sem solução de *proxy* para controle habilitada;<br>5 - Armazenamento não protegido;<br>6 - Documentação de procedimentos operacionais inexistente;<br>7- Falta de monitoramento do armazenamento;<br>8- Serviços desnecessários que permanecem habilitados;<br>9- Trabalho não supervisionado da equipe de limpeza. |
| | *Malwares* | 1 - Ausência de Antivirus;<br>2 - Ausência de monitoramento;<br>3 - Ausência de Capacitação aos colaboradores;<br>4 - Sistema Operacional desatualizado; |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Sala de Equipamentos (CPD) | *Malwares* | 5 - Sem solução de p*roxy* para controle habilitada;<br>6- *Softwares* desatualizados/obsoletos;<br>7- Má configuração dos equipamentos. |
| | Vazamento de informações | 1 - Ausência de Antivirus;<br>2 - Ausência de monitoramento;<br>3 - Ausência de Capacitação aos colaboradores;<br>4 - Ausência de solução de DLP (*Data Loss Protection*);<br>5 - Armazenamento não protegido;<br>6 - *Softwares* desatualizados/obsoletos;<br>7- Atribuição errônea de direitos de acesso. |
| | Indisponibilidade do serviço | 1 - Ausência de enlace redundante de internet;<br>2 - Sem equipamentos redundantes;<br>3 - Sem monitoramento do link de Internet;<br>4- Má configuração dos equipamentos. |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Rede Interna | Vazamanto de informações | 1 - Ausência de Antivirus;<br>2 - Ausência de monitoramento;<br>3 - Ausência de Capacitação aos colaboradores;<br>4 - Ausência de solução de DLP (*Data Loss Protection*);<br>5 - Armazenamento não protegido;<br>6- *Softwares* desatualizados/obsoletos;<br>7- Atribuição errônea de direitos de acesso. |
| | Invasão | 1 - Ausência de monitoramento de acesso remoto;<br>2 - Controle através de ferramentas;<br>3 - Ausência de restrição de acesso através de políticas e ausência de ponto de estrangulamento;<br>4 - Ausência de Antivírus;<br>5 - Ausência de monitoramento Físico;<br>6 - *Softwares* desatualizados/obsoletos;<br>7 - Má configuração dos equipamentos; |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Rede Interna | Invasão | 8 - Atribuição errônea de direitos de acesso. |
| | Espionagem | 1 - Arquitetura da rede desconhecida;<br>2 - Troca de senhas entre colaboradores;<br>3 - Sem restrição de acesso pelos pontos de rede. |
| | Comprometimento dos dados | 1 - Ausência de *Backup;*<br>2 - Falta de política de *backup*;<br>3 - Ausência de *backup* externo;<br>4 - Sem solução de *proxy* para controle habilitada;<br>5 - Armazenamento não protegido;<br>6 - Documentação de procedimentos operacionais inexistente;<br>7 - Falta de monitoramento do armazenamento. |
| | *Malwares* | 1 - Ausência de Antivirus;<br>2 - Ausência de monitoramento;<br>3 - Ausência de Capacitação aos colaboradores;<br>4 - Sistema Operacional desatualizado; |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Rede Interna | *Malwares* | 5 - Sem solução de proxy para controle habilitada<br>6 - Softwares desatualizados/obsoletos<br>7- Má configuração dos equipamentos |
| Estações de Trabalho/Colaboradores | Vazamento de informações | 1 - Ausência de Antivirus<br>2 - Ausência de monitoramento<br>3 - Ausência de Capacitação aos colaboradores<br>4 - Ausência de solução de DLP (Data Loss Protection)<br>5 - Armazenamento não protegido<br>6 - Softwares desatualizados/obsoletos<br>7- Atribuição errônea de direitos de acesso<br>8 - Não execução de logout |
| | Invasão | 1 - Ausência de monitoramento de acesso remoto<br>2 – Ausência de controle através de ferramentas<br>3 - Ausência de restrição de acesso através de políticas e ausência de ponto de estrangulamento |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Estações de Trabalho/Colaboradores | Invasão | 4 - Ausência de Antivírus<br>5 - Ausência de monitoramento Físico<br>6 - Softwares desatualizados/obsoletos<br>7 - Má configuração dos equipamentos<br>8 - Atribuição errônea de direitos de acesso |
| | Espionagem | 1 - Arquitetura da rede desconhecida<br>2 - Troca de senhas entre colaboradores<br>3 - Sem restrição de acesso pelos pontos de rede<br>4 - Engenharia Social |
| | *Malwares* | 1 - Ausência de Antivirus<br>2 - Ausência de monitoramento<br>3 - Ausência de Capacitação aos colaboradores<br>4 - Sistema Operacional desatualizado<br>7- Má configuração dos equipamentos |

| Ativo | Ameaça | Vulnerabilidades |
|---|---|---|
| Estações de Trabalho/Colaboradores | Erro durante ao uso | 1- Uso incorreto dos equipamentos<br>2 - Não existe treinamento/política de segurança da informação<br>3 - Falta de conscientização em segurança |

**Fonte: Autoria Própria.**

## 3.3. AVALIAÇÃO DA PROBABILIDADE DAS VULNERABILIDADES E AMEAÇAS

Para a definição do valor de cada uma das vulnerabilidades, foi adotado o Quadro 2, o qual foi confeccionado levando em consideração a relevância do ativo constante no Quadro 1, em caso da exploração das vulnerabilidades:

**Quadro 2 – Avaliação da probabilidade dos incidentes**

| Vulnerabilidade | Facilidade da exploração | Ameaça | Probabilidade |
|---|---|---|---|
| Climatização não é adequada | Médio | Incêndio | Alto |
| Solução para combate a incêndio é ineficaz | Médio | | |
| Falta de monitoramento de temperatura | Médio | | |
| Ausência de restrição física (tranca ou biometria) | Médio | Acesso Não Autorizado | Alto |
| Ausência de controle de Presença no Local | Médio | | |
| Ausência de monitoramento Físico | Alto | | |
| Acesso irrestrito aos ativos | Alto | | |
| Ausência de monitoramento de | Alto | Invasão | Alto |

| | | | |
|---|---|---|---|
| acesso remoto | | | |
| Ausência de controle através de ferramentas | Médio | | |
| Ausência de restrição de acesso através de políticas e ausência de ponto de estrangulamento | Médio | | |
| Ausência de Antivírus | Alto | | |
| Ausência de monitoramento Físico | Alto | | |
| *Softwares* desatualizados/obsoletos | Médio | | |
| Má configuração dos equipamentos | Alto | | |
| Atribuição errônea de direitos de acesso | Alto | | |
| Falta de *Hardware backup* | Alto | Falha dos Equipamentos | Alto |
| Falta de monitoramento do ambiente | Médio | | |
| Falta de Manutenção Preventiva | Médio | | |
| Inexistência de um plano de continuidade | Médio | | |
| *Softwares* desatualizados/obsoletos | Médio | | |
| Má Configuração dos equipamentos | Alto | | |
| Equipamentos sensíveis à variação de tensão | Médio | | |
| *No-break* com problemas | Médio | Falta de energia | Alto |
| Falta de Monitoramento de carga | Médio | | |
| Ausência de gerador | Médio | | |
| Equipamentos | Médio | | |

| | | | |
|---|---|---|---|
| sensíveis à variação de tensão | | | |
| Ausência de *Backup* | Alto | Comprometimento dos dados | Alto |
| Falta de política de *backup* | Alto | | |
| Ausência de *backup* externo | Médio | | |
| Sem solução de *proxy* para controle habilitada | Alto | | |
| Armazenamento não protegido | Médio | | |
| Documentação de procedimentos operacionais inexistente | Médio | | |
| Falta de monitoramento do armazenamento | Médio | | |
| Serviços desnecessários que permanecem habilitados | Baixo | | |
| Trabalho não supervisionado da equipe de limpeza | Baixo | | |
| Ausência de Antivírus | Alto | Malwares | Alto |
| Ausência de monitoramento | Médio | | |
| Ausência de Capacitação aos colaboradores | Médio | | |
| Sistema Operacional desatualizado | Médio | | |
| Sem solução de *proxy* para controle habilitada | Alto | | |
| *Softwares* desatualizados/obsoletos | Médio | | |
| Má configuração dos equipamentos | Alto | | |
| Ausência de Antivírus | Alto | Vazamento de informações | Alto |
| Ausência de | Médio | | |

| | | | |
|---|---|---|---|
| monitoramento | | | |
| Ausência de Capacitação aos colaboradores | Médio | | |
| Ausência de solução de DLP (*Data Loss Protection*) | Médio | | |
| Armazenamento não protegido | Médio | | |
| *Softwares* desatualizados/obsoletos | Médio | | |
| Atribuição errônea de direitos de acesso | Alto | | |
| Não execução de *logout* | Médio | | |
| Sem enlace redundante de internet | Médio | Indisponibilidade do serviço | Alto |
| Sem equipamentos redundantes | Médio | | |
| Sem monitoramento do *enlace* de Internet | Médio | | |
| Má configuração dos equipamentos | Alto | | |
| Arquitetura da rede desconhecida | Baixo | Espionagem | Alto |
| Troca de senhas entre colaboradores | Alto | | |
| Sem restrição de acesso pelos pontos de rede | Alto | | |
| Engenharia Social | Alto | | |
| Uso incorreto dos equipamentos | Médio | Erro durante ao uso | Médio |
| Não existe treinamento/política de segurança da informação | Médio | | |
| Falta de conscientização em segurança | Médio | | |

**Fonte: Autoria própria**

O impacto foi mensurado a partir do valor do ativo para a empresa, conforme Quadro 3:

**Quadro 3 - Valores de Impacto para os ativos**

| Nível | Valor do Ativo para a empresa |
|---|---|
| Baixo | Ativos de baixo valor e fácil recuperação |
| Médio | Ativos de valor médio |
| Alto | Ativos de grande valor e de difícil recuperação |

**Fonte: Autoria própria**

## 3.4. ANÁLISE DE RISCO

A partir dos dados levantados, com base na norma NBR 27005/2011 foram estabelecidos níveis e valores para ameaça, vulnerabilidade e impacto, conforme mostrado no Quadro 4:

**Quadro 4 - Valores estabelecidos para ameaça, vulnerabilidade e impacto**

| Níveis | Alto | Médio | Baixo |
|---|---|---|---|
| Valores | 3 | 2 | 1 |

**Fonte: Autoria própria**

O nível do risco é feito por meio da multiplicação dos valores estabelecidos no Quadro 3 para vulnerabilidade, ameaça e impacto. Realizando esta operação chegou-se no Quadro 5:

**Quadro 5 – Mensuração do risco**

| Ameaça | | Baixa | | | Média | | | Alta | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Vulnerabilidade | | Baixa | Média | Alta | Baixa | Média | Alta | Baixa | Média | Alta |
| Impacto | Baixo | 1 | 2 | 3 | 2 | 4 | 6 | 3 | 6 | 9 |
| | Médio | 2 | 4 | 6 | 4 | 8 | 12 | 6 | 12 | 18 |
| | Alto | 3 | 6 | 9 | 6 | 12 | 18 | 9 | 18 | 27 |

**Fonte: Autoria própria**

Os níveis de risco podem ser separados conforme Quadro 6:

**Quadro 6 - Níveis de risco**

| | |
|---|---|
| Risco Baixo | De 1 a 6 |
| Risco Médio | De 7 a 12 |
| Risco Alto | De 13 a 27 |

**Fonte: Autoria própria**

Realizando o cruzamento das informações, chegou-se aos valores do Quadro 7:

**Quadro 7 - Análise de Risco**

| Vulnerabilidade | Ameaça | Impacto - Risco |
|---|---|---|
| Climatização não é adequada | Incêndio | Médio - 12 |
| Solução para combate à incêndio é ineficaz | | Médio - 12 |
| Falta de Monitoramento de temperatura | | Baixo - 6 |
| Ausência restrição física (tranca ou biometria) | Acesso Não Autorizado | Médio - 12 |
| Ausência de controle de Presença no Local | | Médio - 12 |
| Ausência de monitoramento Físico | | Médio - 18 |
| Acesso irrestrito aos ativos | | Alto - 27 |
| Ausência de monitoramento de acesso remoto | Invasão | Alto - 27 |
| Ausência de controle através de ferramentas | | Médio - 12 |
| Ausência de restrição de acesso através de políticas e ausência de ponto de estrangulamento | | Médio - 12 |
| Ausência de Antivírus | | Alto - 27 |
| Ausência de monitoramento Físico | | Médio - 18 |
| *Softwares* desatualizados/obsoletos | | Alto - 18 |
| Má configuração dos equipamentos | | Médio - 18 |
| Atribuição errônea de direitos de acesso | | Alto - 27 |
| Falta de *Hardware backup* | Falha dos Equipamentos | Médio - 18 |
| Falta de monitoramento do ambiente | | Baixo - 6 |
| Falta de Manutenção Preventiva | | Médio - 12 |
| Inexistência de um plano de continuidade | | Alto - 18 |
| *Softwares* desatualizados/obsoletos | | Alto - 18 |
| Má Configuração dos equipamentos | | Médio - 18 |
| Equipamentos sensíveis à variação de tensão | | Alto - 18 |
| *No-break* com problemas | Falta de energia | Alto - 18 |
| Falta de Monitoramento de carga | | Médio - 12 |
| Ausência de gerador | | Alto - 18 |
| Equipamentos sensíveis à variação de tensão | | Alto - 18 |
| Ausência de *Backup* | Comprometimento dos dados | Alto - 27 |
| Falta de política de *backup* | | Alto - 27 |
| Ausência de *backup* externo | | Alto - 18 |
| Sem solução de *proxy* para controle habilitada | | Alto - 27 |
| Armazenamento não protegido | | Alto - 18 |
| Documentação de procedimentos operacionais inexistente | | Médio - 12 |
| Falta de monitoramento do armazenamento | | Médio - 12 |
| Serviços desnecessários que permanecem habilitados | | Médio - 6 |
| Trabalho não supervisionado da equipe de | | Baixo - 3 |

| | | |
|---|---|---|
| limpeza | | |
| Ausência de Antivírus | *Malwares* | Alto - 27 |
| Ausência de monitoramento | | Médio - 12 |
| Ausência de Capacitação aos colaboradores | | Médio - 12 |
| Sistema Operacional desatualizado | | Alto - 18 |
| Sem solução de *proxy* para controle habilitada | | Alto - 27 |
| *Softwares* desatualizados/obsoletos | | Alto - 18 |
| Má configuração dos equipamentos | | Médio - 18 |
| Ausência de Antivírus | Vazamento de informações | Alto - 27 |
| Ausência de monitoramento | | Médio - 12 |
| Ausência de Capacitação aos colaboradores | | Médio - 12 |
| Ausência de solução de DLP (*Data Loss Protection*) | | Médio - 12 |
| Armazenamento não protegido | | Alto - 18 |
| Softwares desatualizados/obsoletos | | Alto - 18 |
| Atribuição errônea de direitos de acesso | | Alto - 27 |
| Não execução de *logout* | | Alto - 18 |
| Sem enlace redundante de internet | Indisponibilidade do serviço | Alto - 18 |
| Sem equipamentos redundantes | | Médio - 12 |
| Sem monitoramento do *enlace* de Internet | | Médio - 12 |
| Má configuração dos equipamentos | | Médio - 18 |
| Arquitetura da rede desconhecida | Espionagem | Médio - 3 |
| Troca de senhas entre colaboradores | | Alto - 27 |
| Sem restrição de acesso pelos pontos de rede | | Médio - 18 |
| Engenharia Social | | Alto - 27 |
| Uso incorreto dos equipamentos | Erro durante ao uso | Médio - 8 |
| Não existe treinamento/política de segurança da informação | | Médio - 8 |
| Falta de conscientização em segurança | | Médio - 8 |

**Fonte: Autoria própria**

## 3.5. SUGESTÕES PROPOSTAS

Analisando as vulnerabilidades, ameaças e principalmente o risco encontrado, baseando-se sempre nas normas, foram sugeridas propostas para minimizar os problemas da empresa em relação à segurança da informação.

A princípio, foram sugeridas propostas para neutralização dos impactos e riscos de valor alto, muitas delas precisam de investimento da empresa. Estas propostas foram estudadas pela comissão diretora da organização e os resultados seguem no

item 3.6.

- Acesso irrestrito aos ativos

Em visita ao ambiente, notou-se que o acesso aos ativos da empresa não possui nenhum tipo de controle de acesso, gerando assim vulnerabilidade. A sugestão para esta vulnerabilidade foi à implantação de trava para a porta da sala de equipamento com leitor de acesso.

- Ausência de monitoramento de acesso remoto

Analisando a rede corporativa da empresa, notou-se que o acesso remoto ao servidor principal não possui nenhum sistema de monitoramento e é feito por meio de qualquer ponto de Internet disponível. Sugeriu-se então a implantação de ferramentas de código aberto (*Open Source)* para monitoramento de ativos e para acesso VPN *(Virtual Private Network)*, a qual fará o acesso remoto até o ambiente empresarial através de “túneis” exclusivos entre o colaborador e a rede da empresa.

- Ausência de Antivírus

Em vários computadores da organização a ausência de um *software* antivírus foi observada, inclusive no servidor de arquivos, que não possui tal ferramenta de proteção contra vírus. Para o tratamento desta vulnerabilidade, foi sugerida a implantação de um antivírus pago que será instalado no servidor e nas máquinas dos usuários, para protegê-los de *malwares* de todos os tipos encontrados na rede mundial de computadores.

- *Softwares* desatualizados/obsoletos e Sistema Operacional desatualizado

Foi constatado que em inúmeras máquinas da rede local da empresa e no próprio servidor que os *softwares* utilizados pelos colaboradores encontravam-se desatualizados. Levando em consideração que a cada atualização são corrigidas várias falhas do próprio programa, viu-se a necessidade de realizar tais tarefas

em todas as máquinas do ambiente corporativo, a fim de reduzir as possíveis falhas nos programas e evitando assim algumas ameaças supracitadas.

- Atribuição errônea de direitos de acesso

Foram encontrados usuários com permissão de acesso total a itens que só poderiam ser visualizados ou alterados por certos setores da empresa. Visando minimizar esta vulnerabilidade, foi sugerido realizar uma revisão no diretório de usuários (*Active Directory)* atribuindo a devida permissão aos colaboradores da organização.

- Inexistência de um plano de continuidade

Se algo acontecer com a rede da empresa, nenhum dos colaboradores está instruído a como proceder, portanto viu-se a necessidade de criar um documento básico de contingência, que contenha os procedimentos básicos em caso de desastres, indicando as possíveis ferramentas ou pessoas para suporte.

- Equipamentos sensíveis à variação de tensão

Muitos equipamentos são sensíveis às alterações de tensão da rede elétrica. Em decorrência disto, falhas podem acontecer em um ambiente que não possui a energia estabilizada ou dentro dos padrões dos fabricantes de equipamentos. Analisando esta possibilidade, foi sugerido o monitoramento dos padrões de tensão da concessionária loca e no-break por meio de um multímetro digital, para verificar se os valores de tensão estão dentro dos limites estabelecidos.

- *No-break* com problemas

Quando ocorre uma queda de energia, espera-se que o *no-break* segure a energia para ao menos encerrar as tarefas do servidor de maneira normal e não brusca. No ambiente estudado, viu-se a necessidade de instalar uma ferramenta

de monitoramento do equipamento.

- Ausência de Gerador

Além do *no-break* outra ferramenta importante no combate à quedas de energia é o Gerador. A empresa não dispõe deste equipamento, portanto foi sugerida a instalação de um motogerador para suprir a energia em caso de queda.

- Ausência de *Back-up* / Falta de política de *back-up*

Uma ferramenta importante para a recuperação de dados é o *back-up* das informações. No ambiente em questão, não havia rotinas de recuperação dos dados estabelecidas. Para a solução desta vulnerabilidade, foi sugerida a implantação de rotinas de *back-up* do próprio sistema operacional do servidor de arquivos. Foi sugerido também uma forma de recuperação dos dados fora das dependências da empresa, esta prática faz-se necessária, pois, em caso de desastre do *back-up* local há outra maneira de recuperar os dados.

- Sem solução de *Proxy* para controle habilitada

Uma ferramenta importante para o controle de acesso a Internet dos colaboradores é o *Proxy.* A empresa não possui tal ferramenta, portanto, foi sugerida a instalação da ferramenta, para controle de acesso a Internet dos usuários, que hoje navegam sem quaisquer restrições.

- Armazenamento não protegido

Como informado anteriormente na vulnerabilidade de ausência de monitoramento, para solução desta vulnerabilidade, foi sugerido à instalação de uma ferramenta que monitore os recursos do servidor e ativos da rede, a fim de monitorar quando o armazenamento do servidor atingir níveis críticos de espaço, ou quando o disco apresentar algum problema.

- Não execução de *logout*

Muitos colaboradores deixam suas mesas com os computadores desprotegidos de senhas de acesso, possibilitando assim que alguém possa tomar o controle do aparelho, instalando algum *malware* e etc. Foi sugerida a implantação do bloqueio de tela dos usuários através de políticas de grupo.

- Ausência de enlace redundante de internet

O enlace redundante de internet é importante em caso de indisponibilidade. Visando sanar esta vulnerabilidade, foi proposta a contratação de outro enlace de internet para contingência do existente.

- Troca de senhas entre colaboradores / Engenharia Social

A troca de senhas entre colaboradores em meios corporativos pode prejudicar e muito a organização. Pessoas com más intenções podem levar ao usuário fornecer dados pessoais, mediante ao uso de persuasão, abusando da ingenuidade das pessoas, e com isto roubar dados vitais da empresa. Para que a vulnerabilidade seja neutralizada, foi proposta a criação de um documento de boas práticas do uso dos ativos da empresa, para conscientizar os usuários quanto ao uso dos equipamentos fornecidos pela empresa.

## 3.6. IMPLEMENTAÇÃO DAS SUGESTÕES

- Acesso irrestrito aos ativos

A proposta apresentada a empresa foi à instalação de uma trava que seria controlada por crachá ou biometria, assim controlando o acesso de pessoal não autorizado à sala de equipamentos. Foi realizado um orçamento do valor do equipamento, que girou em torno de dois mil e oitocentos reais (R$ 2.800,00). Em resposta ao orçamento, a empresa decidiu não implantar tal mecanismo de segurança

fisicia a princípio, devido ao alto investimento que seria necessário para a implantação da mesma.

- Ausência de monitoramento de acesso remoto

Em relação ao acesso remoto, a equipe viu a necessidade de implantar uma ferramenta que oferecesse uma maior segurança ao acesso remoto dos colaboradores ao servidor da empresa. Foi escolhida a ferramenta *OpenVPN*, a qual funcionaria em conjunto com um *firewall* chamado *pfSense* (figura 2), que será usado em substituição ao *firewall* existente, pois o mesmo está obsoleto. Foi feita a instalação do *firewall pfSense*, porém não houve tempo hábil para a implementação da ferramenta *OpenVPN,* visto que foram realizadas outras implantações em paralelo.

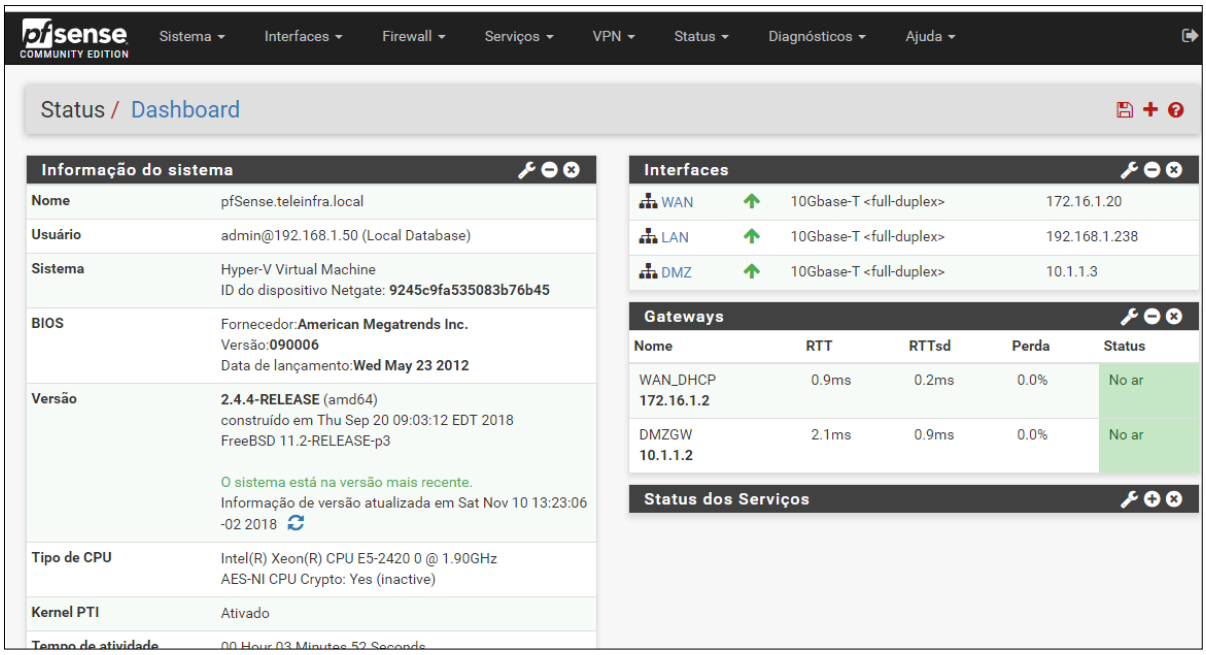



**Figura 2 - *Status/Dashboard pfSense***
**Fonte: Autoria própria**

- Ausência de Antivírus

O antivírus escolhido para a implementação no servidor foi o *Kaspersky Small Office Security 6* (figuras 3 e 4). Diferente dos *softwares* citados anteriormente, ele não é de código aberto (*Open source),* portanto, foi realizado um orçamento e apresentado a empresa, a qual viu a necessidade de obter tal proteção contra vírus e outras ameaças. Para a obtenção do antivírus, a empresa precisou pagar a quantia de

trezentos e noventa e quatro reais (R$ 394,00), pela validade de proteção de um ano, sendo assim, se a organização quiser continuar com a proteção, terá que arcar com os valores novamente quando vencer o prazo. Com a implementação desta ferramenta, espera-se diminuir o risco de invasões e perda de dados em decorrência de vírus provenientes dos acessos a Internet.

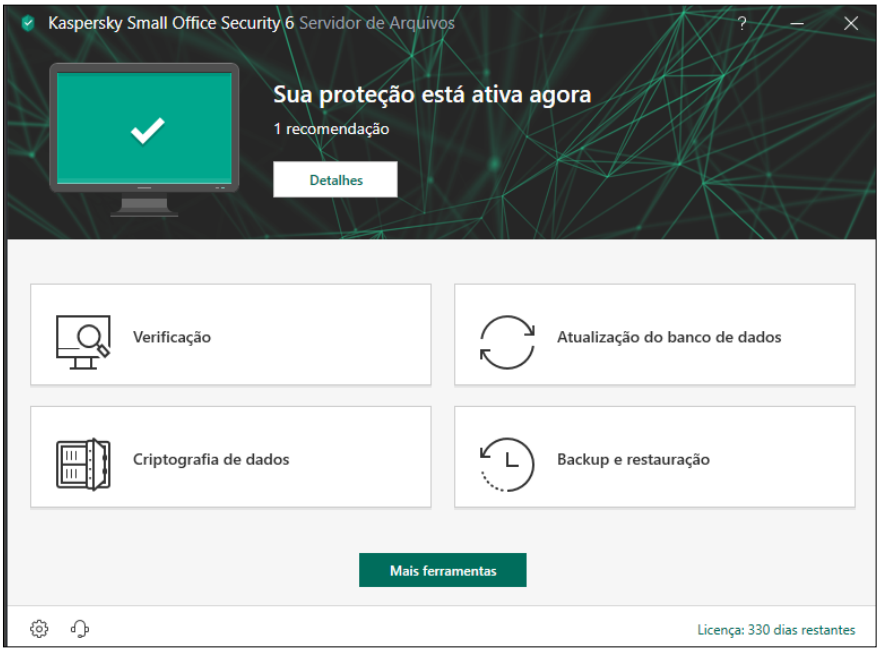



**Figura 3 - Antivírus *Kaspersky Small Office Security 6***
**Fonte: Autoria Própria**

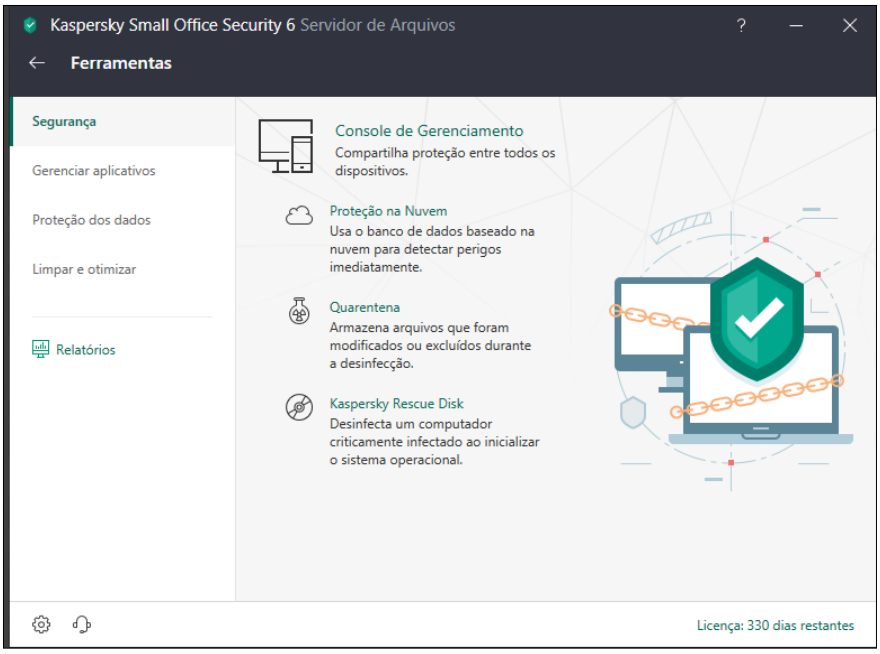



**Figura 4 - Ferramentas do Antivírus**
**Fonte: Autoria própria**

- Softwares desatualizados/obsoletos e Sistema Operacional desatualizado

Um dos problemas encontrados foi a atualização dos softwares instalados nas máquinas dos colaboradores. Para a realização desta tarefa, foram baixadas as atualizações dos sistemas operacionais da máquina de cada um dos colaboradores e em paralelo, todas as atualizações dos softwares que mais são usados por eles, que neste caso, tratam-se dos navegadores de internet (*Google Chrome, Internet Explorer,* etc.). Espera-se que com esta atualização, diminuam-se as probabilidades de um ataque pelas vulnerabilidades dos *softwares*, visto que a cada atualização, são corrigidos vários problemas relacionados a esta questão.

- Atribuição errônea de direitos de acesso

Revisando o *Active Directory* da organização, verificou-se a existência de usuários que não faziam parte do quadro de funcionários da empresa, porém, estavam cadastrados com seu direito de acesso as pastas do servidor da empresa. Haviam também, colaboradores da área técnica com atribuições às pastas da área financeira e comercial. Foi realizada a retirada dos usuários que não fazem parte do quadro da empresa e corrigido os direitos de acesso, destinando as pastas aos devidos setores da

empresa, com isso, espera-se diminuir a possibilidade de vazamento de informações por parte dos colaboradores e perda de documentos importantes para a organização.

- Inexistência de um plano de continuidade

Foi criado um documento básico (vide ANEXO D) de como os colaboradores devem proceder se algo de diferente acontecer com sua máquina de trabalho. O documento mostra a quem o colaborador deve procurar nestes casos, visto que hoje, a empresa não tem um plano de contingência definido, por exemplo, se o usuário sofrer um ataque, ou seu computador parar de funcionar ele não saberia a quem recorrer. Com a implementação deste procedimento, espera-se diminuir a distancia entre o usuário e o gerente da rede, para a resolução de problemas relacionado a tecnologia da informação.

- Equipamentos sensíveis à variação de tensão

Para verificação dos valores de tensão, foram realizadas medidas de tensão em três horários distintos durante o dia, com o auxilio de um multímetro digital. Em um primeiro momento, foi medida a tensão da tomada de energia proveniente da concessionária de energia, da tomada do *No-break* ligado na energia (sem o auxilio das baterias) e do *No-break* desligado da energia (com auxilio das baterias), no período da manhã, tarde e noite. Conforme Quadro 8, verificou-se que os valores (vide ANEXO A) estão dentro dos padrões da concessionária e também dentro dos valores estabelecidos pelas fabricantes dos equipamentos.

**Quadro 8 - Medidas das tensões**

| Medidas das Tensões | | | |
|---|---|---|---|
| | Tomada Concessionária | Tomada *No-break* (ligado na tomada da concessionária) | Tomada No-break (desligado da tomada da concessionária) |
| Manhã | 125,5 V | 125,0 V | 117,7 V |
| Tarde | 124,7 V | 124,3 V | 118,4 V |
| Noite | 124,7 V | 124,9 V | 117,7 V |

**Fonte: Autoria própria**

- *No-break com problemas*

O *No-break* que a empresa dispõe é da marca APC modelo *Smart-UPS 1500*, e para o seu monitoramento utilizou-se o software da própria fabricante, o *PowerChute Business Edition* (figura 5). Com a instalação da ferramenta, pode-se monitorar a vida útil da bateria e os eventos ocorridos (falha na energia, sobretensão na rede elétrica, etc.) e obter relatórios deste tipo de ocorrência. Também foi configurado o envio de *e-mail* do próprio *No-break* para o responsável da rede da empresa, para que ele fique ciente dos eventos ocorridos em tempo real (figuras 6 e 7).

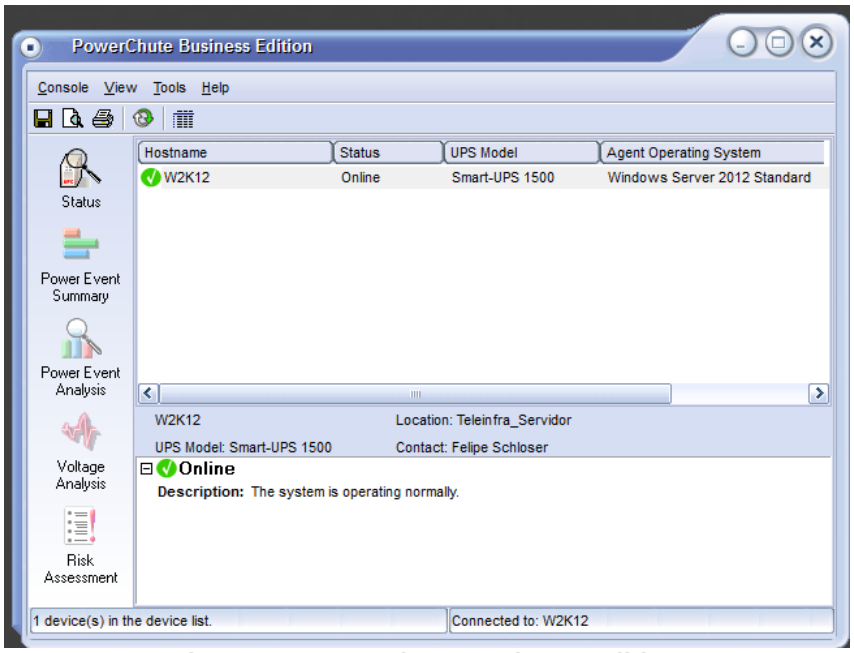



**Figura 5 - *PowerChute Business Edition***
**Fonte: Autoria Própria**

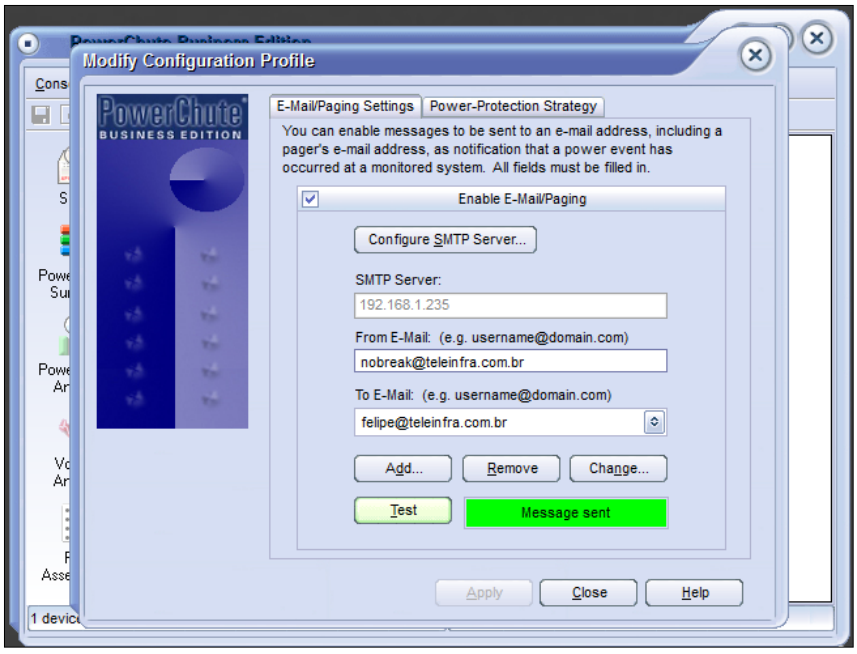



**Figura 6 - Configurações SMTP *PowerChute Business Edition***
**Fonte: Autoria própria**

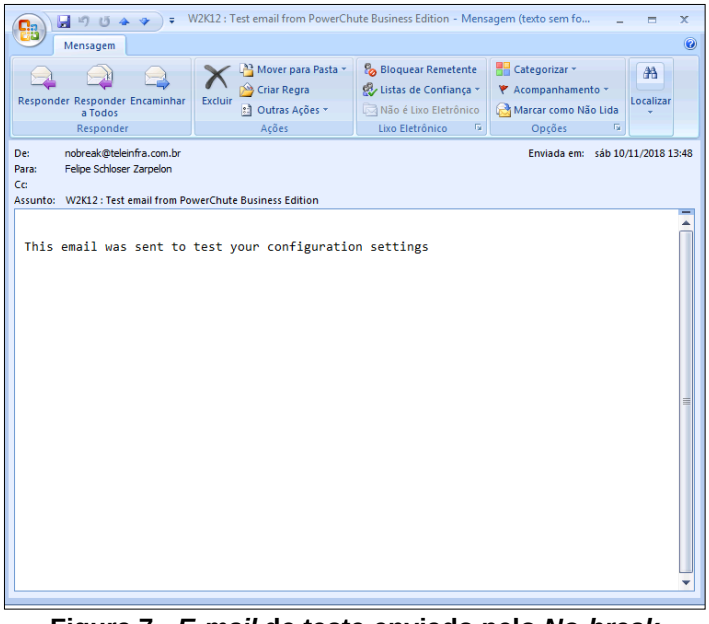



**Figura 7 - *E-mail* de teste enviado pelo *No-break***
**Fonte: Autoria própria**

- Ausência de Gerador

Foi apresentada uma proposta para que a empresa adquiri-se um motogerador da marca CSM modelo GT5500 127Volts Trifásico. Os valores estavam subdivididos, três mil e quinhentos reais (R$ 3.500,00) para obtenção do equipamento e dois mil e quinhentos reais (R$ 2.500,00) de mão de obra para instalação completa do

equipamento, totalizando assim, seis mil reais (R$ 6.000,00). A empresa optou por não implementar tal equipamento, devido ao alto investimento que seria necessário.

- Ausência de Back-up / Falta de política de back-up

Foi criada rotina de *back-up* diário dos arquivos do servidor (figuras 8 e 9), visto que antes, não havia rotinas estabelecidas, somente a modificação de caminhos dos dados para outras pastas do servidor. Com isto, espera-se minimizar a perda de dados, em decorrência de alguma perda de arquivo decorrente de ações dos próprios usuários.

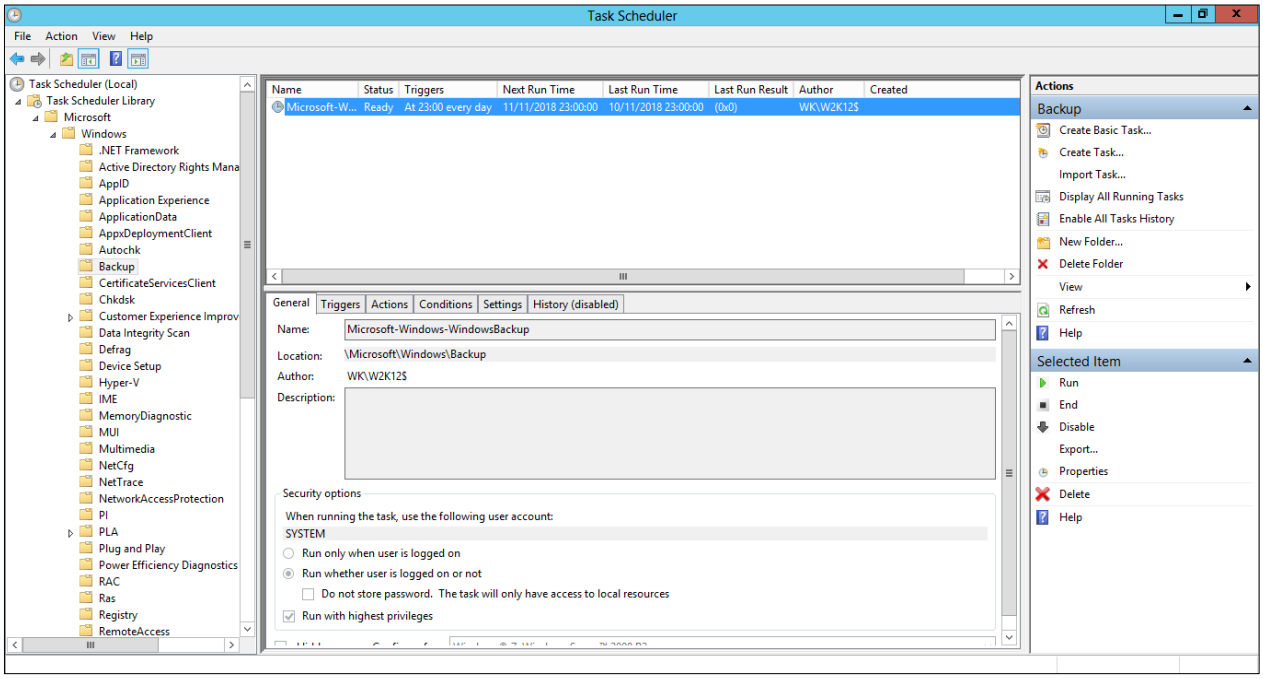



**Figura 8 - Tarefa de *Back-up* agendada**
**Fonte: Autoria própria**

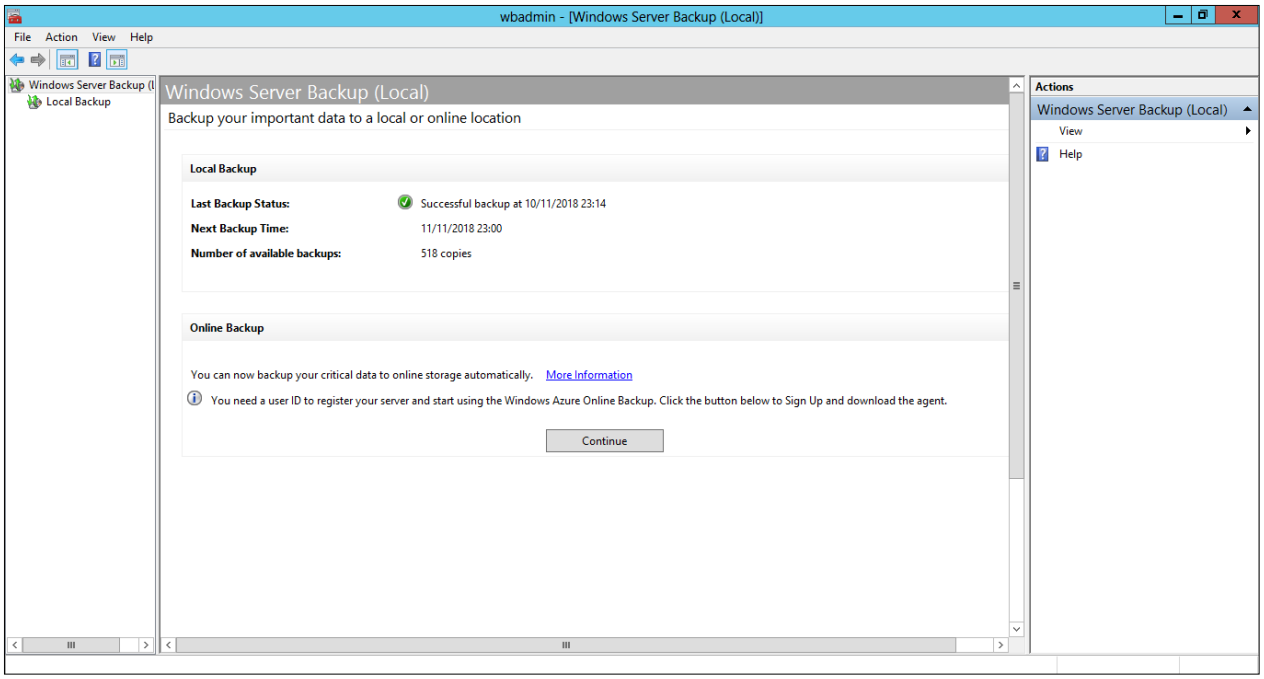



**Figura 9 - Confirmação de *back-up* efetuado**
**Fonte: Autoria própria**

- Sem solução de *Proxy* para controle habilitada

O *software* escolhido para esta implementação foi o *Squid Proxy*, que trabalha em conjunto com o *firewall pfSense.* Ele foi instalado e configurado em um primeiro momento como "*Proxy* transparente" para filtrar o acesso dos usuários a Internet, sem que os mesmos saibam da existência da ferramenta. Com esta implementação, foi gerado os relatórios (vide ANEXO C) para que os diretores da empresa pudessem visualizar os endereços *web* que cada computador dos usuários acessam em horário comercial, e a partir destes dados, começar a realizar os bloqueios necessários aos endereços que nada agregam para a organização.

- Armazenamento não protegido

Para o monitoramento dos ativos foi escolhido o software *Zabbix* (figura 8), o qual proporcionou uma visão geral dos servidores e os status de cada um deles. Espera-se que com a instalação deste programa, os responsáveis pela rede da organização tenham uma visão mais ampla dos problemas, e que o mesmo possa monitorar os recursos do servidor como espaço de armazenamento, uso dos processadores e serviços que não estão em funcionamento. (vide ANEXO B).

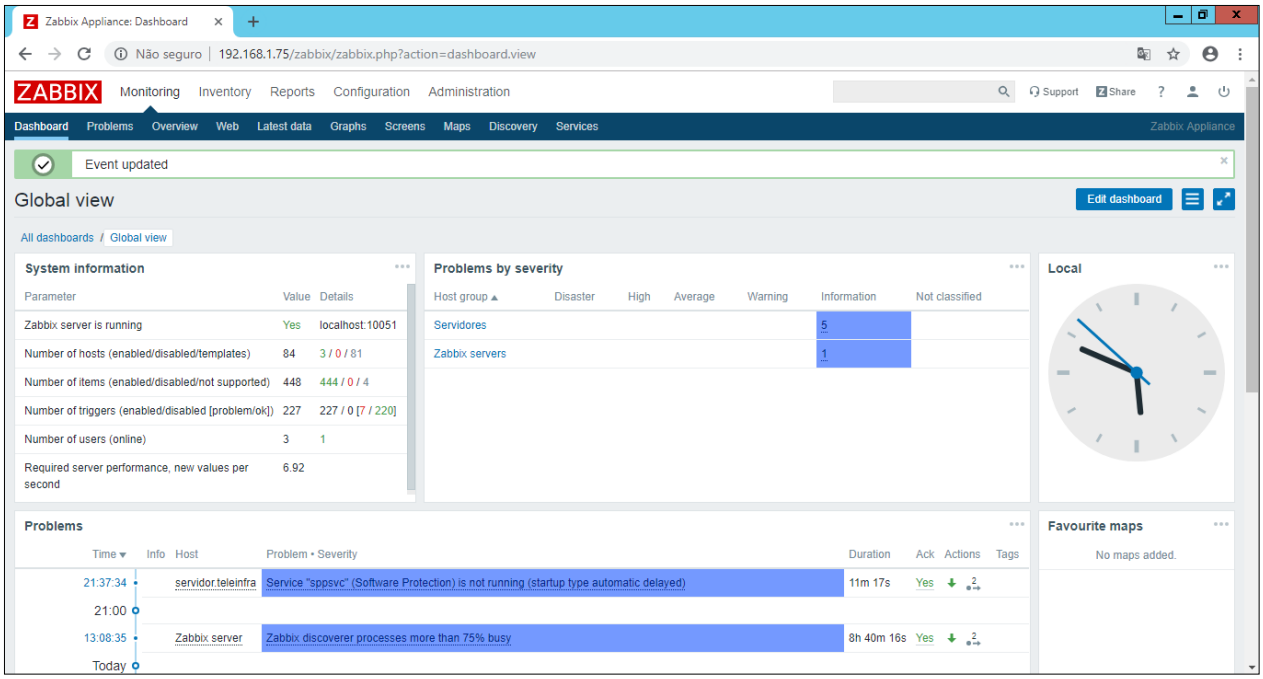



**Figura 10 - *Zabbix Appliance***
**Fonte: Autoria Própria**

- Não execução de logout

Para resolução desta vulnerabilidade, foi criada a política de grupo GPO Teleinfra (figura 11), no servidor, para que os computadores do domínio que permanecerem inativos por quinze minutos, façam *logoff* automaticamente. Além desta configuração, foi estabelecido também que cada usuário tenha uma senha mais forte, com caracteres especiais, para melhor segurança do usuário (figura 12). Foi configurado também um histórico de senhas, para que o usuário mude regularmente sua senha e esta seja diferente das últimas utilizadas por ele (figura 12).

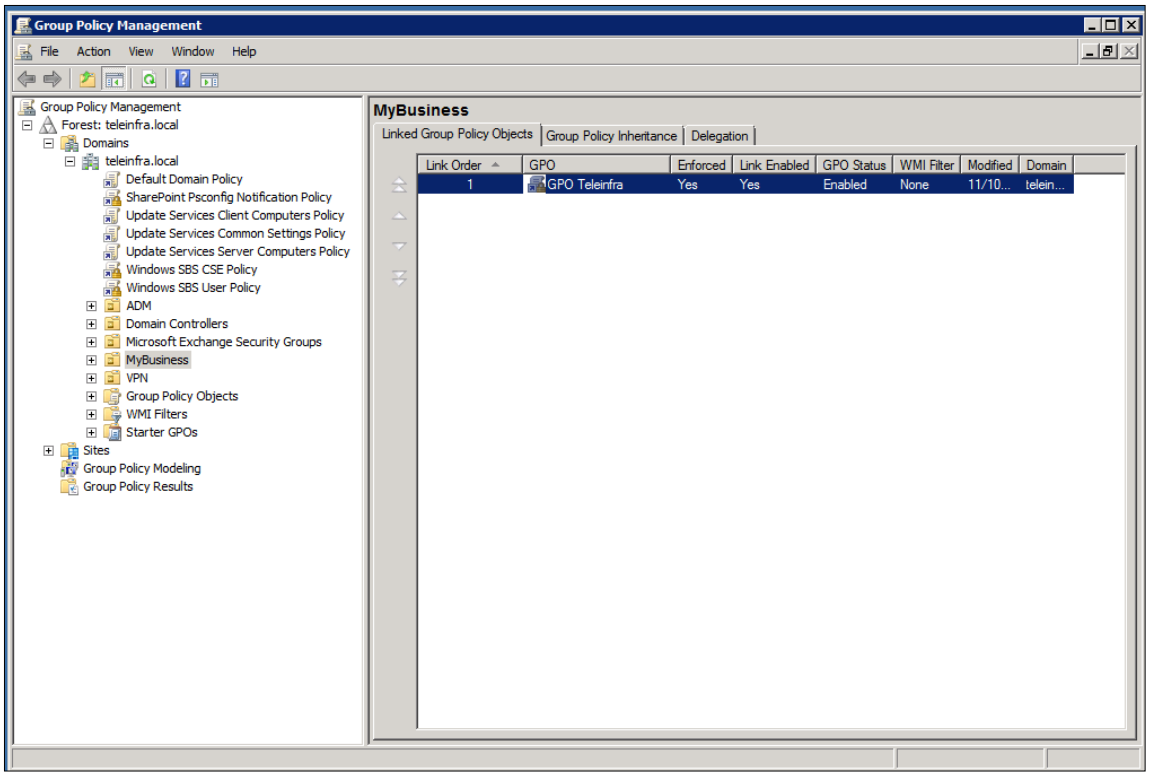



**Figura 11 - Política de Grupo Teleinfra**
**Fonte: Autoria própria**

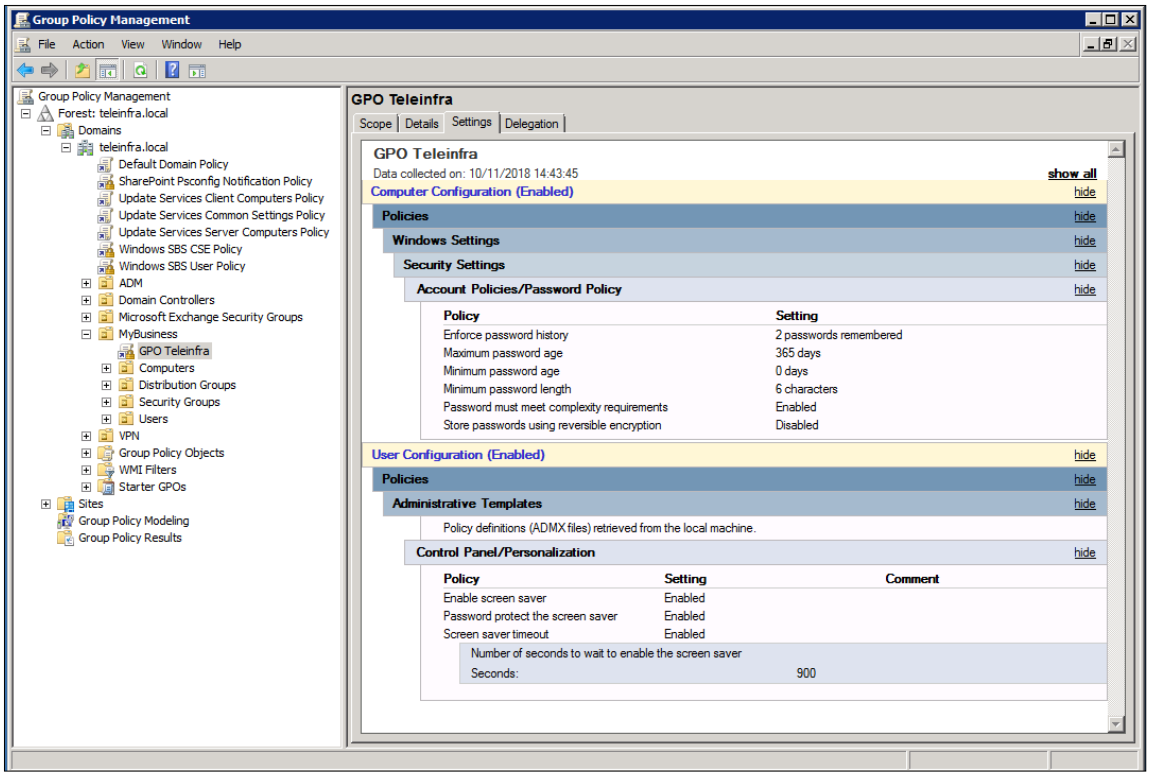



**Figura 12 - Configurações GPO Teleinfra**
**Fonte: Autoria própria**

- Ausência de enlace redundante de internet

Foi realizada a proposta da contratação de um enlace redundante de Internet para a empresa, para que ele trabalhasse em conjunto com o enlace existente. Os valores ficaram em torno de duzentos reais (R$ 200,00) mensais, porém, a empresa não demonstrou interesse em contratar outro enlace no momento. Esperava-se com esta implantação, melhorar a disponibilidade dos recursos da empresa.

- Troca de senhas entre colaboradores / Engenharia Social

Para criação do Manual de Boas Práticas da empresa (vide ANEXO E), foram estabelecidas regras em comum acordo com os diretores da empresa, os quais validaram o documento e disponibilizaram para os colaboradores terem ciência das regras e boas práticas a serem seguidas para o uso dos ativos de rede da empresa. A partir da implantação deste manual, cada usuário saberá as regras e punições as quais estarão sujeitos e com isto, espera-se minimizar as vulnerabilidades decorrente das próprias pessoas que trabalham na organização.

## 4. CONSIDERAÇÕES FINAIS

A segurança da informação é um ativo muito importante dentro da organização, sendo assim, é necessário tratá-la com segurança, pois o seu vazamento pode vir a prejudicar toda a empresa e de maneiras irreversíveis. Seguindo as normas da família NBR ISO/IEC 27000, pode-se estabelecer diretrizes que compõe uma série de requisitos para que as informações sejam tratadas com segurança e se alguma falha no processo acontecer seja identificado o mais breve possível e registrado para fins de auditoria e até melhoria contínua do sistema de gestão de segurança de informação.

As sugestões propostas implementadas e não implementadas no estudo podem e devem ser monitoradas pelo setor responsável da empresa, visando a cada vez mais, minimizar os impactos das vulnerabilidades, procurando soluções em conjunto com os colaboradores, os quais são peças importantes no processo de identificação e tratamento da possível ameaça.

Apesar de algumas soluções que necessitam de verba mais alta não terem sido realizadas em curto prazo, os resultados do estudo foram satisfatórios, pois com algumas ferramentas, softwares *Open Source* e configurações simples, sempre referenciados pelas normas de referência (ABNT ISO/IEC 27001, ABNT ISO/IEC 27002 e ABNT ISO/IEC 27005) conseguiu-se minimizar vários riscos de valor médio e alto, os quais poderiam gerar perdas para a empresa.

## REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.** ABNT, 2006.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2005.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2011.

BATISTA, Isaac Danilo S., DA SILVA, Cícero Alves, DA SILVA, Ronaldo Gomes, DE ARAÚJO, Fernanda Rodrigues. **Governança Da Tecnologia Da Informação Na Atualidade: A Importância Da Adoção De Modelos De Melhores Práticas Nas Organizações.** 2015. Artigo Científico - *II World Congress on Systems Engineering and Information Technology,* Vigo, Espanha, 2015.

CAVALHEIRO, Mario A. L., PADILHA, Willian. **Segurança Digital: Vulnerabilidade De Dados Em Meios Coorporativos.** 2016. Artigo Científico - Revista Uniplac - Anais da XIX Mostra Científica Uniplac, v.4, n.1 - ISSN 2447/2016.

DOS SANTOS, Edenilza P., MOURA, Eulene C., SILVA, Jandira de M. **Segurança Da Informação: Como Garantir A Integridade, A Confidencialidade E A Disponibilidade Das Informações Em Uma Organização Educacional Privada De Teresina.** 2010. Artigo Científico - Revista Científica da FSA - Tesesina, 2010.

KONZEN, Marcos Paulo. **Gestão de Riscos de Segurança da Informação baseada na norma NBR ISO/IEC 27005 usando padrões de Segurança.** 2013. Dissertação de Mestrado – Universidade Federal de Santa Maria UFSM – Santa Maria/RS, 2013

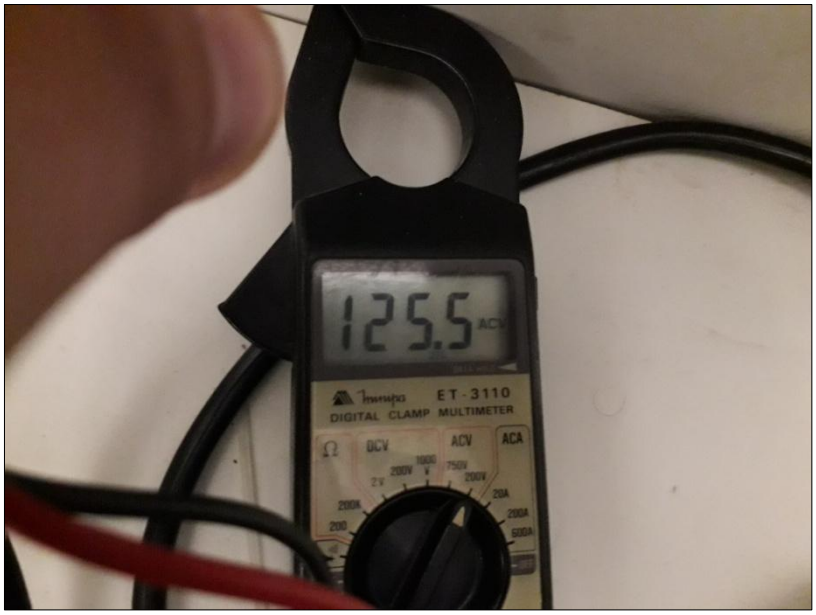
MOTA FILHO, João Eriberto. **Análise de Tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. São Paulo. Novatec Editora, 2013. 351p.

SARAIVA, Fernanda M. **Um estudo prático sobre segurança da informação.** 2012. Trabalho de Conclusão de Curso (Graduação em Computação)—Centro de Ciências Exatas e Sociais Aplicadas, Universidade Estadual da Paraíba, Patos, 2012.

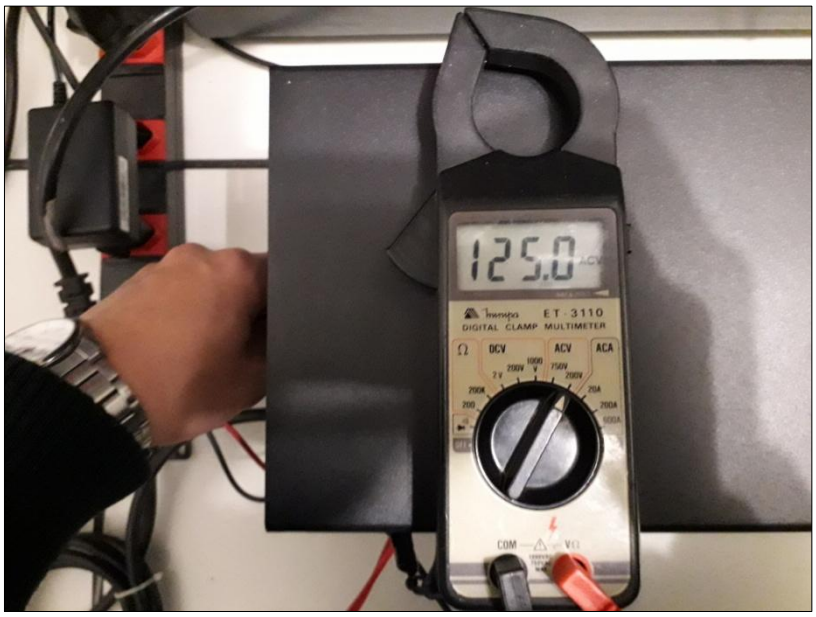
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. Sistema de Bibliotecas. **Normas para elaboração de trabalhos acadêmicos**. Curitiba: Editora UTFPR, 2009. 116p.

# ANEXOS

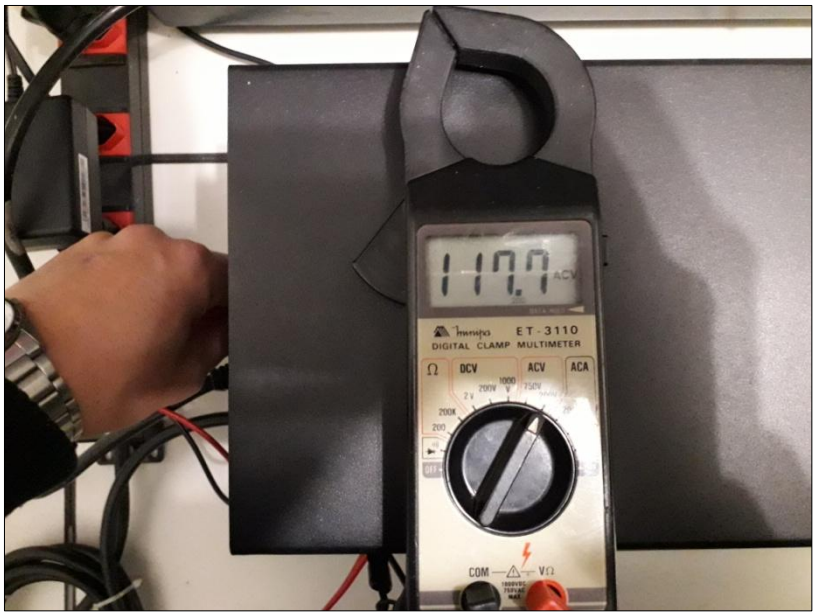
**ANEXO A** – Medidas de Tensões



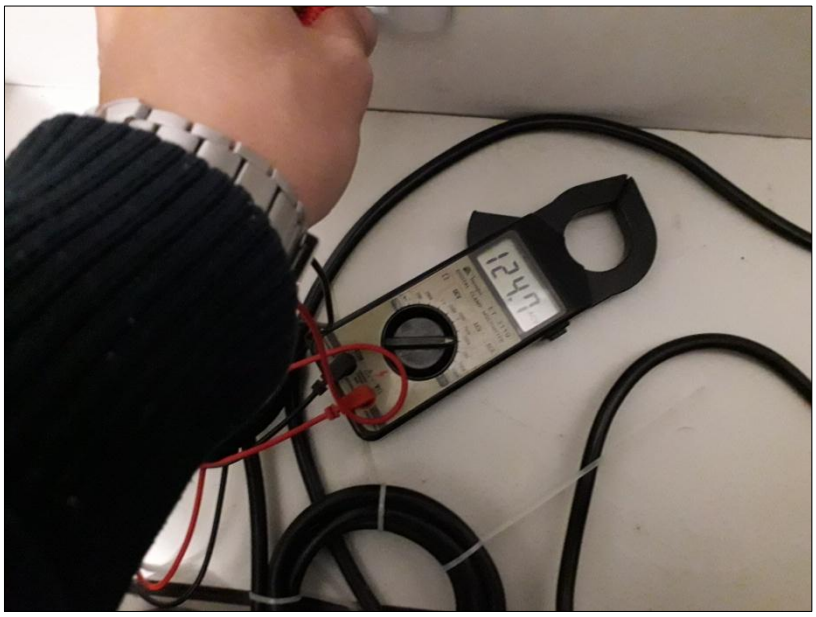

Tensão da tomada da concessionária – manhã




Tensão da tomada do *no-break* (ligado na tomada da concessionária) – manhã



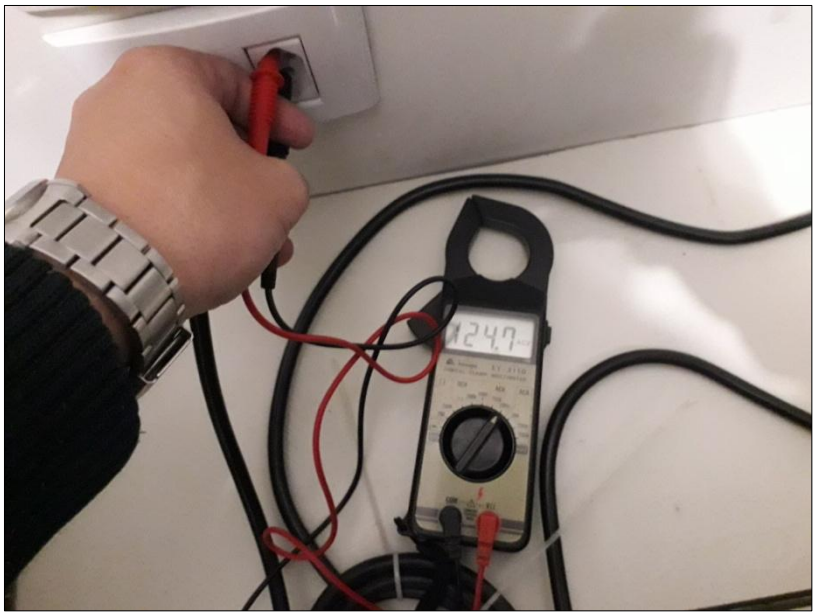

Tensão da tomada do no-break (com a carga da bateria) – manhã



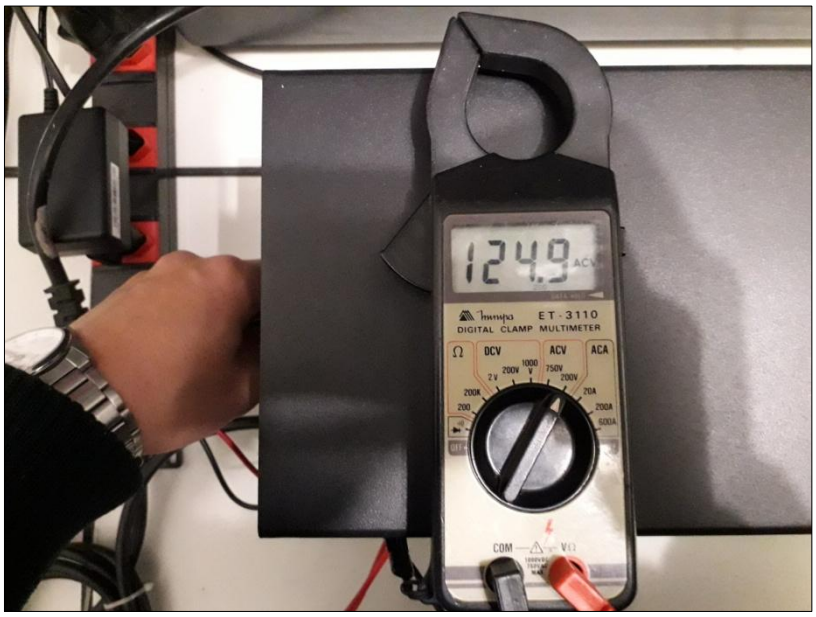

Tensão da tomada da concessionária – tarde


Tensão da tomada do no-break (ligado na tomada da concessionária) – tarde

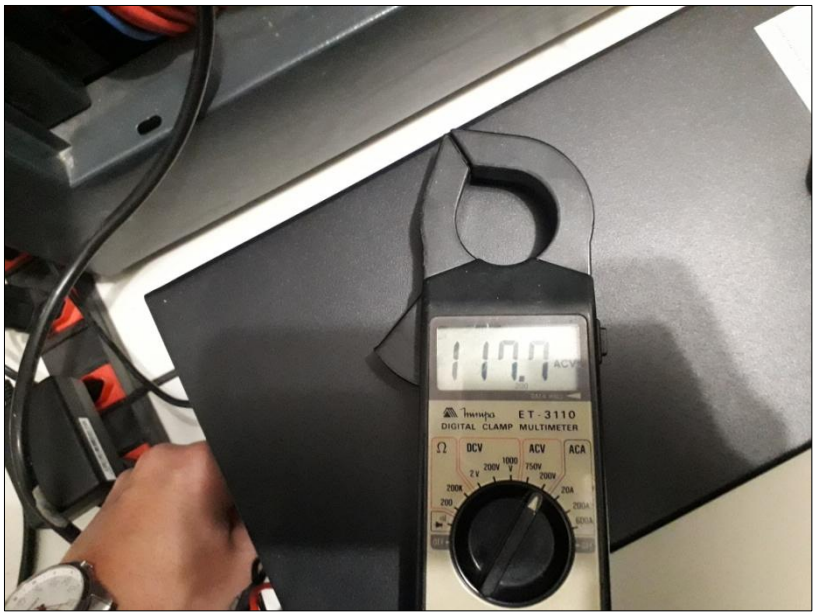

Tensão da tomada do no-break (com a carga da bateria) – tarde




Tensão da tomada da concessionária – noite



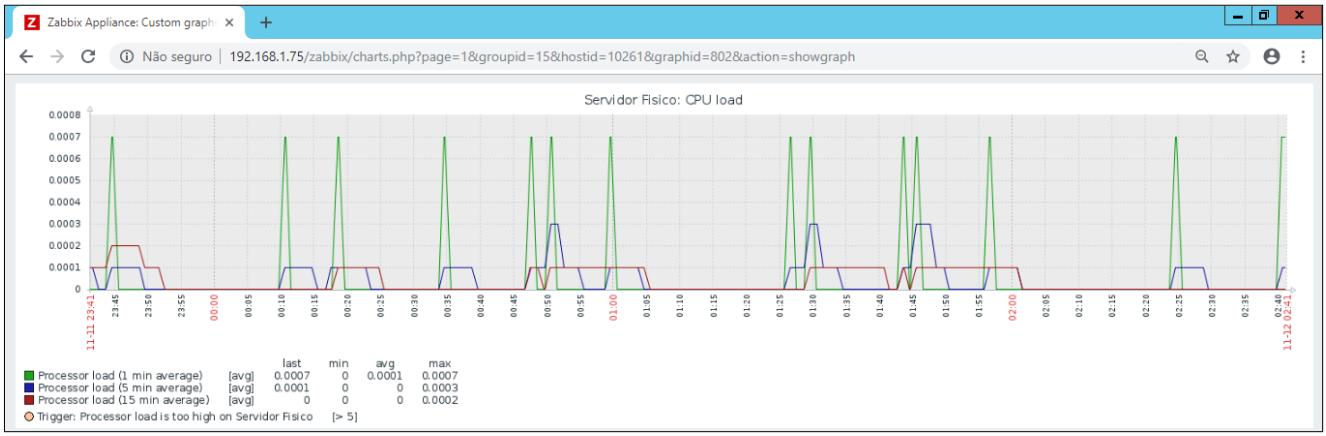

Tensão da tomada do no-break (ligado na tomada da concessionária) – noite



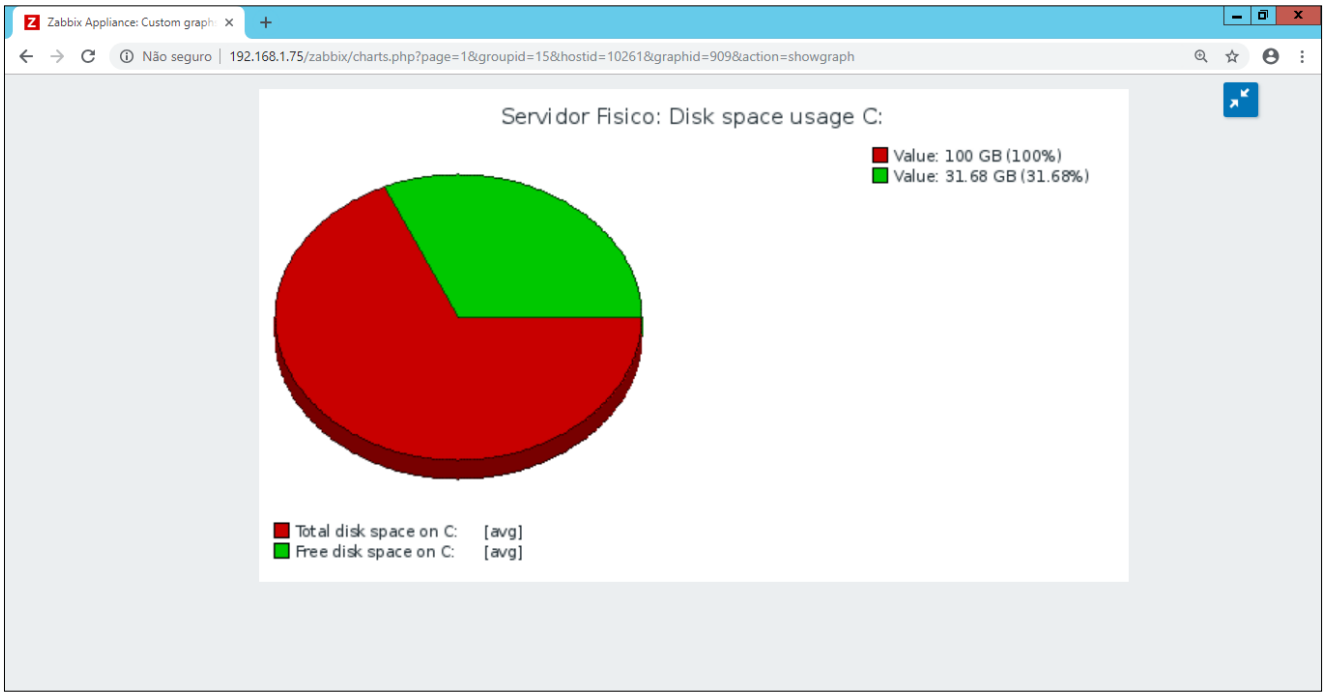

Tensão da tomada do no-break (com a carga da bateria) – tarde

**ANEXO B** – Telas *Zabbix*

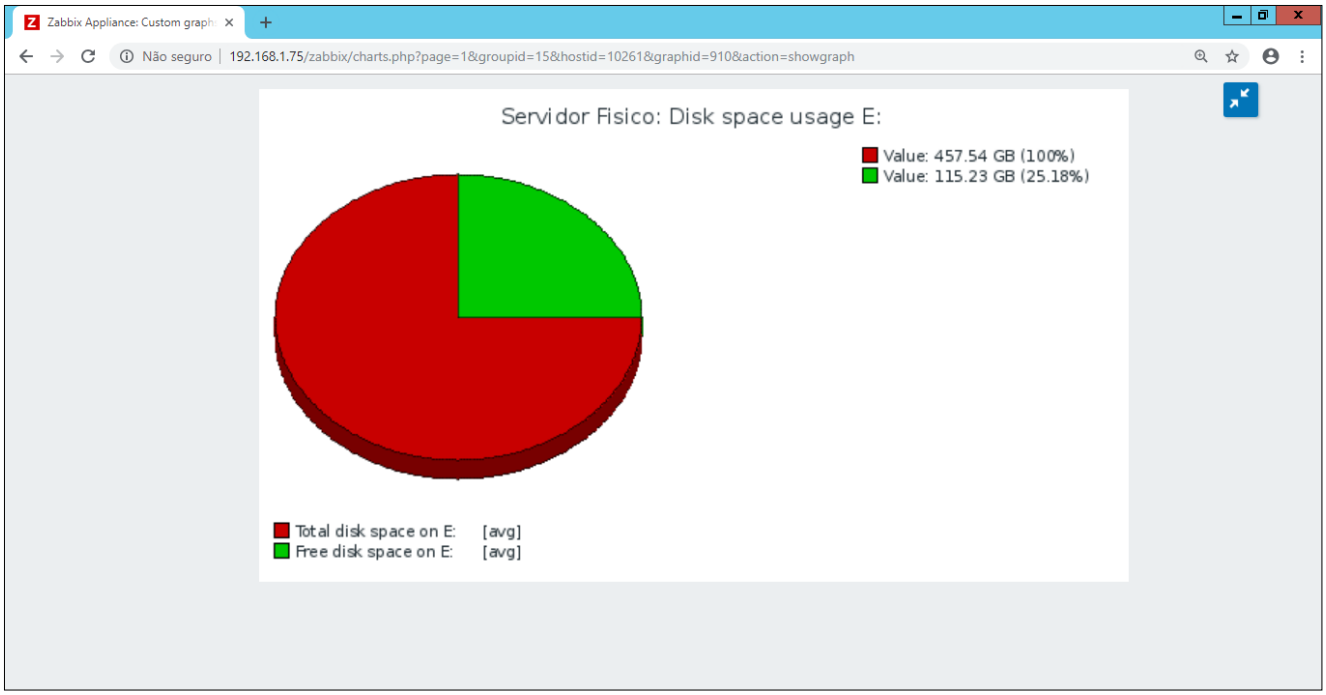
## Telas Servidor Físico



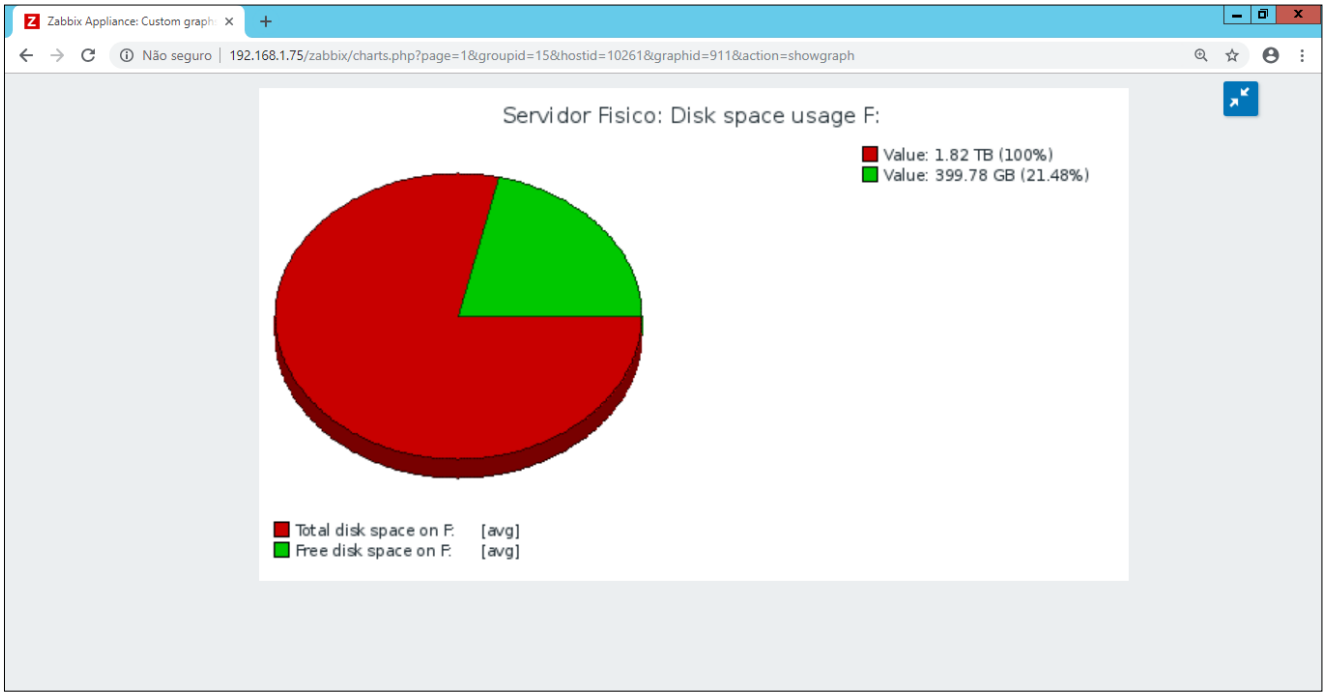

Uso dos processadores do Servidor



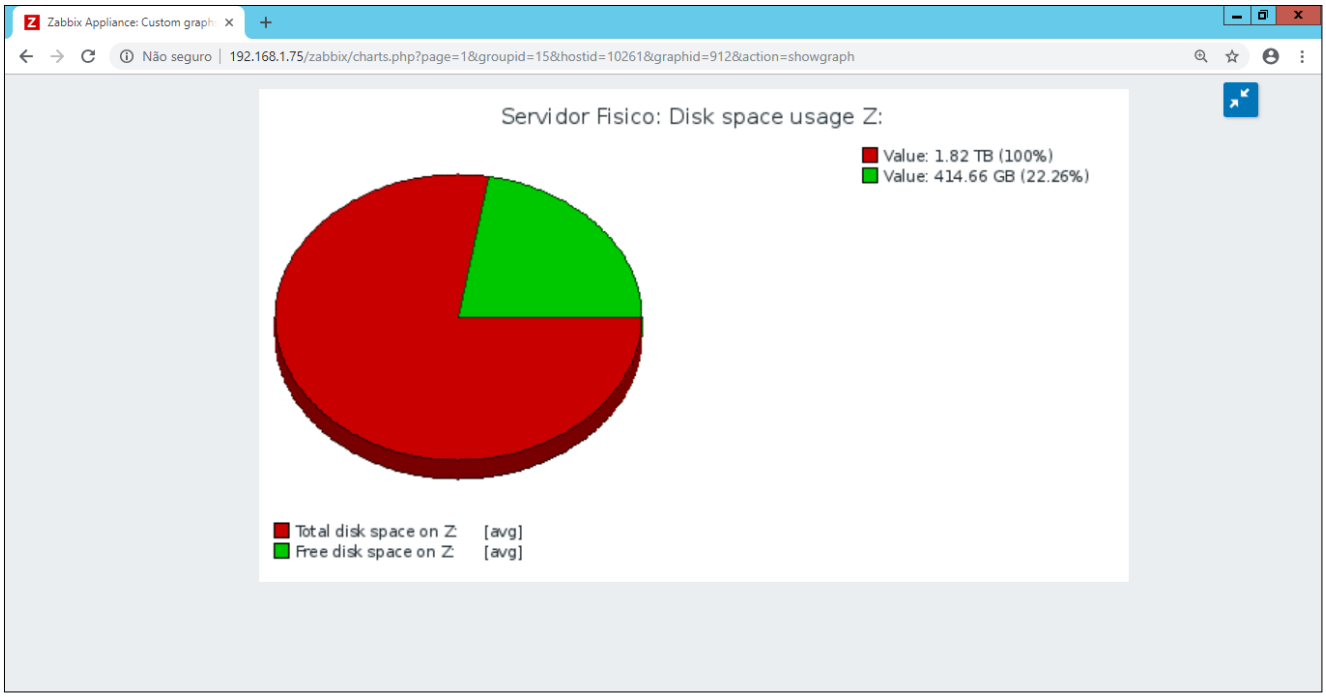

Utilização do espaço no disco C:\ do servidor



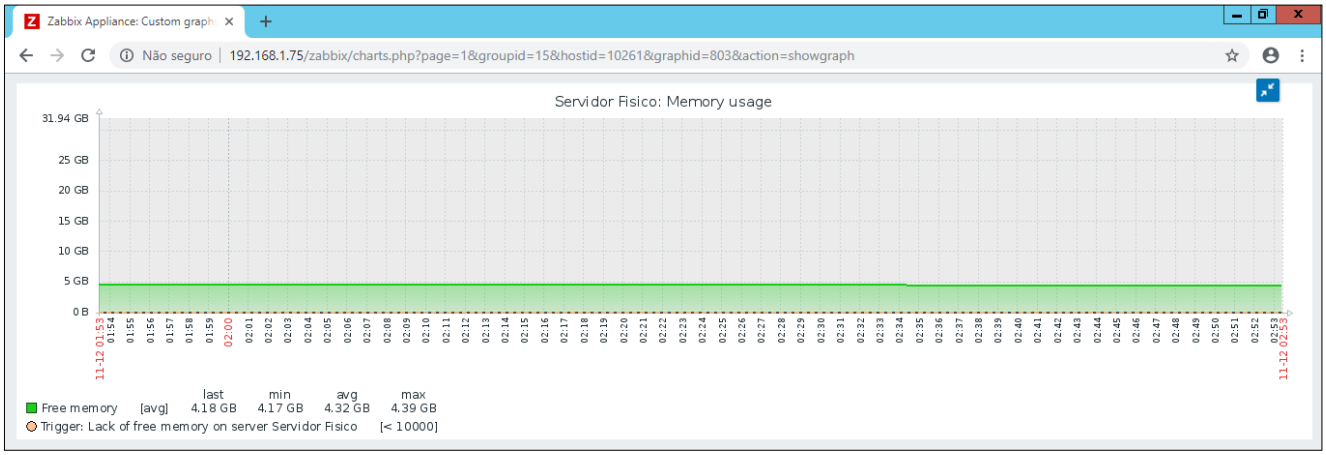

Utilização do espaço no disco E:\ do servidor




Utilização do espaço no disco F:\ do servidor

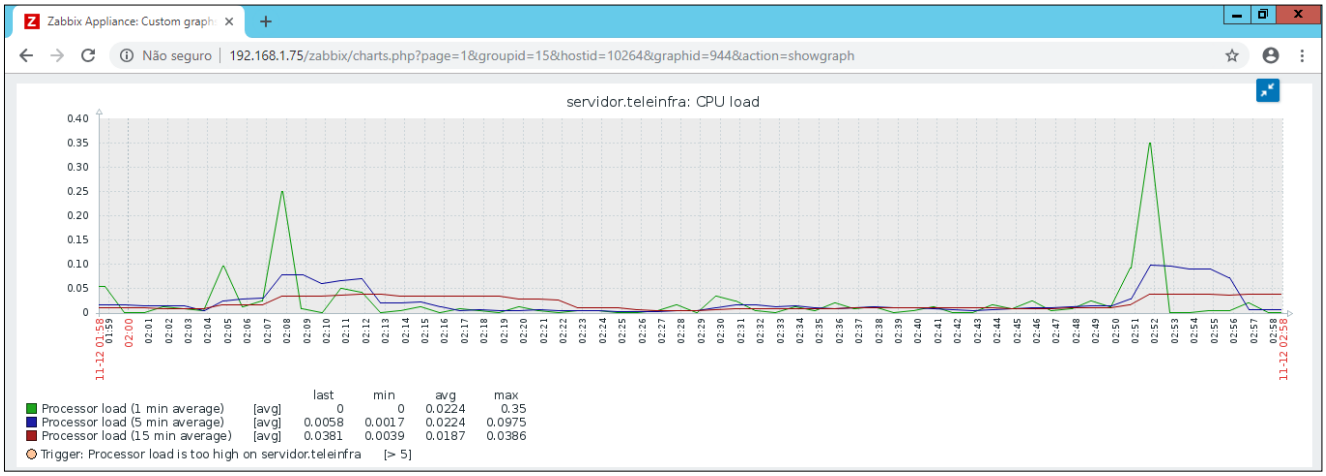



Utilização do espaço no disco Z:\ do servidor

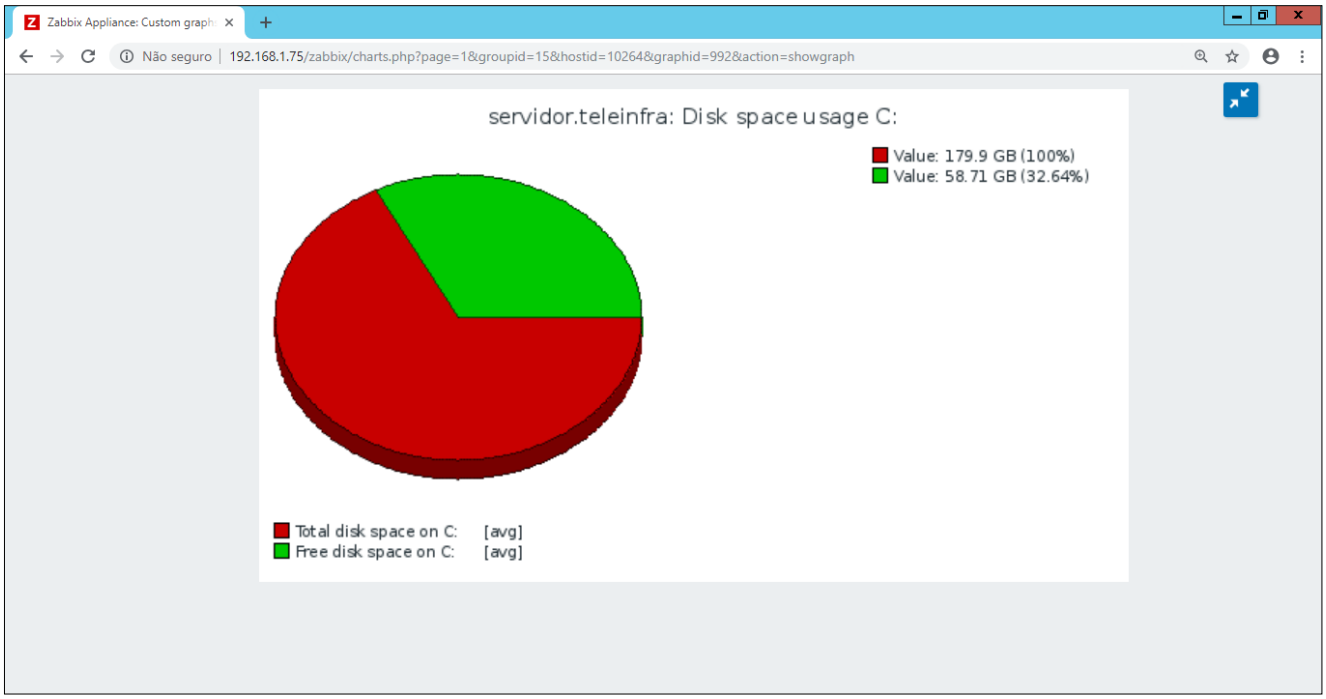



Utilização da memória do servidor

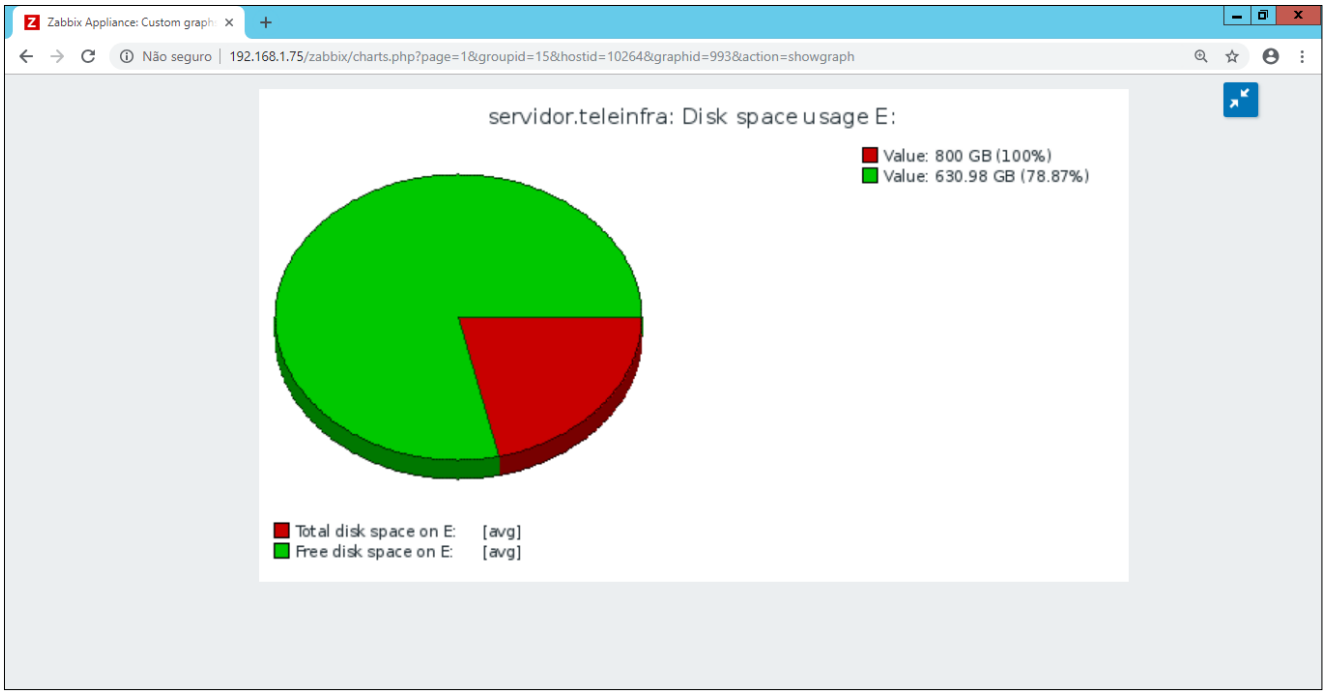
Telas Servidor Virtual *(Hyper-V)*



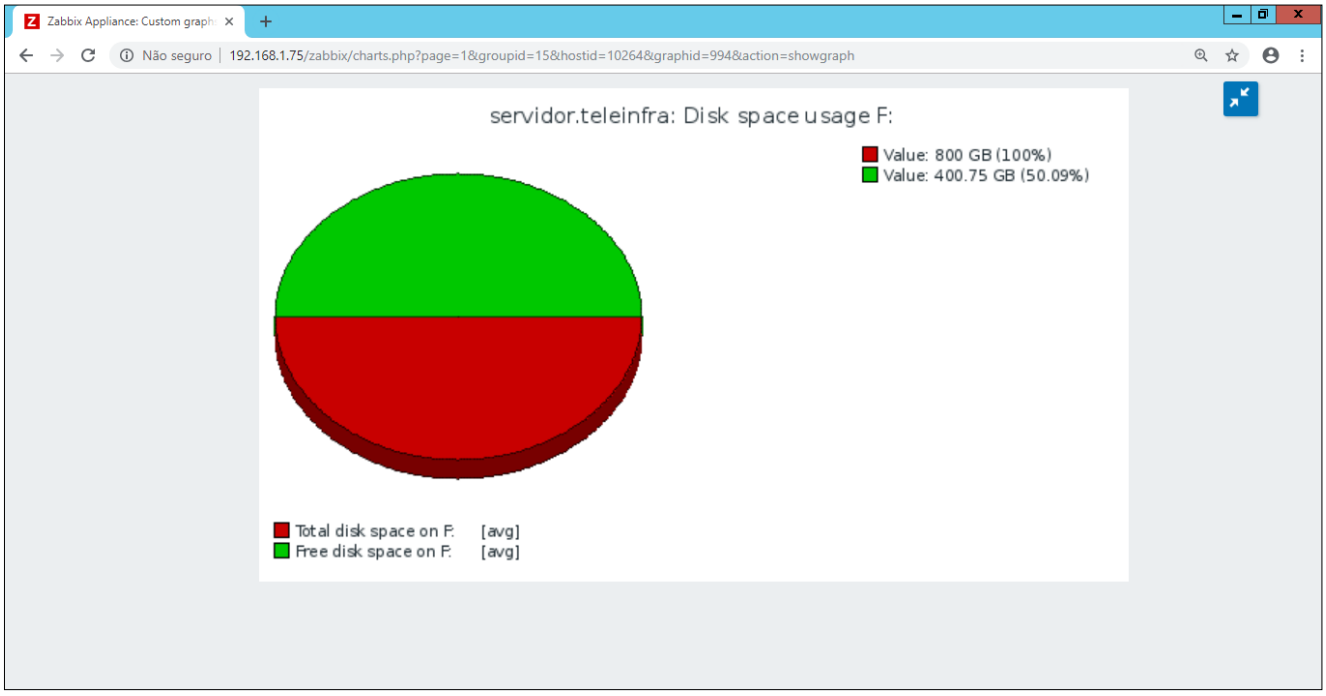

Uso dos processadores do Servidor



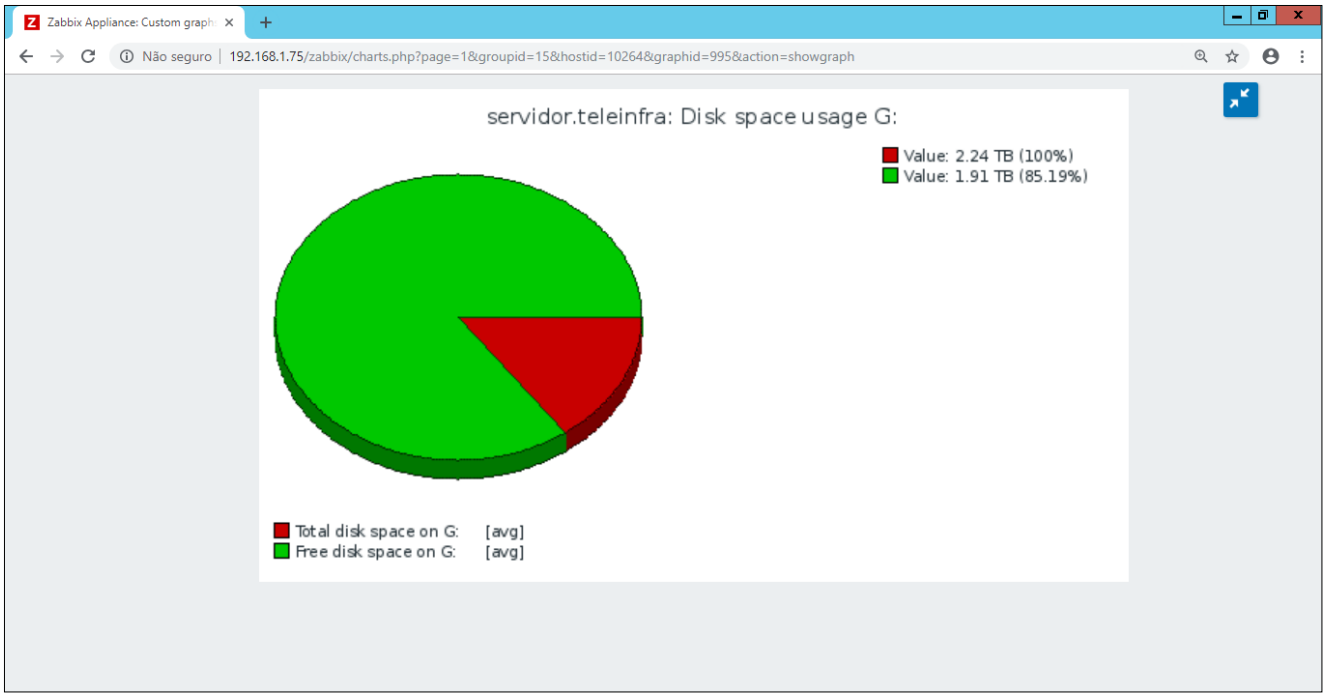

Utilização do espaço no disco C:\ do servidor



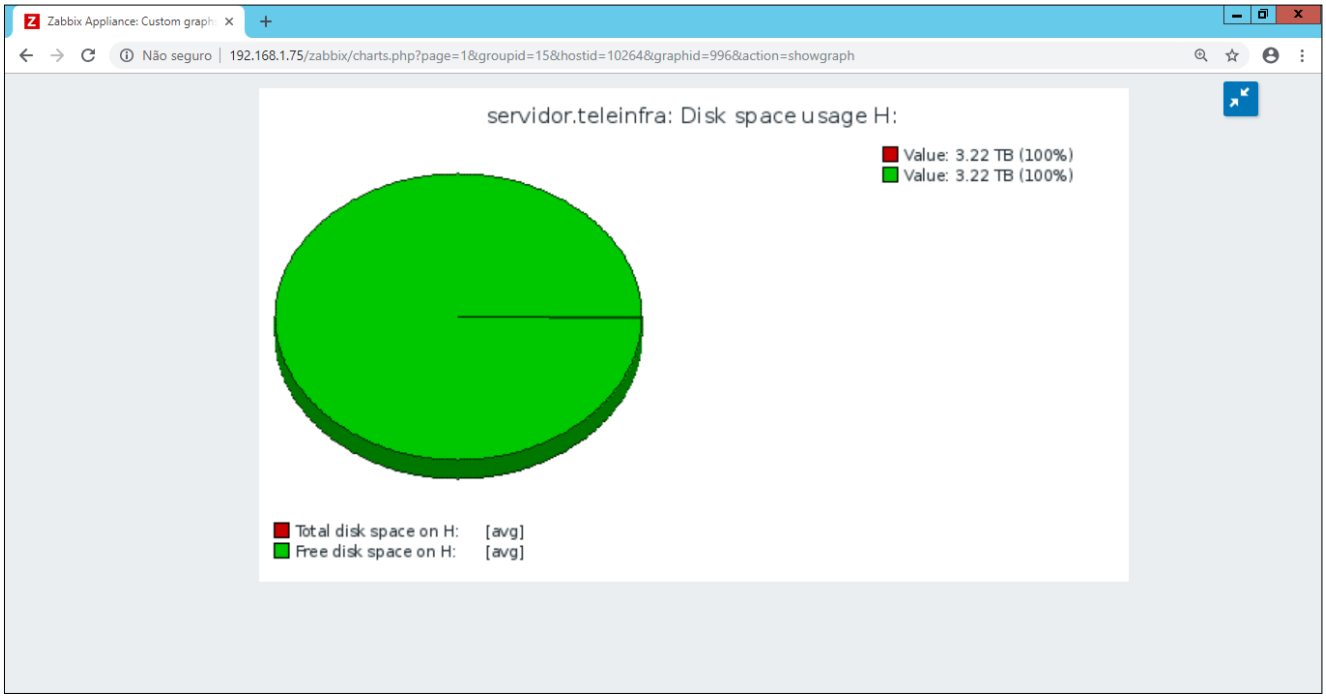

Utilização do espaço no disco E:\ do servidor



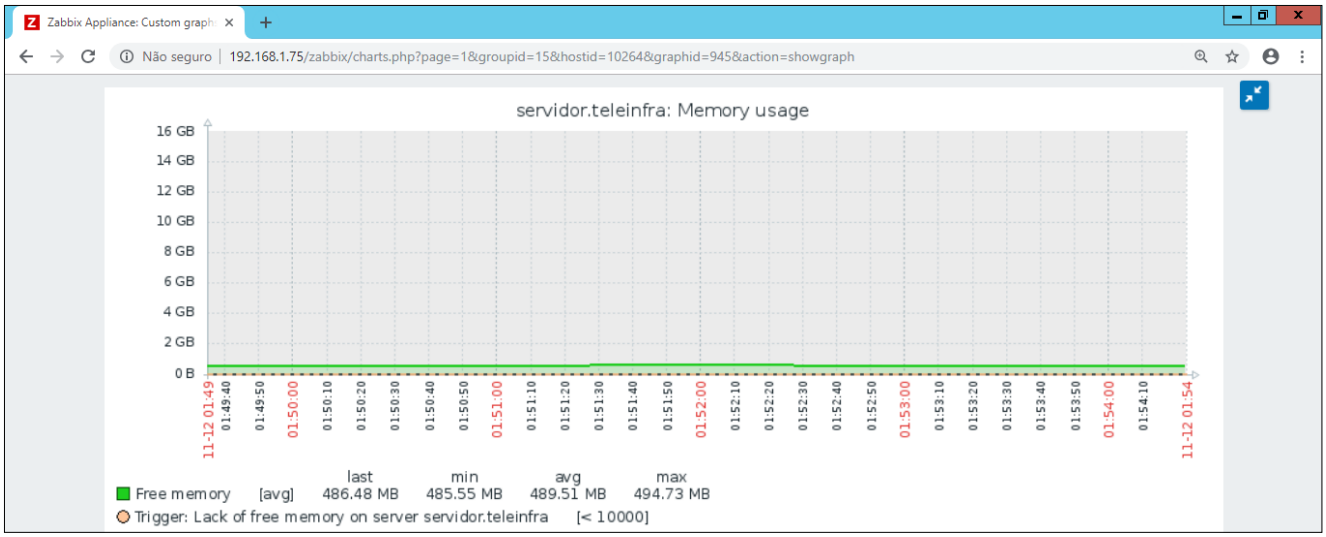

Utilização do espaço no disco F:\ do servidor




Utilização do espaço no disco G:\ do servidor




Utilização do espaço no disco H:\ do servidor




Utilização da memória do servidor

**ANEXO C** – Relatório em tempo real *Proxy Squid*

Squid RealTime stat 1.20 for the proxy server squid/3.5.27 (127.0.0.1:3128).

Auto refresh: 3 sec. Created at: 09:06:50 12/11/2018

| URI | Curr. Speed | Avg. Speed | Size | Time |
|---|---|---|---|---|
| **Total:** | **4** users and **49** connections @ **644.28/176.68** KB/s (CURR/AVG) | | | |
| **192.168.1.28** | | | | |
| login.live.com:443 | | 0.56 KB/s | 13 Kb | 24s |
| windows.policies.live.net:443 | | 0.38 KB/s | 9 Kb | 26s |
| go.microsoft.com:443 | | 0.02 KB/s | 665 b | 26s |
| ad.atdmt.com:443 | | 0.01 KB/s | 716 b | 49s |
| assets.vitrinesglobo.com.br:443 | | 1.35 KB/s | 68 Kb | 51s |
| tpc.googlesyndication.com:443 | | 1.42 KB/s | 75 Kb | 53s |
| display.vitrines.in:443 | | 0.34 KB/s | 18 Kb | 55s |
| vitrines.globo.com:443 | | 0.03 KB/s | 1 Kb | 55s |
| securepubads.g.doubleclick.net:443 | | 0.56 KB/s | 32 Kb | 58s |
| pagead2.googlesyndication.com:443 | | 0.03 KB/s | 1 Kb | 58s |
| safebrowsing.googleapis.com:443 | | 0.02 KB/s | 1 Kb | 1m 17s |
| adservice.google.com:443 | | 0.01 KB/s | 1 Kb | 3m 18s |
| adservice.google.com.br:443 | | 0.01 KB/s | 1 Kb | 3m 18s |
| www.google.com.br:443 | | 0.01 KB/s | 3 Kb | 8m 21s |
| www.google.com:443 | | 0.01 KB/s | 6 Kb | 8m 22s |
| stats.g.doubleclick.net:443 | | 0.02 KB/s | 9 Kb | 8m 23s |
| www.google-analytics.com:443 | | 0.02 KB/s | 11 Kb | 8m 25s |
| cdn.navdmp.com:443 | | | 1 Kb | 18m 37s |
| mtalk.google.com:443 | | | 4 Kb | 25m 53s |
| w1.web.whatsapp.com:443 | 630.17 KB/s | 0.43 KB/s | 1 Mb | 40m |
| w7.web.whatsapp.com:443 | | 0.08 KB/s | 195 Kb | 41m 32s |
| | 630.17 KB/s | 5.31 KB/s | | |
| **192.168.1.44** | | | | |
| mtalk.google.com:443 | | | 4 Kb | 14m 55s |
| w5.web.whatsapp.com:443 | 14.11 KB/s | 0.18 KB/s | 416 Kb | 39m 1s |
| | 14.11 KB/s | 0.18 KB/s | | |
| **192.168.1.50** | | | | |
| static.doubleclick.net:443 | | | 0 b | |
| googleads.g.doubleclick.net:443 | | 0.19 KB/s | 199 b | |
| cdn.syndication.twimg.com:443 | | 4.04 KB/s | 4 Kb | |
| syndication.twitter.com:443 | | 1.16 KB/s | 1 Kb | |
| www.google-analytics.com:443 | | 0.69 KB/s | 710 b | |
| s0.2mdn.net:443 | | 52.45 KB/s | 52 Kb | 1s |
| www.youtube.com:443 | | 16.75 KB/s | 16 Kb | 1s |

| | | | | | |
|---|---|---|---|---|---|
| | connect.facebook.net:443 | | 55.04 KB/s | 55 Kb | 1s |
| | 192.168.1.238:443 | | 4.08 KB/s | 8 Kb | 2s |
| | dc.services.visualstudio.com:443 | | 3.28 KB/s | 6 Kb | 2s |
| | clients4.google.com:443 | | 0.97 KB/s | 1 Kb | 2s |
| | ib.la.ib-ibi.com:443 | | 1.92 KB/s | 3 Kb | 2s |
| | www.google.com.br:443 | | 0.57 KB/s | 1 Kb | 3s |
| | global.ib-ibi.com:443 | | 1.14 KB/s | 3 Kb | 3s |
| | s-akhtm.nspmotion.com:443 | | 1.17 KB/s | 3 Kb | 3s |
| | s-akhtm.nspmotion.com:443 | | 11.11 KB/s | 33 Kb | 3s |
| | static.ads-twitter.com:443 | | 1.31 KB/s | 3 Kb | 3s |
| | utp.br:443 | | 1.99 KB/s | 5 Kb | 3s |
| | sync.navdmp.com:443 | | 1.42 KB/s | 4 Kb | 3s |
| | beacon.krxd.net:443 | | 0.06 KB/s | 184 b | 3s |
| | beacon.krxd.net:443 | | 0.16 KB/s | 666 b | 4s |
| | beacon.krxd.net:443 | | 0.37 KB/s | 1 Kb | 4s |
| | www.tuiuti.edu.br:443 | | 8.79 KB/s | 35 Kb | 4s |
| | dc.services.visualstudio.com:443 | | 2.04 KB/s | 8 Kb | 4s |
| | mtalk.google.com:443 | | 0.03 KB/s | 4 Kb | 2m 33s |
| | | 0.00 KB/s | 170.76 KB/s | | |
| **192.168.1.65** | | | | | |
| | w8.web.whatsapp.com:443 | | 0.44 KB/s | 402 Kb | 15m 17s |
| | | 0.00 KB/s | 0.44 KB/s | | |
| **Total:** | **4** users and **49** connections @ **644.28/176.68** KB/s (CURR/AVG) | | | | |

Report based on SQStat © Alex Samorukov, 2006

**ANEXO D** – Plano básico de continuidade TELEINFRA

TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

PLANO BÁSICO DE CONTINUIDADE DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

O funcionário da empresa Teleinfra Serviços em Teleinformática e Infraestrutura, durante seu expediente de trabalho, vier a se deparar com os problemas abaixo:

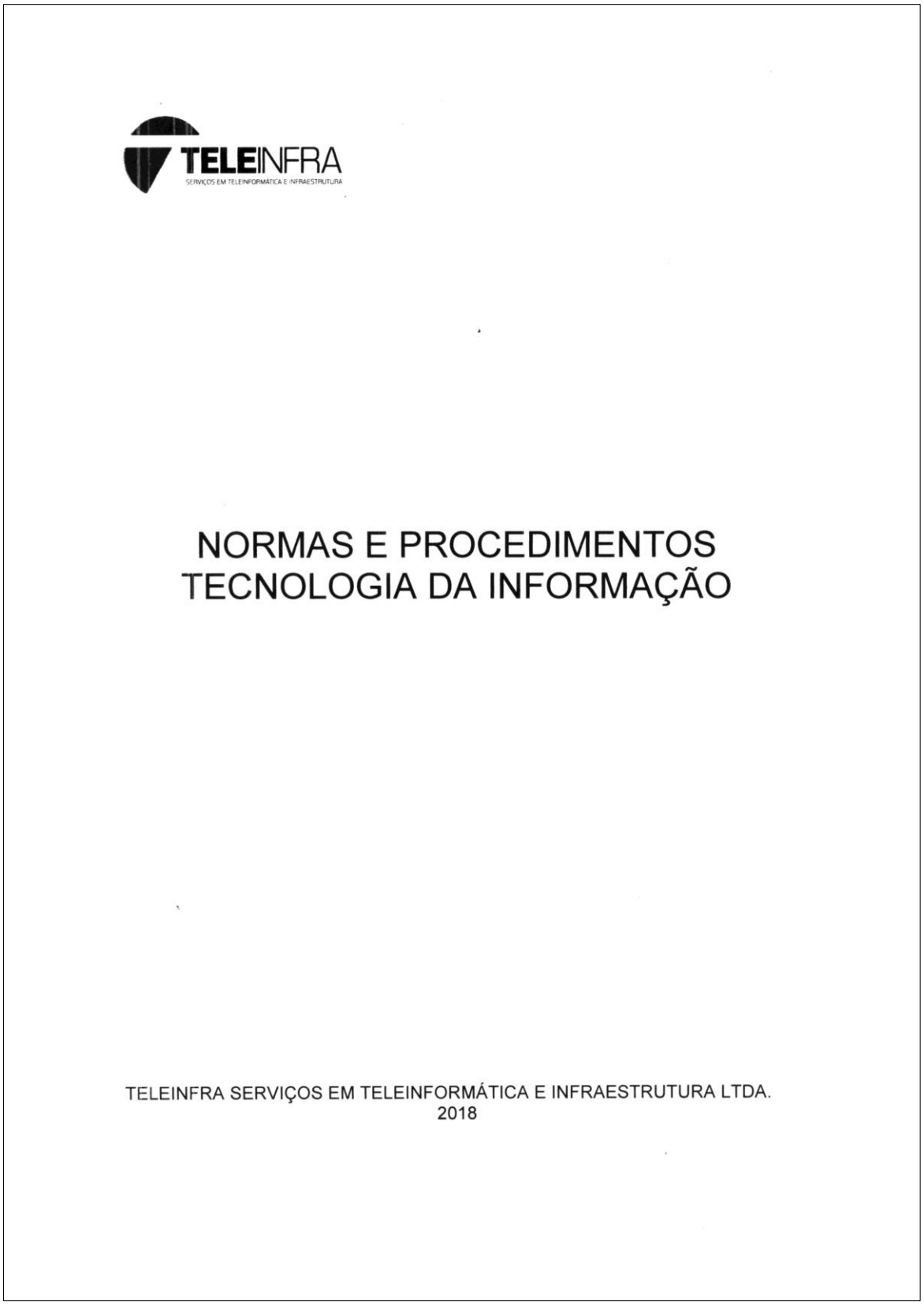
- O seu computador parar de funcionar;
- Recebeu um e-mail suspeito;
- Princípio de incêndio nos equipamentos;
- Presença de vírus no computador de trabalho;
- Alteração não realizada pelo usuário;
- Queda de energia, onde o no-break do seu computador não acionar;
- Sistema operacional acusar falha ("Tela Azul");
- Algum serviço não estiver funcionando corretamente;
- Aplicação SIT (Sistema Integrado Teleinfra) não estiver acessível;
- Não tiver conectividade com a rede de trabalho;
- Esquecer sua senha;
- Modificar sua senha;

Ou qualquer outro problema relacionado a tecnologia da informação não citado acima, tem o DEVER de entrar em contato com o responsável pelo setor de tecnologia da informação afim de relatar, para que as medidas de controle e reparo possam ser efetuadas.

Responsável pelo setor de Tecnologia da Informação
Felipe Schloser Zarpelon
Ramal: 5511
Celular: (41)98804-6754
e-mail: felipe@teleinfra.com.br

1

**ANEXO E** – Manual de boas práticas TELEINFRA



TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

**ÍNDICE**

TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

## 1 INTRODUÇÃO

Este documento visa apresentar os recursos de tecnologia da informação disponibilizados pela empresa ao colaborador, sugerir boas práticas em relação ao uso de tais ferramentas, apresentar os principais riscos a ataques cibernéticos e como geralmente são realizados. Além dos assuntos citados acima, este documento também delimita as proibições e possíveis penalidades se forem transgredidas.

TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

## 2 SALA DO SERVIDOR

Na sala do servidor, encontram-se os principais ativos de rede da empresa, portanto, é a parte mais importante do universo de tecnologia de informação da organização. Dentre os principais ativos, um se destaca pela sua importância, o servidor. Ele é monitorado e gerenciado pelo Gerente de Tecnologia da informação (T.I.) e qualquer alteração de usuário, senha e outros, deve ser solicitado a ele.

Neste ambiente também está localizado nosso Sistema Integrado Teleinfra (SIT) que, como o servidor, é de responsabilidade do Gerente de T.I., realizar qualquer solicitação dos usuários.

A sala do servidor têm acesso restrito aos colaboradores, sendo somente permitida a sua entrada mediante autorização do gerente de Tecnologia da Informação (T.I.) ou de algum dos Sócios-administradores.

## 3 COMPUTADORES DA EMPRESA

Os computadores da empresa são de uso exclusivamente a serviço.

Não serão aceitas instalações de jogos ou outros programas sem a autorização do Gerente de T.I.. Este procedimento visa evitar possíveis problemas em campo, quando o técnico mais necessita do equipamento em um local com poucos recursos.

O mau uso ou negligência por parte do colaborador quanto ao equipamento, o mesmo poderá ser advertido e os possíveis valores decorrentes do ato, debitados.

Os equipamentos da empresa deverão ser deixados na empresa ao término das atividades. Caso o mesmo não seja deixado na empresa e, por alguma razão for roubado ou danificado, as despesas decorrentes poderão ser cobradas do colaborador responsável.

TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

Casos específicos deverão ser autorizados pela gerência de T.I. ou pela gerência da empresa.

## 4 USO DA INTERNET

O uso da Internet pelos colaboradores é permitido desde que seu uso seja inerente aos objetivos e atividades e para fins de pesquisa.

Solicitamos a todos os colaboradores / usuários, que tomem conhecimento das regras e se comprometam a seguir cada uma das orientações abaixo:

- Seguir a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias);
- Usar a Internet de uma forma aceitável e somente para fins profissionais;
- Não criar riscos desnecessários para a empresa.

**É terminantemente proibido:**

- Visitar sites da Internet que contenha material obsceno e/ou pornográfico;
- Acessar redes sociais como Facebook / Whatsapp para assuntos pessoais, etc.
- Usar a Internet para enviar material ofensivo ou de assédio para outros usuários;
- Usar o computador para executar quaisquer tipos ou formas de fraudes, ou software/musica pirata;
- Atacar e/ou pesquisar em áreas não autorizadas;
- Criar ou transmitir material difamatório;
- Introduzir de qualquer forma um vírus de computador dentro da rede

corporativa;

A Teleinfra afirma que o uso da Internet é uma ferramenta para seus negócios. E o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos colaboradores, por isso, a empresa se dá ao direito de monitorar, juntamente com os endereços web visitados. Bem como ter a liberdade de a qualquer momento bloquear o seu uso.

## 5 BOAS PRÁTICAS COMO USUÁRIO

Seguem abaixo algumas instruções para as boas práticas do usuário da rede da empresa:

- Evitar usar as ferramentas de trabalho para uso pessoal;
- Não deixar documentos importantes jogados em sua estação de trabalho;
- Não realizar o compartilhamento de senhas entre colaboradores;
- Efetuar *Logoff* em sua estação de trabalho quando não estiver realizando o uso da mesma;
- Não instalar nenhum tipo de software pirata em seu computador de trabalho;
- Usar o e-mail corporativo somente para assuntos inerentes ao trabalho;
- Comunicar à gerência de T.I. qualquer anomalia em seu computador;
- Comunicar à gerência de T.I. caso receba algum *spam* ou e-mail suspeito.

## 6 GOLPES, ATAQUES E CÓDIGOS MALICIOSOS

Abaixo serão comentados alguns tipos de golpes, ataques e códigos maliciosos mais comuns no meio corporativo e que podem ser encontrados no dia-a-dia de nossa empresa:

TELEINFRA
SERVIÇOS EM TELEINFORMÁTICA E INFRAESTRUTURA

- Furto de identidade: é o ato de uma pessoa se passar pela outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens

  indevidas. Os golpistas virtuais geralmente utilizam mecanismos como códigos maliciosos para obter os dados das vítimas
- Phishing: tipo de fraude que o golpista utiliza meios técnicos e a Engenharia Social. Ele ocorre por meio do envio de mensagens eletrônicas que possam ser parecidas com sites de bancos oficiais, ou até mesmo sites populares, procuram atrair atenção, seja por curiosidade ou pelo fato do usuário vir a obter vantagem financeira;
- Negação de Serviço (DoS e DDoS): Negação de serviço (*Denial of Service*), é uma técnica pelo qual o atacante utiliza um computador para retirar algum serviço do ar, a partir de várias requisições ao mesmo tempo, para uma mesma vítima. O objetivo destes ataques não é invadir nem coletar informações, mas sim tornar indisponível os serviços da vítima;
- *Spam:* Termo usado para se referir a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Este tipo de mensagem é usada para propagar os códigos maliciosos para um grande número de usuários da internet através de e-mail. Ele combina quase tudo que já falamos acima para infectar o computador do usuário;
- Vírus: programa ou parte de programa de computador, normalmente malicioso que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
- *Worm*: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias dele mesmo, mas sim pela execução direta de suas cópias.
- *Spyware*: programa projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros;

- Cavalo de Tróia (*Trojan*): programa que além de executar as funções para as quais foram projetados, também executa outras funções, geralmente maliciosas e sem conhecimento do usuário.

## 7 REFERÊNCIAS

Cartila de segurança para internet Cert.br:
http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf