

## IMPLEMENTAÇÃO DE FERRAMENTAS DE SEGURANÇA ENVOLVENDO PFSENSE, FREENAS, PSI E PCN<sup>1</sup>

**Pedro Henrique Moreira Braga**

Graduando do 8º período do curso de Sistemas de Informação do UNIPAM.  
E-mail: pedroh@unipam.edu.br

**Fabício Geraldo Araújo**

Professor do curso de Sistemas de Informação do UNIPAM.  
E-mail: fabricioa@unipam.edu.br

---

**RESUMO:** O presente projeto refere-se à mudança da segurança digital na empresa foco do presente projeto, através da construção de servidor de firewall e backup e da criação de documentações, que se deu por meio do Plano de Continuidade de Negócio e da Política de Segurança de Informação. A mudança implementada gerou alterações significativas na empresa, como a reformulação da infraestrutura de redes, novas documentações de segurança e continuidade de negócio.

**PALAVRAS-CHAVE:** Wifi. Segurança. Firewall. Backup.

**ABSTRACT:** The present project refers to the change of the digital security in the company focus of the present project, through the construction of firewall server and backup and the creation of documentation, which was given through the Business Continuity Plan and the Security Policy of Information. The implemented change generated significant changes in the company, such as the redesign of the network infrastructure, new security documentation and business continuity.

**KEYWORDS:** Wifi. Safety. Firewall. Backup.

---

### 1 INTRODUÇÃO

Atualmente a informação é arma estratégica em qualquer empresa e também é um recurso de vital importância nas organizações. A segurança da informação é um recurso que tem por finalidade proteger e também é uma forma de gestão. Nesse sentido, "a segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." [FERNANDA, S/ANO, p.1].

As ferramentas tecnológicas utilizadas hoje pelas empresas são, em sua maioria obsoletas, deixando o ambiente vulnerável a ataques e invasões de *hackers*. Além disso, há os colaboradores das empresas que têm uma parcela significativa nesse contexto e que, por isso, devem buscar melhorias no processo administrativo e de execução.

---

<sup>1</sup> Trabalho apresentado na área temática IV - Hardware e redes de computadores do XIV Congresso Mineiro de Empreendedorismo, realizado de 5 a 7 de novembro de 2018.

Diante desse cenário, o presente projeto de pesquisa tem como proposta a construção de ferramentas de proteção organizacional em rede, utilizando o PFSense como *firewall* e roteador, o sistema de *backup* de arquivos, o FreeNas, e também a elaboração de uma cartilha de segurança interna para os colaboradores, por meio de análise de Política de Segurança Da Informação (PSI) e Plano de Continuidade de Negócios (PCN).

Em nosso cotidiano, já não é mais novidade noticiários que informam roubo de dados, invasão de *hackers*, criação de novos vírus e vulnerabilidades em computadores. Em virtude disso, e devido a tentativas de invasão na área tecnológica da empresa em que o projeto será desenvolvido, foi identificado um cenário ideal para este projeto, visando o desenvolvimento de métodos e ferramentas de proteção à segurança digital.

Sendo assim, é relevante a adoção de ferramentas e métodos de segurança digital, para que problemas ligados a perda de dados, disponibilidade e integridade de informações em servidores, vulnerabilidades sistêmicas e também ações incorretas executadas em rede aberta por parte dos colaboradores da empresa, possam ser minimizados (solucionados).

Com isso, obtém-se um conjunto de processos e ferramentas que aumentam a segurança digital da empresa, o que possibilita de forma escalável a melhoria dos processos executados pelos colaboradores e a diminuição do risco de incidentes.

Dessa forma, espera-se que este estudo possa contribuir para o ambiente empresarial, com foco em potencializar a segurança interna e externa, bem como a política de segurança voltada para os colaboradores.

O objetivo geral deste projeto é implementar ferramentas de segurança interna e externa, como por exemplo, o PFSense na parte do servidor de *firewall* e roteador, o FreeNas sendo um servidor de *backup* de dados e uma cartilha de segurança interna, por meio de análise de PSI e PCN, para colaboradores da empresa. Através destas implementações iremos ter no cenário da empresa uma maior segurança de seus dados e ativos digitais.

Para se atingir o objetivo geral, apresentamos a seguir os seguintes objetivos específicos, os quais envolvem o estudo das ferramentas de segurança “PFSense e FreeNas”, análise dos processos executados diariamente na empresa em que o projeto será desenvolvido, implementação dos servidores e verificação de risco dos processos executados:

- Estudar sobre a ferramenta livre PFSense;
- Estudar sobre a ferramenta livre FreeNas;
- Estudar sobre desenvolvimento do PSI;
- Estudar sobre desenvolvimento do PCN;
- Analisar os processos executados diariamente na empresa;
- Implementar o servidor de *firewall* utilizando PFSense;
- Implementar o servidor de *backup* utilizando FreeNas;
- Implementar a documentação de risco com base no PSI e PCN;
- Elaborar a política de segurança;
- Implementar a cartilha de segurança.

## 2 REFERENCIAL TEÓRICO

A seguir será apresentado uma breve descrição dos tópicos e temáticas a serem estudados e implementados no projeto.

### 2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um assunto que está presente em nosso cotidiano cada vez mais, uma vez que se trata de um meio que requer extrema atenção devido as falhas que possam ocorrer, acarretando vários problemas. Em sua forma simplificada, a segurança da informação tem como responsabilidade garantir a integridade de dados e servidores, evitando que pessoas não autorizadas tenham acesso a eles. (TANENBAUM, 2002)

Outro aspecto que a segurança da informação abrange seria as vulnerabilidades e riscos, onde se tem como processo a análise sistêmica e o gerador de riscos, deixando seu sistema mais protegido. Entretanto, é errado afirmar que se tenha um sistema com total segurança, porém através dos métodos descritos as chances de invasões são minimizadas. (WINTER, 2000)

### 2.2 PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação auxilia em foco organizacional a forma como o meio sistêmico é utilizado, impondo processos e rotinas a serem seguidos para manter o ambiente com menor chance de brechas vulneráveis, fazendo com que colaboradores das empresas se mantêm seguros e deixando também o ambiente com maior segurança. (LUIZ, 2006)

### 2.3 PCN - PLANO DE CONTINUIDADE DE NEGÓCIOS

O plano de continuidade de negócios tem como foco analisar ameaças e riscos que possam vir a ocorrer, realizando métodos e processos a serem seguidos, deixando assim a organização preparada para possíveis incidentes e já com plano de ação para tais. A implementação do plano de continuidade de negócio geralmente é feita juntamente com setores e colaboradores da organização, analisando não somente os riscos sistêmicos, mas também de todos os processos a serem executados na empresa, com impactos operacionais e financeiros. (HOSNI, 2008)

### 2.4 PFSense

Pfsense é um sistema operacional de código aberto baseado em Unix FreeBSD adaptado para ser usado como um *firewall* e/ou roteador. O sistema em foco teve seu lançamento em 2004 e hoje a sua versão mais atual é a 2.4.2. É um projeto popular com mais de 1 milhão de downloads desde seu início, possuindo uma grande comunidade que apoia o projeto fazendo implementações e melhoria no seu código. (ANDRADE, 2013)

O Pfsense pode ser utilizado em pequenas, médias e grandes empresas, protegendo sua rede interna e disponibilizando acesso a dados de maneira segura, além de disponibilizar dados de utilização da rede. (ANDRADE, 2013)

## 2.5 FREENAS

O FreeNAS (NAS - Network Attached Storage) é um sistema operacional de armazenamento de dados em rede, de código aberto baseado em FreeBSD e lançado sob uma licença BSD de 2 cláusulas. Um NAS possui um sistema operacional otimizado para armazenamento e compartilhamento de arquivos. (IXSYSTEMS, 2017)

FreeNAS fornece uma interface de configuração gráfica baseada no navegador. Os protocolos de rede incorporados fornecem acesso de armazenamento a vários sistemas operacionais. Um sistema de *plugin* é fornecido para ampliar os recursos internos, instalando *software* adicional. (IXSYSTEMS<sup>2</sup>, 2017).

## 3 METODOLOGIA

A presente pesquisa foi desenvolvida por meio de uma pesquisa bibliográfica através de livros e tutoriais de autores na área de segurança digital, de uma pesquisa de campo na empresa e de uma pesquisa documental, verificando documentos relacionados as ferramentas citadas. Os procedimentos iniciais foram baseados em análise de requisitos, processos e infraestrutura de rede já composta pela empresa. Foram implementadas ferramentas e métodos que contribuiriam para a segurança digital na empresa.

As análises foram realizadas através de visitas a empresa, monitorando os processos e rotinas dos colaboradores, bem como *softwares* utilizados diariamente. A infraestrutura foi analisada juntamente com o técnico em Tecnologia da Informação (TI) responsável pela tal.

O processo de implementação foi realizado após análises, focando as ferramentas como o Pfsense na restrição de sites pornográficos e maliciosos, bloqueio de portas, e a monitoração da rede *wireless*, o FreeNas no arquivamento de dados, o PSI na mudança da política de segurança da empresa, e por fim, o PCN, no plano de continuidade de negócio em relação ao grau de riscos de cada processo e ambiente. Além disso, os servidores foram implementados em ambientes virtuais para testes, passando posteriormente para ambientes físicos. As cartilhas de segurança foram descritas conforme a família das ISOs 27000<sup>3</sup> referentes à gestão de segurança e de acordo com as normas da empresa. Após serem finalizadas, será repassado aos colaboradores da empresa por meio de uma cartilha ou palestra sobre políticas e normas de segurança no âmbito da segurança digital.

<sup>2</sup> Disponível em: <http://doc.freenas.org/11/freenas.html>. Acesso em: 10/03/2018

<sup>3</sup> Disponível em: <https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html> Acesso em: 20/08/2018

#### 4 DESENVOLVIMENTO E RESULTADOS

O estudo sobre as ferramentas citadas no projeto levou ao aprofundamento sobre técnicas de segurança digital, verificando sua grande importância para empresas e organizações, podendo deixá-las com maior proteção no âmbito digital.

O servidor de *firewall* com PFSense (Apêndice I) foi implementado conforme o cenário repassado pela empresa, o qual os usuários tiveram alguns impedimentos como o acesso a sites pornográficos, sites de *torrent*, realizar download de *torrents*, acesso a sites maliciosos, acesso direto ao modem e ao próprio *firewall*, também se teve bloqueio de portas e o monitoramento de acesso, verificando sites visitados que podem ser futuramente bloqueados.

O servidor de *backup* com FreeNas (Apêndice II) foi implementado próximo ao cenário da empresa em questão, utilizando-se em suas configurações de compartilhamento o sistema operacional que a empresa possui, o Windows. O servidor teve um desempenho satisfatório, o qual se teve transferências de arquivos de maneira prática, segura e rápida, possibilitando a instalação futura do mesmo em ambiente empresarial.

Com base na análise de riscos de acordo com os critérios de criticidade, probabilidade, impacto, e visitas juntamente com o técnico em TI da empresa, verificando pontos de melhorias, como por exemplo: energia, internet, inundações, vazamentos de água, poeira, interrupção de *backup*, VPN, acessos não autorizados, vírus, incêndio, falha em equipamentos, local inapropriado para equipamentos e computadores obsoletos o PCN foi escrito (Apêndice IV). Também foram inseridos no PCN níveis de impacto e severidade, probabilidade de ocorrência, ação, consequências, gatilhos, resposta ao risco, tempo máximo de resposta e melhorias.

O PSI (Apêndice III) foi descrito com o foco no cotidiano dos colaboradores da empresa, repassando informações de como se portar no ambiente digital, verificando pontos como: confidencialidade, integridade, disponibilidade, boas práticas de senhas, boas práticas para uso de redes sociais, boas práticas para o uso do e-mail, boas práticas de navegação na internet e como se portar ao ser infectado por vírus, deixando o colaborador informado sobre as melhores práticas de segurança digital em ambiente empresarial.

Os resultados obtidos foram conhecimento de técnicas referentes ao PCN e ao PSI, conhecimento em ferramentas *open source* (ferramentas de código aberto/livre), como o FreeNas e o PFSense. No âmbito da empresa, se teve um ganho de documentação referente ao plano de continuidade de negócios onde durante o projeto a empresa investiu na infraestrutura de rede, mostrando sua preocupação nesta área, já a política de segurança interna que estava obsoleta, foi alterada com a criação de uma nova através deste projeto.

#### 5 CONCLUSÃO

Inicialmente a empresa demonstrava alguns pontos de vulnerabilidade, o qual poderia ser utilizado por *hackers* para obtenção de dados sigilosos e realização de

fraudes, visando este cenário as ferramentas e métodos utilizados no projeto, foram implementados de acordo com as necessidades demandadas da empresa.

Durante a realização do projeto, alguns entraves aconteceram como, por exemplo, a falta de conhecimento sobre as ferramentas PFSense, FreeNAS, PSI e o PCN. Sendo assim, boa parte do tempo foi voltada para aprendizado e aperfeiçoamento de técnicas para construção dos servidores com o foco no cenário da empresa, na construção do PCN, verificando as normas referentes à segurança digital, e na elaboração do PSI, que, por sua vez, foi buscado boas práticas de utilização do meio digital em ambiente empresarial.

Em ocasiões futuras, os servidores como o PFSense e o FreeNas podem ser implantados fisicamente na empresa, auxiliando-os no quesito segurança, disponibilidade e integridade de dados se tratando somente da aprovação da diretoria e do técnico em TI. Já o PCN e o PSI podem ser alterados de acordo com as mudanças no cenário da empresa, ficando com seu ambiente interno e externo protegidos, além de evitar falhas de segurança digital e garantir a continuidade do negócio.

Com servidores e documentações implantados na empresa, espera-se aumentar sua segurança digital, garantindo níveis de confiabilidade e reduzindo risco de ocorrência de incidentes destinados a essa área.

## REFERÊNCIAS

ANDRADE, Márcio. **Conhecendo e configurando o PFSense**, 2015. Disponível em: <<http://sejalivre.org/conhecendo-configurando-pfsense/>>. Acesso em: 18 fev. 2018.

FERNANDA, Adrielle. **Segurança Da Informação**. [s/ano]. Disponível em: <[http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno\\_adrielle\\_fernanda\\_seguranca\\_da\\_informacao.pdf](http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf)>. Acesso em: 23 fev. 2018.

HOSNI, Jorge. **PLANO DE CONTINUIDADE de negócios aplicado à segurança da informação**, 2008. Disponível em: <<http://www.lume.ufrgs.br/bitstream/handle/10183/15974/000695265.pdf>>. Acesso em: 18 fev. 2018

IXSYSTEMS. **GUIA DO USUÁRIO 11.1**, 2017. Disponível em: <<http://doc.freenas.org/11/freenas.html>>. Acesso em: 18 fev. 2018.

LUIZ, João. **SEGURANÇA da informação - uma abordagem social**, 2006, Disponível em: <<http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf>>. Acesso em: 18 fev. 2018

TANENBAUM, Andrew. **Computer Networks**, Fourth Edition, Estados Unidos, Prentice Hall, 2002. 960

WINTER, Débora. **SEGURANÇA na internet**, 2000, Disponível em: <<https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/78962/170924.pdf?squence=1&isAllowed=y>>. Acesso em: 18 fev. 2018

## APÊNDICE I - Servidor Firewall

Na Figura I são apresentadas informações gerais do sistema de firewall como nome, tipo de sistema, interfaces, serviços ativos/desabilitados, tipo de CPU, versão do sistema, BIOS, tempo de atividade, servidor DNS, carga média, utilização de CPU e memória.

**Figura I: Informações gerais do sistema de firewall**

The screenshot shows the pfSense web interface. The top left corner displays a warning icon and the text "Não seguro" next to the URL "https://10.10.10.1".

**Informação do sistema**

- Nome:** pfSense.localdomain
- Sistema:** pfSense, ID do dispositivo Netgate: 984252906e0117c2eabc
- BIOS:** Fornecedor: American Megatrends Inc., Versão: 0402, Data de lançamento: Wed May 20 2009
- Versão:** 2.4.2-RELEASE (amd64), construído em Mon Nov 20 08:12:56 CST 2017, FreeBSD 11.1-RELEASE-p4. Versão 2.4.3\_1 está disponível. Informação de versão atualizada em Wed Sep 12 14:10:49 UTC 2018.
- Tipo de CPU:** Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz, 2 CPUs: 1 package(s) x 2 core(s), AES-NI CPU Crypto: No
- Tempo de atividade:** 3 Days 02 Hours 02 Minutes 27 Seconds
- Data/hora atuais:** Wed Sep 12 14:12:02 UTC 2018
- Servidores DNS:** 127.0.0.1, 208.67.222.222, 208.67.220.220
- Última alteração de configuração:** Mon Sep 10 0:00:28 UTC 2018
- Tamanho da tabela do estado:** 0% (144/404000) [Mostrar estados](#)
- Uso MBUF:** 0% (770/251124)
- Carga média:** 0.16, 0.22, 0.22
- utilização do CPU:** 4%
- Utilização da Memória:** 19% of 4042 MiB

**Interfaces**

- WAN:** 100baseTX <full-duplex>, 192.168.1.50
- LAN:** 100baseTX <full-duplex>, 10.10.10.1

**pfBlockerNG**

MaxMind: Last-Modified: Tue, 03 Jul 2018 21:24:23 GMT

Alias	Contagem	Pacotes	Atualizado
pfB_DShild_list_v4	2.627	0	Sep 12 00:00:29 ↑ (2)
pfB_binarydefense_v4	8.153	0	Sep 12 00:00:29 ↑ (2)
pfB_list_bambenekconsultin_v4	113	0	Sep 12 00:00:29 ↑ (2)

**Status dos Serviços**

Serviço	Descrição	Ação
c-icap	ICAP Interface for Squid and ClamAV Integration	🔴
clamd	ClamAV Antivirus	🔴
dhcpcd	Serviço DHCP	🟢
dpinger	Daemon de Monitoramento do Gateway	🟢
lightsquid_web	Lightsquid Web Server	🟢
ntopng	ntopng Network Traffic Monitor	🟢
ntpd	Sincronização de relógio NTP	🟢
pfB_dnsbl	pfBlockerNG DNSBL service	🔴
pfB_filter	pfBlockerNG firewall filter service	🟢
squid	Squid Proxy Server Service	🟢
squidGuard	Proxy server filter Service	🔴
syslogd	Daemon do sistema de log	🟢
unbound	DNS Resolver	🟢

Fonte: Elaborado pelo autor

A Figura II apresenta as regras de bloqueio do servidor de firewall, em específico, a regra de bloqueio a sites de torrentes e pornográficos e ao acesso do firewall, assim como a de liberação de rede interna à internet.



**Figura II: Regras de bloqueio do servidor de firewall**

As alterações foram aplicadas com sucesso. As regras do firewall estão agora sendo recarregadas em segundo plano.  
Monitorar o progresso de recarregamento do filtro.

Flutuante WAN LAN

**Regras (Arraste para mudar a ordem)**

Estados	Protocolo	Origem	Porta	Destino	Porta	Gateway	FILA	Agenda	Descrição	Ações
<input checked="" type="checkbox"/>	0/468 B	IPv4 TCP	*	Bloqueio_de_sites_de_torrents	*	*	nenhum			
<input checked="" type="checkbox"/>	0/5 KIB	IPv4 TCP	*	Sites_porno_block	*	*	nenhum			
<input checked="" type="checkbox"/>	0/1 KIB	IPv4 TCP	Bloqueio_Pfsense_rede_DHCP	IP_DE_ACESSO_PFSENSE	443 (HTTPS)	*	nenhum			
<input checked="" type="checkbox"/>	94 /17.19 GIB	IPv4 *	LAN net	*	*	*	nenhum		Default allow LAN to any rule	

Fonte: Elaborado pelo autor

A Figura III apresenta o serviço de listas do servidor de firewall contendo sites maliciosos. As listas são definidas por meio da frequência de atualização do seu conteúdo, do estado de ativação/desativação e da ação a ser tomada referente ao conteúdo da lista.

**Figura III: Serviço de listas do servidor de firewall**

Firewall / pfBlockerNG / IP / IPv4

Geral IP DNSBL Atualizar Reports Feeds Logs Sync

IPv4 IPv6 GeolIP Reputation

**IPv4 Summary (Drag to change order)**

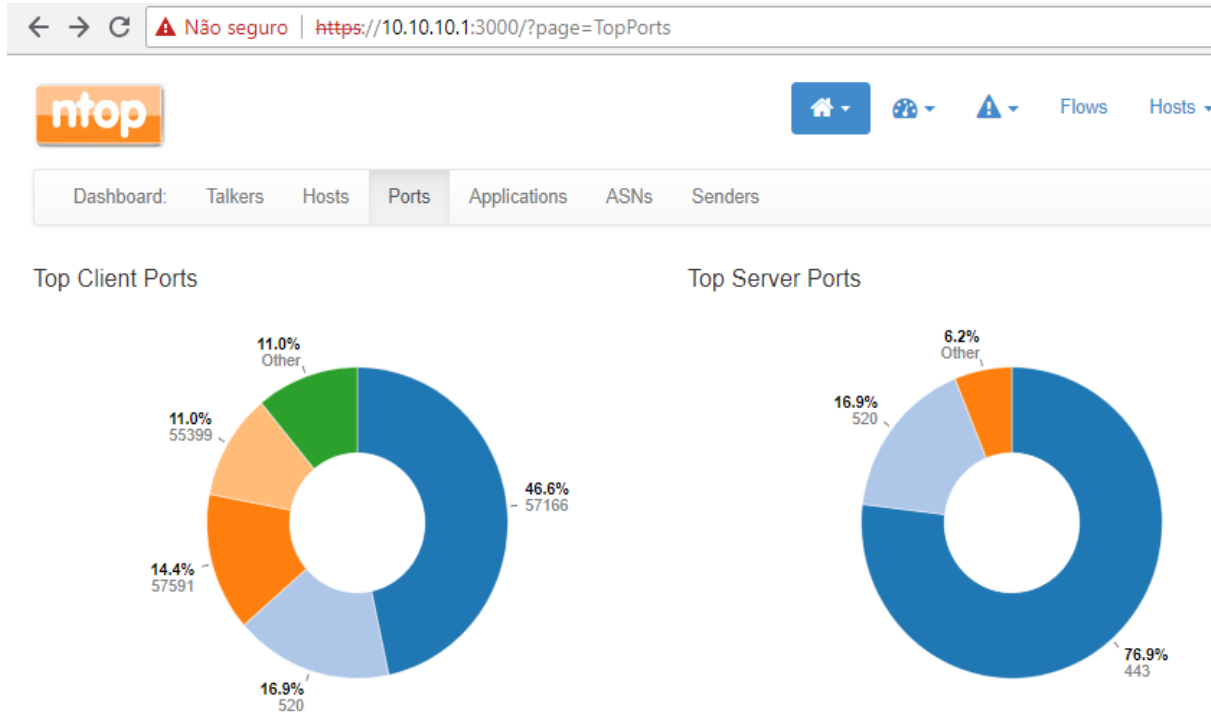
Nome	Descrição	Ação	Frequency	Entrando	Ações
list_bambenekco...	BLACK LIST IP 3...	Deny Both	Every 3 hours	Ativado	
DShild_list	black list DSHI...	Deny Both	Once a day	Ativado	
binarydefense	Black list IP S...	Deny Both	Every hour	Ativado	

Fonte: Elaborado pelo autor

A Figura IV apresenta um gráfico que mostra o serviço do servidor de firewall, Ntop. O gráfico indica as portas mais acessadas pelos serviços utilizados por clientes e servidor.



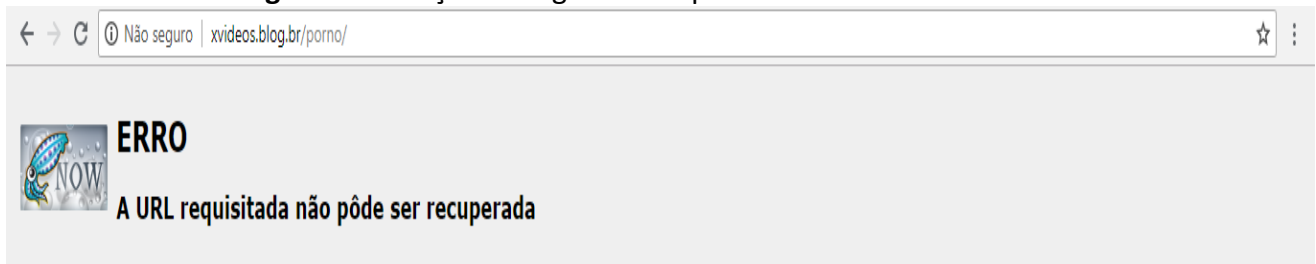
**Figura IV: Portas mais acessadas**



Fonte: Elaborado pelo autor

A Figura V apresenta a ativação da regra de bloqueio do servidor de firewall ocasionado pelo acesso negado ao site pornográfico demonstrado na URL.

**Figura V: Ativação da regra de bloqueio do servidor de firewall**



O seguinte erro foi encontrado ao tentar recuperar a URL: <http://xvideos.blog.br/porno/>

Acesso negado.

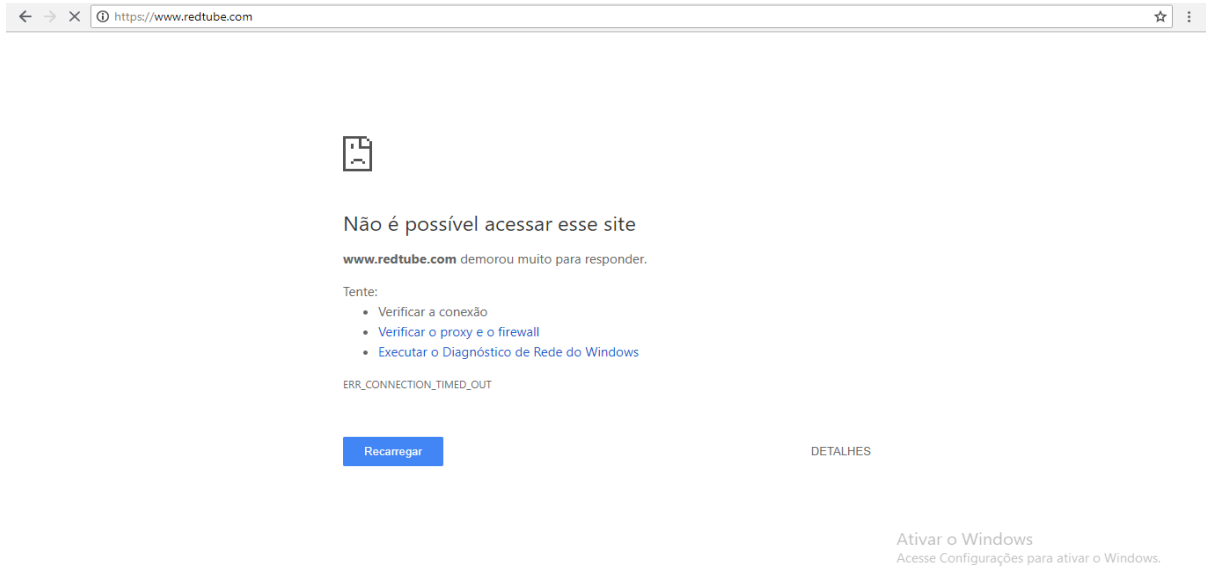
A configuração do controle de acesso impede que sua requisição seja permitida neste momento. Por favor, contate seu provedor de serviço se você acha que isso está incorreto.

Seu administrador do cache é [admin@localhost](mailto:admin@localhost).

Fonte: Elaborado pelo autor

A Figura VI apresenta a ativação da regra de bloqueio do servidor de firewall ocasionado pelo acesso negado ao site pornográfico demonstrado na URL.

**Figura VI:** Ativação da regra de bloqueio do servidor de firewall



**Fonte:** Elaborado pelo autor

## APÊNDICE II - Servidor FreeNAS

A Figura I apresenta a interface gráfica do servidor de backup demonstrando o espaço de armazenamento destinado à aplicação Windows, que representa 7.9 GB para backup de arquivos.

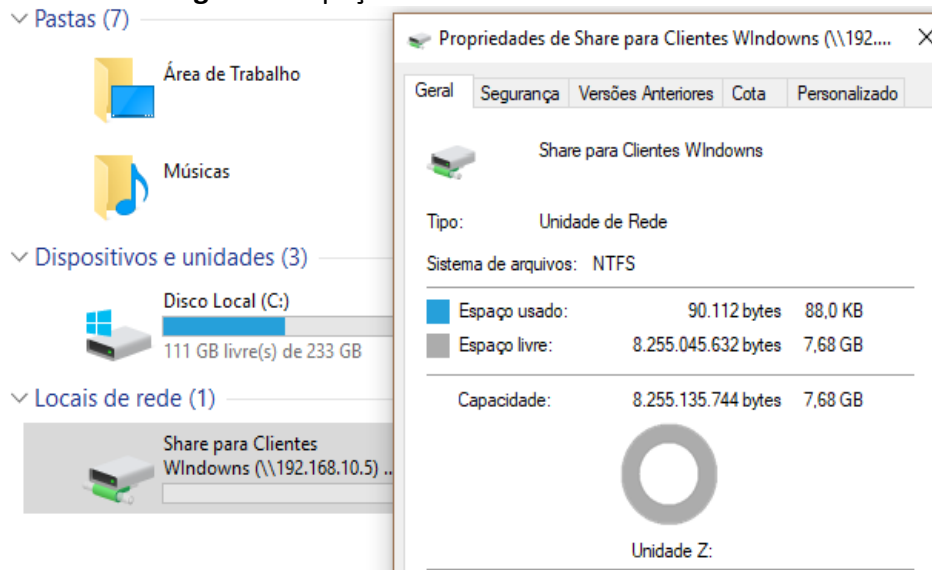
**Figura I:** Interface gráfica do servidor de backup

Name	Used	Available	Compression	Compression Ratio	Status	Readonly	Comments
pool-data01	1.4 MiB (0%)	7.9 GiB	-	-	HEALTHY		
pool-data01	5.0 GiB (65%)	2.7 GiB	lz4	7.42x	-	inherit (off)	
share_windows	5.0 GiB (39%)	7.7 GiB	lz4	1.00x	-	inherit (off)	Dataset para Share Windows

Fonte: Elaborado pelo autor

A Figura II apresenta o espaço de armazenamento Windows em máquina cliente, demonstrando o tamanho disponível para armazenamento de dados, sendo de 7,68 GB livres.

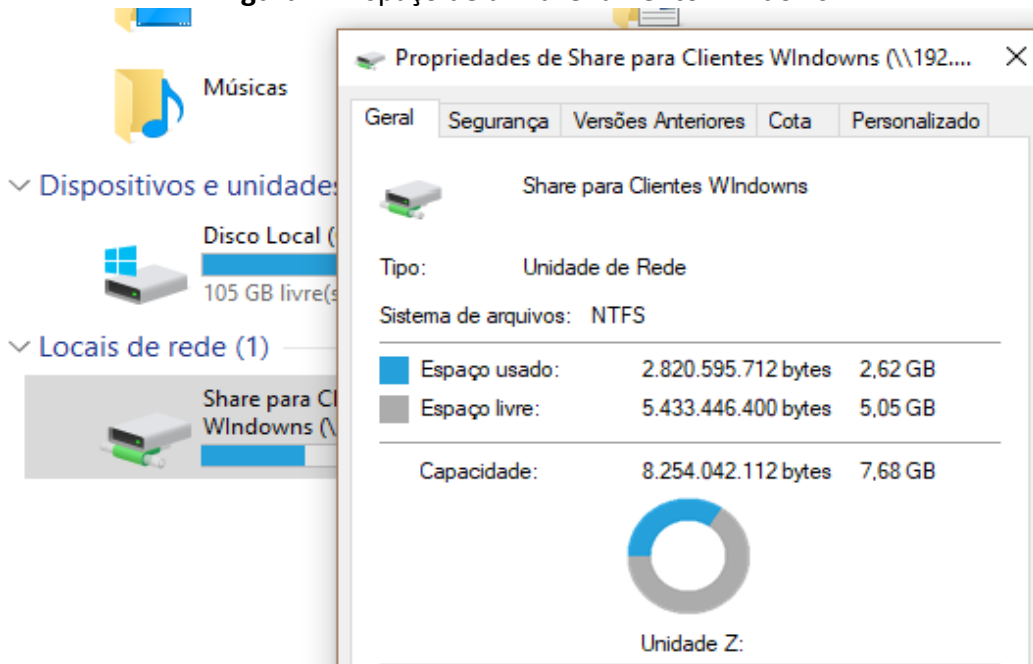
**Figura II: Espaço de armazenamento Windows**



**Fonte:** Elaborado pelo autor

A Figura III apresenta o espaço de armazenamento Windows em máquina cliente demonstrando o tamanho disponível para armazenamento de dados, após a inserção de arquivos, de 5,05 GB livres.

**Figura III: Espaço de armazenamento Windows**



Fonte: Elaborado pelo autor

### APÊNDICE III - Política de Segurança de Informação - PSI

A Figura I apresenta a Política de Segurança de Informação que traz as boas práticas de comportamento no âmbito digital da empresa em que o projeto foi desenvolvido e informações relevantes à empresa e ao posicionamento do colaborador em relação a ações tomadas em ambiente digital. A Política de Segurança de Informação foi aprovada e assinada pelo técnico em TI e sócio proprietário da empresa.

**Figura I: Política de Segurança de Informação**

Política de Segurança de Informação - PSI

**Colaborador**

O conteúdo desta cartilha tem como objetivo compartilhar alguns conceitos relacionados ao tema Segurança da Informação. Além de dicas de como tratar os recursos e as informações corporativas com que lidamos em nosso dia a dia, este material busca enfatizar a responsabilidade de todos os funcionários, estagiários, terceiros, parceiros e visitantes que acessem informações da DI

Proteger as informações da empresa para a qual trabalhamos é um dever de todos nós!

Esperamos que este guia ajude a esclarecer eventuais dúvidas e possa orientá-los sobre como exercer o papel de "colaborador-chave" para a Segurança da Informação

**Segurança da Informação**

Os três pilares da segurança da informação são:

- **Confidencialidade:** Limita o acesso à informação somente a pessoas devidamente autorizadas.
- **Integridade:** Garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo o controle de mudanças e a garantia do seu ciclo de vida (criação, manutenção e destruição).
- **Disponibilidade:** Garante que a informação esteja sempre disponível para o uso legítimo

**Fonte:** Elaborado pelo autor


**APÊNDICE IV - Plano de Continuidade de Negócio - PCN**

A Figura I apresenta o Plano de continuidade de negócio desenvolvido para o ambiente digital da empresa em que o projeto foi desenvolvido. Há no Plano em foco informações como os riscos, consequências, probabilidade de ocorrência, impacto, severidade, ação, resposta aos riscos, gatilho, tempo de resposta e melhorias. O PCN foi aprovado e assinado pelo técnico em TI da empresa e sócio proprietário.

**Figura I: Plano de Continuidade de Negócio**

Planilha de Riscos

PLANILHA DE CONTINUIDADE DE NEGÓCIO									
Descrição do Risco	Consequências	Probabilidade de Ocorrência	Impacto	Severidade	Ação	Gatilho	Resposta ao Risco	Tempo máximo de resposta	Melhorias
Interrupção do funcionamento correto do condicionador de ar da sala dos servidores	Superaquecimento de computadores e servidores. Danos aos servidores e computadores. Interrupção do funcionamento dos computadores e servidores	Média	Alto	Alta	Melhorar	Falha no computador ou servidor; Interrupção do funcionamento do computador ou servidor.	Acionar o reparo do condicionador de ar	3 horas	Monitoramento contínuo; Manutenção preventiva; Condicionador de ar reserva
Interrupção da internet	Falha em comunicação em rede com filiais; Falha em consulta de dados externos; Falha no envio de informações a clientes; Falha no armazenamento de dados.	Baixa	Alto	Média	Melhorar	Interrupção; Falha no envio de pacotes; Envio de pacotes abaixo do controlado	Acionar o suporte do provedor de internet; Acionar o responsável pela TI	1 hora	Plano de suporte melhor
Interrupção da energia	Desligamento inesperado de computadores, servidores e todos os equipamentos eletrônicos	Baixa	Alto	Média	Melhorar	Interrupção; Piques de energia; Alta/Baixa voltagem entregue	Acionar a fornecedora de energia; Acionar um electricista.	1 hora	Aquisição de notebooks com maior carga de baterias
Acesso não autorizado aos servidores	Roubo de dados; Interrupção de serviços; Perda de Integridade dos dados; Indisponibilidade de acesso aos servidores	Média	Alto	Alta	Melhorar	Perda de acesso; Falha em funcionalidades; Visualização de usuários não autorizados	Acionar o responsável pela TI	1 hora	Monitoramento constante; Política de criação de senha fortes; Ambiente próprio para servidores; Atualização de servidores; Ambiente restrito para servidores
Interrupção de backup	Perda de dados;	Média	Alto	Alta	Melhorar	Perda de dados em servidor; Exclusão de dados em servidor; Perda do servidor	Acionar o responsável pela TI	1 hora	Possuir mais de um meio de backup; Monitorar o backup; Atualizar servidor de backup; Restringir o acesso ao servidor de backup;
Interrupção da VPN	Perda de comunicação com filiais; Perda de acesso a dados	Média	Alto	Alta	Melhorar	Interrupção de comunicação com filiais	Acionar o responsável pela TI	1 hora	Monitoramento constante;
Interrupção/Falha da Routerboard - RB-Firewall	Interrupção de internet; Perda de comunicação com filiais; Perda de acesso dos dados; Perda de proteção dos dados; Perda da VPN	Média	Alto	Alta	Melhorar	Interrupção de comunicação com filiais; Interrupção de internet; Roubo de dados;	Acionar o responsável pela TI	1 hora	Monitoramento constante; Backup de configurações realizado constantemente
Local Inapropriado dos servidores	Dano aos servidores; Manutenção dificultada; Refrigeração pouco eficaz; Acesso a terceiros.	Média	Alto	Alta	Melhorar	Incidente; Falha no funcionamento; Manutenção longa.	Acionar o responsável pela TI	1 hora	Espaco próprio para servidores; Equipamentos apropriados para alojar o servidores
Computadores antigos	Falha em hardware; Incompatibilidade com sistemas operacionais e programas atualizados	Baixa	Médio	Baixa	Melhorar	Defeito em hardware; Incompatibilidade de instalação de novos Sistemas Operacionais.	Acionar o responsável pela TI	24 horas	Troca de computadores antigos para novos; Alocação de computadores antigos para serviços de pouco impacto.
Cabos de rede próximo a rede elétrica	Perda de envio de dados; Perda de desempenho do cabo de rede;	Média	Médio	Média	Melhorar	Falha de acesso à internet; Perda de acesso à internet.	Acionar o responsável pela TI	24 horas	Passagem dos cabos de rede em trajeto próprio e com distância da rede elétrica
Rede wifi visitante sem proteção	Fácil acesso de hackers; Fácil acesso a usuários conectados na rede;	Alta	Alto	Alta	Melhorar	Roubo de dados; Injeção de vírus aos usuários	Acionar o responsável pela TI	1 hora	Configuração de firewall; Instalação de firewall; Monitoramento do firewall.
Desorganização de cabos	Manutenção dificultada; Perda de desempenho	Média	Alto	Alta	Melhorar	Perda de acesso a internet; Tempo maior para manutenção	Acionar o responsável pela TI	24 horas	Organização dos cabos de rede
Acesso não autorizado a máquinas dos departamentos	Roubo de dados; Interrupção de serviços de computadores; Interrupção de serviços da rede;	Alta	Alto	Alta	Melhorar	Perda de acesso na máquina; Roubo de dados da máquina; Perda de acesso a outras máquinas.	Acionar o responsável pela TI	1 hora	Reformulação da política de senhas e logoff ao utilizar máquinas; Desligamento de máquinas após expediente; Política de acesso a sites desconhecidos; Política de download de arquivos; Política de uso de pen drive
Windows desatualizado	Fácil acesso de hackers; Roubo de dados; Interrupção de serviços de computadores; Interrupção de serviços da rede	Alta	Alto	Alta	Melhorar	Perda de acesso na máquina; Roubo de dados da máquina; Perda de acesso a outras máquinas.	Acionar o responsável pela TI	1 hora	Atualização do Windows para versão atual e com suporte; Política de atualização de pacotes
Vírus em computadores	Interrupção de serviços de computadores; Roubo de dados; Fácil acesso a hackers; Interrupção de serviços da rede	Alta	Alto	Alta	Melhorar	Perda de acesso aos computadores; Roubo de dados dos computadores; Perda de dados nos processos dos computadores	Acionar o responsável pela TI	1 hora	Política de uso correto das máquinas; Política de senhas e logoff ao utilizar máquinas; Desligamento de máquinas após expediente; Política de acesso a sites desconhecidos; Política de download de arquivos; Política de uso de pen drive
Incêndio	Queima de computadores e servidores; Interrupção de serviços da rede; Queima de cabos de rede	Baixa	Alto	Média	Melhorar	Propagação de fogo	Acionar os Bombeiros Acionar um Engenheiro Acionar o Responsável pela TI	1 hora	Política de treinamento contra incêndio oferecida aos colaboradores; Possuir extintores de incêndios nos departamentos; Possuir avaliação de risco por parte dos bombeiros
Poeira	Falha de hardware em computadores; Interrupção de serviços de computadores; Interrupção de serviços da rede	Baixa	Alto	Média	Melhorar	Falha em hardware na máquina	Acionar o responsável pela TI	1 hora	Possuir ambiente limpo e arejado para servidores; Limitar periódica de máquinas
Vazamento de Água	Interrupção de serviços de servidores e computadores; Interrupção de serviços da rede; Perda de desempenho na rede; Perda de acesso dos dados; Perda de computadores e servidores	Baixa	Alto	Média	Melhorar	Baixo desempenho da rede; Marcas de vazamento de água;	Acionar o responsável pela TI Acionar um bombeiro	3 horas	Possuir estrutura anti vazamentos; Possuir monitoramento de estrutura;
Acesso não autorizado a documentos	Roubo de dados; Perda de Integridade de dados; Indisponibilidade de acesso aos dados	Média	Alto	Alta	Melhorar	Perda de documentos	Acionar o responsável pela TI Acionar o responsável pelo departamento	1 hora	Possuir local adequado de armazenamento de documentos; Possuir documentação em nuvem; Possuir restrição ao acesso de documentos
Indisponibilidade do acesso ao site da DITRASA	Perdas de acesso de usuários; Perda de vendas	Baixa	Médio	Baixa	Melhorar	Falha no acesso ao site	Acionar o responsável pela TI Acionar o servidor de hospedagem do site	1 hora	Monitoramento de disponibilidade do acesso ao site
Inundação	Perda de servidores e computadores; Indisponibilidade de acesso dos dados; Perda de desempenho da rede; Perda de documentos	Baixa	Alto	Média	Melhorar	Aumento de poças de água dentro da empresa	Acionar o responsável pela TI Acionar um Engenheiro Acionar um Bombeiro	1 hora	Monitoramento de infraestrutura da empresa



Fonte: Elaborado pelo autor