

**FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO**

Victor Hugo Benjamin Vieira

**MELHORIA DO NÍVEL DE SEGURANÇA DA INFORMAÇÃO DE
UMA ESCOLA TÉCNICA**

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO

Victor Hugo Benjamin Vieira

**MELHORIA DO NÍVEL DE SEGURANÇA DA INFORMAÇÃO DE
UMA ESCOLA TÉCNICA**

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Professor Esp. Ricardo Kiyoshi Batori.

Área de concentração:
Segurança da Informação

Americana, SP

2016

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

V719m VIEIRA, Victor Hugo Benjamin
 Melhoria do nível de segurança da informação
 de uma escola técnica. / Victor Hugo Benjamin Vieira. –
Americana: 2016.
 49f.

 Monografia (Curso de Tecnologia em Segurança
da Informação). - - Faculdade de Tecnologia de
Americana – Centro Estadual de Educação Tecnológica
Paula Souza.

 Orientador: Prof. Esp. Ricardo Kiyoshi Batori

 1. Segurança em sistemas de informação I.
BATORI, Ricardo Kiyoshi II. Centro Estadual de
Educação Tecnológica Paula Souza – Faculdade de
Tecnologia de Americana.

CDU: 681.518.5

VICTOR HUGO BENJAMIN VIEIRA

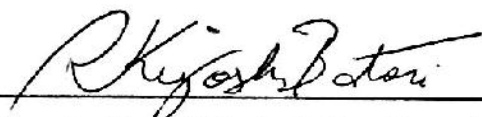
**MELHORIA DO NÍVEL DE SEGURANÇA DA INFORMAÇÃO DE UMA
ESCOLA TÉCNICA**

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação.

Americana, 08 de Dezembro de 2016.

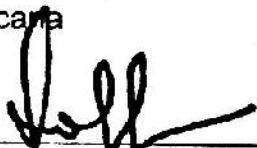
Banca Examinadora:



Ricardo Kiyoshi Batori (Presidente)
Especialista
Fatec Americana



Maria Cristina Luz Fraga Moreira Aranha (Membro)
Mestre
Fatec Americana



Renato Kraide Soffner (Membro)
Doutor
Fatec Americana

AGRADECIMENTOS

Primeiramente, gostaria de agradecer à Escola Técnica utilizada como base desse estudo, por ceder suas instalações para meses de análise do ambiente e implementação dos controles de segurança.

À FATEC Americana, por oferecer a base do conhecimento necessário para a realização das atividades descritas neste trabalho.

Ao meu eterno chefe Luciano, por me ensinar com muita paciência e postura que o cargo exige, tudo o que hoje chamo de conhecimento.

Ao professor orientador Ricardo, que apesar do pouco tempo, pode me direcionar ao caminho a ser seguido neste trabalho.

A todos os funcionários da instituição que fiz estágio, pelo acolhimento, troca de experiência e cobranças que fazem parte do que sou hoje.

DEDICATÓRIA

À minha queridíssima mãe que sempre teve a força, coragem e amor que me impulsionaram até aqui, e que eu espero um dia ter ao menos um terço. E a minha namorada que está comigo em todos os momentos e me deu estabilidade emocional para chegar até aqui.

RESUMO

Trazendo uma abordagem direta à segurança da informação, o trabalho apresenta o caminho prático percorrido para a implementação de melhorias de segurança em uma escola – situada na região de Campinas, que atua oferecendo cursos técnicos e ensino médio -, desde o entendimento dos conceitos da área, situando a atividade de foco, e o campo de atuação especificamente, a análise dos riscos. Analisando o ambiente cuidadosamente, foi possível identificar os ativos importantes para a abordagem, as vulnerabilidades existentes sobre estes ativos, os controles já aplicados que afetam diretamente a probabilidade e consequência de um risco e as ameaças que poderiam explorar as vulnerabilidades. Com isso foi elaborado um plano de tratamento. Este, forneceu conscientização dos riscos e a definição do que era prioridade e o que poderia ser adiado ou aceito. Partindo desse ponto foi possível sugerir as melhorias de fato. Um *firewall* foi implantado e todo esse processo foi acompanhado desde a instalação até os testes finais que demonstram a eficácia do mesmo, reduzindo por fim a probabilidade e consequência dos riscos.

Palavras Chave: Segurança da Informação; Análise de Riscos; *Firewall*;

ABSTRACT

Bringing a direct approach to information security, the paper presents a practical path taken to implement security in a school - in the region of Campinas, which operates offering technical courses and high school -, improvements from the understanding of the concepts of the area, locating the focus activity and the field of action, specifically the analysis of risks. Analyzing carefully the environment it was possible to identify the assets that are important to the approach, the vulnerabilities that exist on it, the controls already applied that directly affect probability and consequence of a risk and the threats that could exploit vulnerabilities. Thereby, a treatment plan was elaborated. It provided awareness of the risks and a definition of what was a priority and what could be postponed or accepted. Starting from that point, it was possible to suggest improvements. A firewall was deployed and the entire process was followed from the installation to the final tests that demonstrate the effectiveness of the firewall, ultimately reducing probability and consequence of the risks.

Key Words: Information Security; Risks Analysis; Firewall.

SUMÁRIO

1 INTRODUÇÃO	12
2 SEGURANÇA DA INFORMAÇÃO E ANÁLISE E GESTÃO DE RISCOS	13
3 ANÁLISE DE RISCO DE SEGURANÇA DA INFORMAÇÃO	17
3.1 ATIVOS.....	17
3.1.1 Sistema acadêmico.....	18
3.1.2 Dispositivos de rede.....	18
3.1.3 Computadores	19
3.1.4 Servidores.....	19
3.2 IDENTIFICAÇÃO DAS VULNERABILIDADES	19
3.2.1 Falta de maturidade e administração inadequada	20
3.2.2 Exposição, falta de controle, e má distribuição	21
3.2.3 Acesso permissivo e pouco controle sobre as ações	21
3.2.4 Hardware inadequado, exposição, ausência de controles.....	22
3.3 CONTROLES EXISTENTES.....	23
3.4 IDENTIFICAÇÃO DAS AMEAÇAS.....	24
3.5 CRITÉRIOS DE ESTIMATIVA E CÁLCULO DOS RISCOS.....	25
3.6 TRATAMENTO DOS RISCOS	29
4 IMPLANTAÇÃO DE CONTROLES	33
5 TESTES E RESULTADOS.....	41
6 CONSIDERAÇÕES FINAIS	45
REFERÊNCIAS.....	46

LISTA DE FIGURAS

- Figura 1 - Conceito de Segurança da Informação
- Figura 2 - Atividade de tratamento do risco
- Figura 3 - Diagrama de proposta da estrutura de rede
- Figura 4 - Tela principal do *Netdeep Firewall*
- Figura 5 - Configuração de Política de Grupo no Windows Server 2008
- Figura 6 - Menu de seleção para restrição de navegadores
- Figura 7 - Seleção de categorias para bloqueio no *proxy*
- Figura 8 - Regras atribuídas automaticamente após definição das interfaces
- Figura 9 - Menu de seleção para criação de regras no *firewall*
- Figura 10 - Bloqueio a site de conteúdo de jogos
- Figura 11 - Bloqueio a site de conteúdo pornográfico
- Figura 12 - Registro dos Bloqueios realizados pelo *proxy*

LISTA DE TABELAS

Tabela 1 - Probabilidade dos riscos

Tabela 2 – Consequência dos riscos

Tabela 3 - Cálculo e registros dos riscos

Tabela 4 – Riscos Residuais

1 INTRODUÇÃO

Com a evolução da tecnologia, surgem novas dificuldades para a segurança da informação e para que a abordagem do tratamento de prevenção aos perigos seja adequada é preciso entender alguns conceitos que auxiliem no entendimento do cenário lidado. Um destes conceitos é a análise dos riscos que oferece uma visão clara do âmbito de atuação como um todo e direciona os recursos para atividades fundamentais ao negócio, oferecendo melhorias significativas para as atividades desenvolvidas no local.

O objetivo geral deste trabalho é oferecer uma melhoria no nível de segurança da informação em uma escola técnica.

Como objetivos específicos foram organizadas ações que orientaram a execução e o cumprimento do que foi proposto inicialmente, como:

- ✓ Analisar o ambiente cuidadosamente para obter uma visão clara do cenário de abordagem, identificando os principais ativos.
- ✓ Identificar as vulnerabilidades, e as ameaças que podem explorar estas vulnerabilidades.
- ✓ Analisar os controles já existentes para fornecer um plano de tratamento adequado, conduzindo os recursos ao necessário.
- ✓ Implantar controles que atuem sobre os maiores riscos encontrados intencionando controlá-los.
- ✓ Exibir os resultados e comprovar a eficácia das ações realizadas.

O trabalho foi estruturado em 7 capítulos que iniciam com esta introdução. No capítulo 2 passa por uma visão geral dos conceitos de segurança da informação, e oferece uma reflexão da análise e gestão de riscos. No capítulo 4 o cenário estudado é apresentado e começa o processo de análise de fato, identificando as vulnerabilidades, as ameaças, os controles, para assim conceituar o risco como um todo. No capítulo 5, as implantações são realizadas. O sexto capítulo exhibe os testes que justificam a implantação.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo sete se reserva às considerações finais.

2 SEGURANÇA DA INFORMAÇÃO E ANÁLISE E GESTÃO DE RISCOS

Frente ao cenário de desenvolvimento constante da tecnologia, está consequentemente relacionado o aumento significativo da informação gerada. Atualmente é inquestionável a importância deste bem, para todo e qualquer tipo de organização. Ao mesmo tempo que é considerada patrimônio principal, é também o maior alvo ataques e está sob constante risco. Com isso, a necessidade de atividades que garantam a segurança da informação, já são consideradas cruciais para a continuidade de qualquer ambiente. A NBR ISO/IEC 27002 *apud* Dantas (2011, p.11) fala um pouco sobre a contribuição da segurança para um negócio:

A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio.

A segurança da informação baseia-se em três pilares que solidificam o conceito e orientam as atividades para que o objetivo final seja alcançado. Estes pilares são:

Confidencialidade: O termo usado para a ação capaz de garantir que uma informação não seja disponibilizada a indivíduos não pertinentes, aos quais a mensagem não é direcionada intencionalmente. Feruza e Kim (2007, p.2, tradução própria), exemplificam a definição:

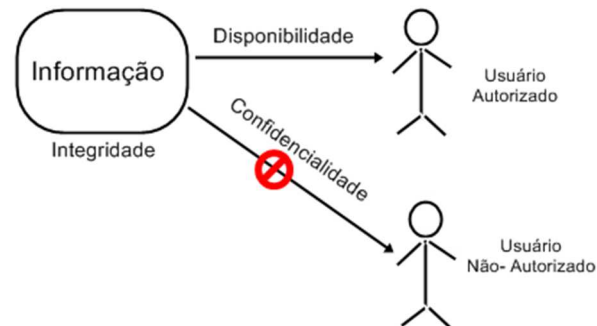
Uma transação de cartão de crédito na Internet requer que o número seja transmitido do comprador para o vendedor e do vendedor para a rede de processamento da transação. O sistema tenta reforçar a **confidencialidade** pela encriptação das informações durante a transmissão, pela limitação dos locais onde a informação aparece e restringido o acesso aos locais onde a informação é armazenada.

Integridade: Refere-se à garantia de que a informação que é gerenciada não seja danificada, ou tenha seu estado original distorcido. Dantas (2011, p.11) explica que “ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original.

Disponibilidade: É a intenção de manter a informação pretendida sempre à disposição do indivíduo que necessita da mesma. Uma informação não disponível não é uma informação com que possa se contar.

A figura 1 representa o conceito de segurança da informação.

Figura 1 - Conceito de Segurança da Informação.



Fonte: Autoria própria (Adaptado da imagem de Per Oscarson, 2003, p. 5).

O fundamento de Segurança da Informação pode ser bem amplo e alguns autores, segundo Laureano (2005, p.12), defendem a ideia de que uma informação só estará segura se atender outros requisitos, como por exemplo:

Autenticidade: Este conceito atesta que a informação tem uma origem determinada, é possível identificar o autor da atividade.

Não-Repúdio: Garantindo a autenticidade o não-repúdio também é praticamente garantido. Refere-se à impossibilidade de negação de uma ação realizada pelo usuário, pode ser obtido através de registros, mas é preciso estar atrelado à autenticidade.

Legalidade: Garante que a informação esteja de acordo com as políticas internas da organização e com o código legal jurídico nacional ou internacional.

A autenticidade e o não repúdio terão seus exemplos apresentados posteriormente neste trabalho.

A análise e gerenciamento dos riscos é pauta corriqueira nas organizações mundo a fora, obtém-se muita expectativa a respeito deste tema. O conceito de risco surgiu para definir atitudes tomadas por instituições ou pessoas em condições de incerteza. Essas condições podem ser medidas trazendo à tona a concepção matemática sobre um assunto teórico. The Orange Book (2004, p. 9, tradução própria) define os riscos como sendo:

A incerteza de um resultado, seja positiva como uma oportunidade, ou negativa como uma ameaça. O risco deve ser avaliado considerando a probabilidade de que algo aconteça e o impacto do que realmente acontece. O gerenciamento dos riscos inclui sua identificação e se avaliação para em seguida oferecer uma resposta a eles.

O gerenciamento do risco não é um processo linear, é o equilíbrio entre uma série de elementos que se relacionam uns com os outros, portanto o tratamento de um risco não pode ser visualizado individualmente, uma vez que atuam em cadeia e a modificação de um deles pode alterar outro processo correlacionado. Os riscos não podem ser extintos por completo do âmbito de uma empresa, porém deve ser buscada a diminuição máxima da possibilidade de ocorrência, alinhando os recursos disponíveis aos riscos com maior prioridade em relação aos outros. As respostas oferecidas aos riscos são chamadas de controles internos e envolvem os quesitos de tratamento que serão abordados profundamente a posteriori. São elas:

- ✓ Aceitar o risco
- ✓ Evitar o risco
- ✓ Transferir o risco
- ✓ Reduzir a probabilidade
- ✓ Reduzir a consequência do risco

A escolha do tratamento é fornecida entre comunicação dos setores responsáveis que indicam se o risco pode ser ou se vale a pena ser tratado.

A NBR ISO/IEC 27005 conceitua a probabilidade, palavra muito utilizada ao decorrer do trabalho:

Na terminologia de gestão de riscos, a palavra "probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se de forma definida, medida ou determinada ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (tal como probabilidade ou frequência durante um determinado período de tempo).

O impacto ou consequência dos riscos também deve ser considerado em uma análise, e é fundamental para definir o tratamento, uma vez que um risco que caso ocorra oferece impacto mínimo à organização, não deve e não se espera que sejam despendidos recursos com atividades que não apresentarão resultados claros após a ação.

Depois de aplicados os tratamentos, riscos residuais devem ser obtidos e analisados para que estejam sempre sob controle e se possível obter uma diminuição ainda maior dos mesmos. Como processo cíclico a gerência dos riscos não deve parar e espera-se que esteja sempre atenta aos novos riscos constantes no mundo. Principalmente no ramo da tecnologia que é o alvo abordado nesse trabalho, a importância de garantir a segurança da informação é clara atualmente e parte do processo de proteção conta com o auxílio da Análise e Gestão de Riscos para direcionar as atividades.

3 ANÁLISE DE RISCO DE SEGURANÇA DA INFORMAÇÃO

Anteriormente foi visto a importância da segurança da informação e como ela é fundamental na continuidade de uma organização, além de uma visão geral de análise e gestão de riscos e seus processos e atividades. Como caso prático, uma escola técnica foi utilizada para estudo. Após o enfoque da análise dos riscos na segurança da informação, foram identificados ativos, vulnerabilidades, controles e ameaças para a partir disso fornecer um plano de tratamento onde alguns dos riscos levantados almeja-se solucionar, melhorando assim o nível de segurança da instituição.

Antes que sejam tomadas medidas para a melhoria da infraestrutura de rede, é essencial qualificar o ambiente onde serão aplicadas as mudanças para que os recursos e tempo disponíveis sejam direcionados onde é realmente necessário. O propósito de melhorias passa por algumas etapas e deve levar em conta as características do local para que a abordagem seja adequada. O estudo é cuidadoso e segundo Stallings e Brown (2014) é necessário responder três questões fundamentais:

1. Quais ativos precisamos proteger?
2. Como esses ativos são ameaçados?
3. O que podemos fazer para contrapor essas ameaças?

As principais referências que fornecem diretrizes para a análise dos riscos feita nesse capítulo são baseadas na norma ISO/IEC 27005, em conjunto com o livro Segurança de Computadores (STALLINGS e BROWN, 2014). Ao final deste, será possível conhecer detalhadamente o cenário avaliado e propor controles pontuais.

3.1 ATIVOS

Para que seja melhorada a segurança da instituição como um todo é preciso que seja definido um ponto de abrangência; o âmbito onde discorrerá todo o processo de investigação e qualificação dos riscos.

Como ponto inicial, é importante identificar os principais ativos dentro da organização e como preservá-los, para que não se tornem pontos de ameaças para o ambiente, em outras palavras, deve-se indicar o escopo da análise. Uma

escola, como qualquer outra, possui muitos de seus ativos comuns, como alunos, professores, funcionários, materiais escolares, entre outros. A instituição observada neste trabalho possui, todas estas características, mas contém algumas particularidades que indicam seu ramo de atuação: o ensino técnico. Para que as atividades sigam normalmente é preciso que toda a infraestrutura do local esteja sempre preparada para atender o utilizador. A gama de equipamentos necessários para garantir as atividades desta escola pode ser considerada grande e equivale à uma empresa de médio porte. Com isso, os objetos de estudo nesta análise serão fundamentados em toda a informação que trafega sobre a infraestrutura de rede e computadores do ambiente, desconsiderando ativos básicos, que fogem do contexto do trabalho. Destaca-se sobre a importância da abstração na análise e gestão de riscos:

É importante enfatizar que, embora o ideal seria considerar todo ativo concebível, na prática isso não é possível. Em vez disso, a meta é identificar todos os ativos que contribuem significativamente para alcançar os objetivos da organização e cujo comprometimento ou perda causaria sérios impactos à operação da organização. (STALLINGS E BROWN 2004, p. 349)

O levantamento dos ativos que segue, passou por um processo análise junto aos principais responsáveis pela escola e mostram resumidamente sua descrição e o nível de importância para o local.

3.1.1 Sistema acadêmico

Principal responsável pela insatisfação dos funcionários e professores da instituição, o sistema, ainda novo, apresenta uma série de problemas relacionados ao seu próprio desenvolvimento. Este, aposenta cadernetas de falta, planilhas administrativas, lança notas e basicamente centraliza boa parte das informações sobre os alunos. Por isso é um sistema atualmente essencial para a escola e é fundamental garantir sua segurança, dentro do possível, visto que a base de dados é armazenada dentro da instituição, mas o desenvolvimento é independente, portanto os meios de disponibilidade nos servidores e na infraestrutura de rede devem ser garantidos pela escola.

3.1.2 Dispositivos de rede

Em um ambiente onde 180 computadores necessitam estar conectados em um mesmo local, estes dispositivos são indispensáveis. *Switches, hubs* e

pontos de acesso fornecem acesso direto aos dispositivos finais e distribuem a conexão de forma simplificada. Dependentes uns dos outros, esses dispositivos necessitam estar bem alocados e distribuídos, pois a indisponibilidade de um deles tem o potencial de pode causar problemas em uma sala ou dependendo da hierarquia até na escola inteira.

3.1.3 Computadores

Equipamentos que estão em contato direto com o usuário precisam estar bem amparados pela infraestrutura e requerem disponibilidade constante. No contexto da instituição, os computadores são utilizados por todos os níveis de usuários. Os alunos necessitam dos computadores para realizar muitas de suas atividades. Como a escola possui 6 laboratórios de em média vinte computadores cada, estes são os principais usuários deste recurso. Funcionários administrativos também discorrem todo o seu tempo de trabalho à frente de um computador e necessitam que esteja sempre disponível, além dos professores que possuem um computador em cada sala de aula à sua disposição para fazer chamadas e acessarem o sistema acadêmico.

3.1.4 Servidores

A instituição atualmente conta com cinco servidores físicos ativos, e outros dez virtualizados que fornecem todos os recursos básicos para que as atividades da escola transcorram adequadamente. Afirma-se que se três dos cinco servidores físicos apresentarem algum tipo de problema, o trabalho da maioria dos funcionários é prejudicado.

Os seções 4.2, 4.3 e 4.4 utilizam a mesma estrutura deste (4.1) abordando cada uma das atribuições em cada ativo específico.

3.2 IDENTIFICAÇÃO DAS VULNERABILIDADES

Após a identificação dos principais ativos da organização e do perímetro da abordagem, é hora de destacar as possíveis vulnerabilidades que podem ser exploradas pelas ameaças, resultando em riscos potenciais para a instituição.

O material de orientação para avaliação dos riscos neste trabalho a norma NBR ISO/IEC 27005, possui um anexo onde são fornecidos exemplos de

vulnerabilidades em diversas áreas da segurança. Este é usado como base o levantamento de informações referentes à rede e ajudam a identificar com clareza onde ameaças podem atacar.

Com uma análise detalhada do local, foram identificadas algumas vulnerabilidades que podem prejudicar a continuidade dos ativos. As informações citadas nesse capítulo tomam como base a análise pessoal do ambiente e as declarações dos administradores quando indagados sobre a atual situação.

3.2.1 Falta de maturidade e administração inadequada

É fato que o sistema acadêmico facilitou a tarefa de alguns professores e ajudou a centralizar as informações dos alunos, seus benefícios são incontestáveis. Apesar disso, o *software* é novo e leva com suas frequentes e entendíveis atualizações, a desconfiança dos usuários. A base de dados do programa é armazenada em um servidor que por sua vez faz uma conexão em VPN com uma central de dados onde usuários têm acesso via interface web, possibilitando ser acessado de qualquer local, visto que os acessos aos dados do programa ficariam restrito apenas à instituição. As constantes falhas no programa somado às consequentes atualizações, destacam a falta de planejamento dos criadores para com o programa.

Além disso, vê-se que uma vez que a base de dados está presente apenas na escola, o cuidado e zelo pela informação é de toda responsabilidade dos administradores do ambiente. Na análise foi identificado o tratamento no qual o sistema está inserido, este, segue em breve descrição: o servidor não possui tratamento específico, é executado em Windows Server 2008, não está inserido no domínio da escola, é alocado dentro da sala de informática onde é um dos cinco servidores empilhados em uma estante. O *backup* é virtualmente realizado, no momento do questionamento o último *backup* era cinco meses anteriores, quando o disco no qual é feito, esgotou o espaço de armazenamento. Não é realizado qualquer tipo controle sobre a auditoria padrão realizada pelo sistema do servidor.

3.2.2 Exposição, falta de controle, e má distribuição

Os dispositivos de rede essenciais para a infraestrutura, são encontrados sobre ou sob mesas, calhas, estantes, armários e ao alcance de qualquer pessoa. Conseqüentemente, é uma das causas mais frequentes de problemas ocasionados na escola, segundo relato dos administradores. O usuário, certo de que ele mesmo pode fazer a mudança que julga necessário nos dispositivos, não titubeia quando tem a oportunidade. A hierarquia dos dispositivos é baseada em uma infraestrutura que foi realizada cinco anos anteriores à data de desenvolvimento desse trabalho. Por isso, a organização e a árvore de nós da rede são inseridas conforme a ocasião, sem que seja feita anteriormente uma análise do ambiente e de onde está sendo aplicada a mudança para que seja feita de modo adequado. Quando um ponto da rede apresenta falha, a dificuldade para encontrar a origem do problema é evidente. Os dispositivos são antigos e limitados, apesar disso o controle destes poderia ser melhor realizado para manter extrair o máximo de recurso que podem oferecer.

A segmentação de Rede surgiu para, entre outros motivos, limitar a disseminação de broadcasts em uma rede local e consiste em inserir dispositivos na rede que bloqueiam a passagem de pacotes de broadcasts quando atravessam suas interfaces. Estes dispositivos também tem a função de interligar redes locais diferentes. (HAFFERMANN, 2009, p. 2)

Com a limitação de *broadcasts* na rede, mensagens são enviadas apenas ao seu destinatário, evitando assim que pessoas não autorizadas tenham acesso a conteúdo que não fazem parte do seu cunho.

3.2.3 Acesso permissivo e pouco controle sobre as ações

Em um local onde quase duzentos computadores são mantidos é importante que haja o controle do conteúdo acessado e dos recursos disponíveis para cada tipo de usuário.

Para impedir que informações inerentes aos negócios de determinada organização sejam trafegados do mundo externo para o interno, ocupando largura de banda, tempo produtivo da organização, bem como, influenciando na formação educacional e moral de nossos filhos, devem ser implementados mecanismos capazes de analisar tal conteúdo, através de técnicas que possibilitem avaliar palavras e montando frases ligadas às regras de negócios ou simplesmente realizar, por exemplo, filtragem de conteúdo pornográfico. (ROSA, TAMAE e SPINOLLA; 2005)

Como destacam os autores, o controle de conteúdo é fundamental para garantir que apenas informações relevantes ao cenário possam ser acessadas. Na escola, alunos, professores funcionários e visitantes, possuem acesso ao mesmo tipo de conteúdo, seja durante uma aula, seja durante o trabalho no setor administrativo. A exposição à internet pode oferecer risco à integridade de toda a rede visto que um computador que é infectado através de um site malicioso, pode propagar seu vírus por toda o local, pois, como foi explanado no tópico anterior, todas as informações do ambiente, independente do grau de importância, trafegam sob a mesma estrutura, todos em uma única rede, física e lógica.

3.2.4 Hardware inadequado, exposição, ausência de controles

Os servidores, último grupo de ativos aqui citados, mas não menos importante, têm a função de prover os principais recursos para os *hosts* e a missão de garantir a disponibilidade, integridade e confidencialidade das informações. Quando se pensa em gerenciamento, é esperado que este seja fácil e prático. Os servidores físicos do ambiente são identificados seguindo um padrão da escola, porém não é tão simples identificar qual tipo de serviço cada um oferece. A falta de documentação das implementações e mudanças no local dificulta a solução dos problemas. Foi identificado que 60% - três dos cinco - dos servidores, atuam sobre *hardwares* de máquinas fabricadas para funcionar como estações de trabalho. É sabido que servidores possuem por padrão um *hardware* mais robusto para suportar as suas funções, grandes consumidoras de recursos. Os administradores do local, quando indagados sobre a razão da utilização deste tipo de máquina para essas funções, alegaram a falta de recursos financeiros disponibilizados para a aquisição de equipamentos específicos.

Ciente da utilização de equipamentos inadequados para exercer determinadas funções, reforça-se a importância de um monitoramento destes servidores para identificar qual seu estado atual, qual o consumo de componentes importantes, como memória ou processador, a fim de identificar rapidamente um possível incidente. No cenário atual, este controle não é feito sob nenhuma circunstância e os problemas são tratados de forma corretiva, método que pode prejudicar a disponibilidade e integridade de alguns serviços.

O servidor de internet, executado em Debian Linux faz o roteamento necessário entre a rede pública e a rede interna, nele também são aplicadas as políticas primárias de acesso. A política padrão do local tem a função de encaminhamento de pacotes liberada e possui apenas uma restrição para serviços de e-mail. Portanto, o controle externo é praticamente nulo e a entrada e saída da rede, ponto com mais exposição no local, é caracterizado como vulnerável e passivo de exploração de vulnerabilidades.

3.3 CONTROLES EXISTENTES

Os controles aqui levantados são importantes para identificar qual a atual preocupação da instituição a respeito das ameaças, a partir daí, pode ser analisada a consequência e probabilidade de um risco, podendo ser considerados altos se poucos controles estiverem sendo realizados.

A transmissão de informações do sistema acadêmico para a base de dados externa é feita através de uma VPN que garante a segurança dos dados na rede pública. Existe um *backup* antigo dos dados que pode auxiliar na reestruturação da aplicação em caso de incidente. Os *bugs* no programa são rapidamente comunicados ao desenvolvedor, que rapidamente realiza o reparo, encurtando a vida do problema. Apesar da base de dados estar alocada em um servidor inadequado, seu hardware pode encontrar vários equipamentos semelhantes para executar suas atividades em caso de falha, o que inicialmente é um problema que pode ser contornado com a rápida substituição.

O principal dos dispositivos de rede, um *switch* gerenciável alocado no setor de informática atua como controlador de banda para algumas portas e ajuda a direcionar os recursos aos domínios de acordo com sua necessidade, as alterações realizadas nos mesmo por parte dos funcionários são anotadas em um quadro para a visualização de todos.

Os computadores possuem a auditoria de sistema habilitada, o que pode auxiliar na identificação de ação realizada pelo usuário. Isso aliado à individualização dos usuários pode ser de grande valia para garantir o não-repúdio.

O servidor que fornece acesso à internet possui algumas políticas básicas aplicadas, como a orientação à conexão que agiliza a filtragem dos pacotes, o bloqueio à porta¹ de serviço de *e-mails*, o que impede a invasão e utilização do servidor por um terceiro para enviar *spams*. As alterações realizadas nos servidores em geral são anotadas em um quadro comum, que os funcionários do setor têm visão direta, sua ideia é disseminar a informação da alteração realizada. Os servidores Windows são configurados para realizar auditoria no sistema automaticamente, esta facilita na resolução de problemas e ajuda a garantir o não-repúdio.

3.4 IDENTIFICAÇÃO DAS AMEAÇAS

A identificação das ameaças é parte fundamental da análise dos riscos para justificar o tratamento posteriormente identificando os ativos de maior prioridade e situar-se sobre os perigos expostos.

No sistema acadêmico, as vulnerabilidades apresentadas podem ocasionar na perda da base de dados e prejuízo em caso de retomada, já que a cópia de segurança é considerada antiga. Um incidente desse porte tem grandes chances de acontecer, uma vez que muitos usuários têm acesso à aplicação e podem excluir alguma informação acidentalmente ou mesmo a falha no *hardware* inadequado ocasionar sequelas no disco rígido. Como foi identificada a imaturidade da aplicação, pode acontecer exploração de vulnerabilidades ainda não identificadas, já que os erros são frequentes.

Os dispositivos de rede são passíveis de indisponibilidade, visto sua grande exposição, uma alteração indevida em qualquer um destes equipamentos pode oferecer prejuízo para toda a rede. Com a falta de segmentação, as informações são trafegadas sob a mesma estrutura lógica e um *sniffer* de pacotes, como o Wireshark pode obter informações antes sigilosas.

A falta de controle sobre o conteúdo disponibilizado nos computadores aos usuários pode ocasionar uma infecção dos computadores ao acessar *sites* maliciosos, por exemplo. A infecção de um computador pode gerar a infecção de

¹ Uma porta de uma aplicação é a conexão virtual utilizada na transmissão dos dados.

toda a rede. Os poucos controles sobre as atividades dos usuários também podem abrir precedente para ataques oriundos da própria rede.

Os servidores podem ter sua atividade prejudicada devido a utilização de *hardware* inadequado, uma vez que estes podem não suportar por muito tempo a exigência que é esperada de um servidor. O servidor que dá acesso à internet pode ser alvo de ataques, devido suas poucas políticas de acesso, seja de entrada, saída ou encaminhamento. O que também pode ser ocasionado através de mudanças inadequadas, não controladas ou testadas previamente.

3.5 CRITÉRIOS DE ESTIMATIVA E CÁLCULO DOS RISCOS

Após a identificação dos ativos e das possíveis ameaças que podem afetá-los, é importante quantificar a real significância de cada atividade para a organização. Assim sendo, probabilidades e estimativas são classificadas junto de métodos para identificação das consequências e do impacto sobre a organização. Para esta tarefa, serão utilizadas duas tabelas do livro *Segurança de Computadores* (STALLINGS e BROWN, 2014) que indicam a definição da classificação dos adjetivos empregados aos riscos, a Tabela 1 explana sobre a probabilidade do risco, já a Tabela 2 trata da “consequência da concretização de uma ameaça específica”.

Tabela 1 - Probabilidade dos riscos

CLASSIFICAÇÃO	PROBABILIDADE	DEFINIÇÃO EXPANDIDA
1	RARA	Pode ocorrer somente em circunstâncias excepcionais e ser considerada como "azar" ou muito improvável.
2	IMPROVÁVEL	Pode ocorrer a qualquer momento, mas não é esperada dados os controles, as circunstâncias e os eventos recentes.
3	POSSÍVEL	Pode ocorrer a qualquer momento, mas a probabilidade de não acontecer é a mesma. Pode ser difícil controlar sua ocorrência em razão de influências externas.
4	PROVÁVEL	Provavelmente ocorrerá em alguma circunstância e não será surpresa se ocorrer.
5	QUASE CERTA	Espera-se que ocorra na maioria das circunstâncias e certamente ocorrerá mais cedo ou mais tarde.

Fonte: *Segurança de Computadores* (STALLINGS e BROWN, p 452, 2014)

Tabela 2 – Consequência dos riscos

CLASSIFICAÇÃO	CONSEQUÊNCIA	DEFINIÇÃO EXPANDIDA
1	INSIGNIFICANTE	Geralmente o resultado de uma brecha de segurança menor e em uma única área. É provável que o impacto dure menos do que alguns dias e que sua retificação exija apenas dispêndia insignificante. Em geral, não resulta em qualquer prejuízo tangível para a organização.
2	PEQUENA	Resulta de uma brecha de segurança em uma ou duas áreas. O impacto provavelmente durará menos de uma semana, mas pode ser tratado no nível de segmento ou de projeto, sem intervenção da gerência. Em geral, pode ser retificada usando apenas os recursos de projeto ou de equipe. Novamente, isso não resulta em qualquer prejuízo tangível para a organização, mas pode, em retrospecto, mostrar oportunidades perdidas ou falta de eficiência anteriores.
3	MODERADA	Brechas de segurança sistêmicas limitadas (e possivelmente continuadas). O impacto provavelmente durará até duas semanas e, em geral, exigirá a intervenção da gerência, embora ainda seja possível tratá-lo no nível de projeto ou de equipe. Isso exigirá alguns custos de investimento em conformidade para que o impacto seja superado. Clientes ou o público podem ter conhecimento indireto ou informações limitadas sobre esse evento.
4	GRANDE	Brecha de segurança sistêmica continuada. O impacto durará provavelmente 4-8 semanas exigirá intervenção significativa da gerência e recursos para ser superado. A gerência sênior terá de agir direta e continuamente durante o incidente, e espera-se que os custos para obter conformidade sejam substanciais. Clientes ou o público saberão da ocorrência de tal evento e terão conhecimento de vários fatos importantes. É possível que haja perda de negócios ou de resultados organizacionais, mas isso não é esperado, especialmente se esse for um acontecimento isolado.
5	CATASTRÓFICA	Grande brecha de segurança sistêmica. O impacto durará três meses ou mais, e a gerência sênior terá de intervir durante todo o evento para superar deficiências. Espera-se que os custos para obter conformidade sejam significativos para a organização. Provavelmente haverá debate público ou político sobre a organização e também perda de confiança na organização. Possivelmente haverá ações criminais ou disciplinares contra o pessoal envolvido.
6	DIA DO JUÍZO FINAL	Várias instâncias de grandes brechas de segurança sistêmicas. A duração do impacto não pode ser determinada, a gerência sênior será interdita e a empresa terá de se submeter à administração externa ou a outra forma de reestruturação ampla. Esperam-se ações criminais contra a gerência sênior, e a perda substancial de negócios e o fracasso no cumprimento dos objetivos organizacionais serão inevitáveis. Os custos para obter conformidade provavelmente resultarão em perdas anuais durante alguns anos, com a possível liquidação da empresa.

Fonte: Segurança de Computadores (STALLINGS e BROWN, p 453, 2014)

Após levantados todos os requisitos que antecedem a análise dos riscos, é hora de avaliá-los, medi-los e documentá-los. O intuito das tabelas anteriores era definir valores para obtenção de parâmetros que justifiquem ou não o tratamento de um risco. A tabela 3 é baseada também na principal referência

deste capítulo e elenca três ameaças ou vulnerabilidades para cada ativo apresentado. Os valores definidos nas tabelas foram obtidos através de reuniões com os responsáveis pela manutenção da infraestrutura da escola para chegar um consenso que dão consistência aos resultados.

Tabela 3 - Cálculo e registros dos riscos

ID	ATIVO	VULNERABILIDADE	AMEAÇA	CONTROLE EXISTENTE	PROBABILIDADE	CONSEQUÊNCIA	I.P.T
A	SERVIDORES	Elo com a internet exposto, política permissiva, controles de acesso escassos	Ataques externos que podem causar prejuízo a integridade e disponibilidade da rede	Política padrão definida com bloqueio à acesso remoto externo e envio de mensagens de email	Provável	Catastrófica	9
B	COMPUTADOR	Sem controle de acesso na camada de aplicação, ou seja, todo conteúdo web está disponível	Acesso à conteúdos maliciosos que podem infectar o equipamento e toda a rede	Inexistente (Nenhum filtro de conteúdo ou de protocolos)	Quase certa	Grande	9
C	SISTEMA ACADÊMICO	Ausência de planejamento de backup da base de dados	Perda da base de dados, por ataque mal intencionado ou exclusão acidental	Backup antigo, que pode ajudar na reestruturação do sistema	Provável	Grande	8
D	COMPUTADOR	Falta de controle das ações realizadas pelos usuários da rede	Ataque mal intencionado originado da rede interna	Auditoria do sistema operacional que pode identificar o usuário autor do ataque, caso parta de um computador da própria escola	Possível	Grande	7
E	SISTEMA ACADÊMICO	Uso de equipamento inadequado para executar as tarefas atribuídas	Danificação do hardware do equipamento, indisponibilidade do serviço	Computadores disponíveis que podem substituir o atual e desempenhar o papel sem grande desempenho	Quase certa	Pequena	7
F	DISPOSITIVOS REDE	Falta de segurança no acesso físico aos dispositivos	Ocorrer indisponibilidade da rede porque um usuário fez uma alteração indevida	Inexistente (Nenhum controle de endereço físico dos equipamentos, possibilitando a inserção de qualquer dispositivo)	Provável	Moderada	7

G	DISPOSITIVOS REDE	Falta de um processo controlado de gestão de mudança	Atualização ou alteração indevida no dispositivo que prejudique o funcionamento	Inexistente (Não existe nenhum controle de disponibilidade dos equipamentos)	Possível	Grande	7
H	SISTEMA ACADÊMICO	Imaturidade do software, falta de planejamento no desenvolvimento	Exploração de vulnerabilidade no software ainda não identificadas	Atualizações constantes, contato rápido com o desenvolvedor	Possível	Moderada	6
I	SERVIDORES	Erro ao realizar uma atualização, causa indisponibilidade e pode prejudicar a disponibilidade dos recursos da rede	Indisponibilidade do sistema, devido a alteração não controlada	Serviço de auditoria automática no sistema operacional que podem ajudar na identificação da alteração realizada	Possível	Moderada	6
J	DISPOSITIVOS REDE	Falta de segmentação do ambiente, ocasionando em domínios de broadcast desnecessários	Subtração de dados confidenciais de setores restritos da instituição	Controle de tráfego por portas de um único switch gerenciável da instituição, definição prioridade aos domínios principais	Possível	Moderada	6
K	SERVIDORES	Falta de documentação dos equipamentos e das mudanças realizadas	Dano a um sistema e impossibilidade de retorno ao estado anterior	Quadro usado para informes de atividades realizadas no ambiente	Possível	Pequena	5
L	COMPUTADOR	Falta de segurança física nos ambientes	Acesso de indivíduos não autorizados aos computadores	Usuários individualizados e controlados quando entram e saem da instituição	Improvável	Moderada	5
I.P.T = ÍNDICE DE PRIORIDADE DE TRATAMENTO							

Fonte: Autoria Própria.

A classificação dos riscos é feita em ordem decrescente pelo índice de prioridade de tratamento, que é resultado soma da probabilidade e da consequência de determinada ocorrência ($RISCO = PROBABILIDADE + CONSEQUÊNCIA$). Neste momento são obtidas as prioridades e definidos os pontos críticos que necessitam de uma atenção maior. As fórmulas apresentadas baseiam-se no livro Segurança de Computadores (STALLINGS e BROWN, 2014).

3.6 TRATAMENTO DOS RISCOS

Após a priorização dos riscos, convém que sejam adotadas medidas para contê-los definindo um plano de tratamento. Neste momento, é feito um alinhamento entre as prioridades e os recursos disponíveis para a aplicação de determinada mudança. Quando falamos de recurso sempre submetemos à ideia de dinheiro. Contudo, diante de um cenário público, a demanda de verba requer um processo burocrático que foge do escopo e da linha do trabalho. Portanto, foi definido em acordo com o pessoal responsável que a inserção de controles ficaria restrita à adaptação e reutilização dos recursos já disponíveis e soluções livres² e gratuitas.

Segundo Stallings e Brown (2014) há cinco formas diferentes de tratar um risco:

Aceitar o risco: Optar por aceitar o risco, devido à dificuldade de lidar com ele, então conscientizam-se das consequências caso ocorra.

Evitar o risco: Abrir mão do serviço ou atividade que gera o risco. Pode ocasionar insatisfação pela indisponibilidade de executar algumas funções importantes para o negócio.

Transferir o risco: Compartilhar a responsabilidade do risco com terceiros, na maioria das vezes é justificada fazendo a contratação de empresas seguradoras que se responsabilizem por determinada atividade.

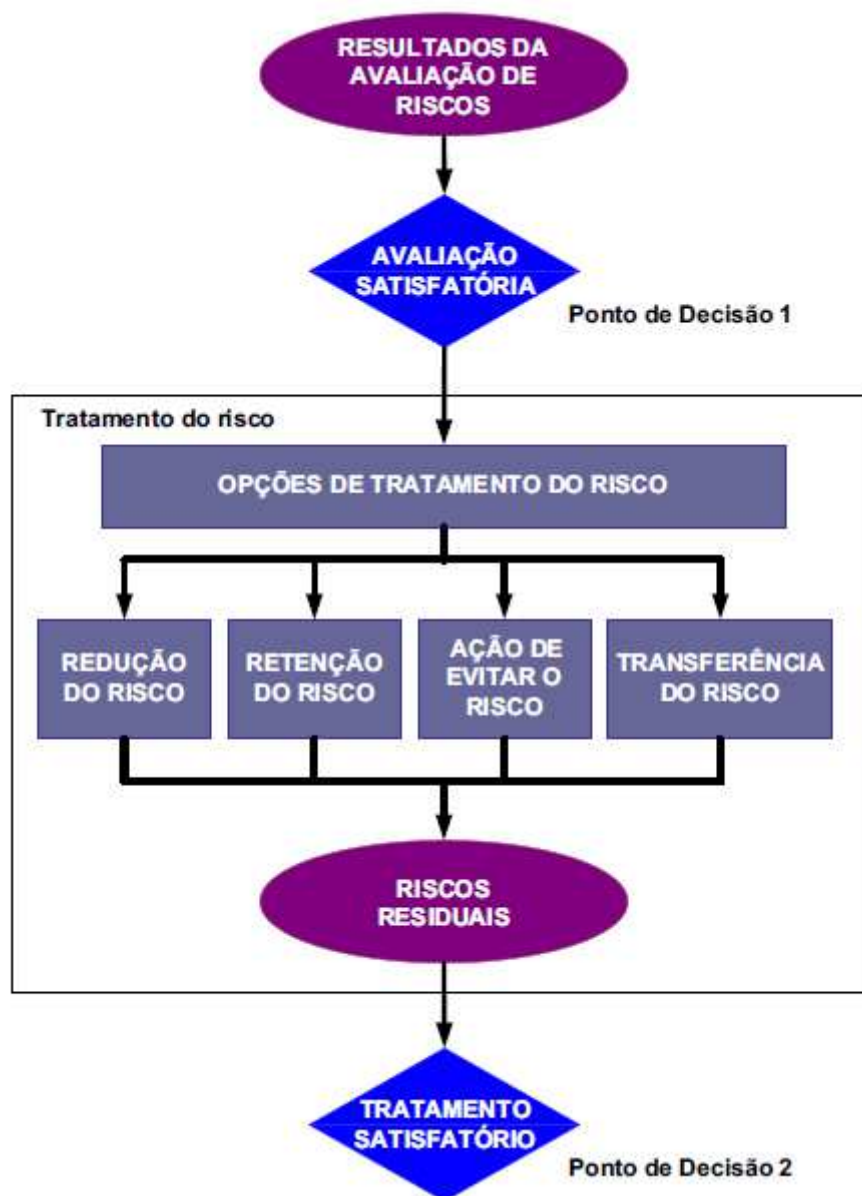
Reduzir a consequência: Mudar a maneira como os recursos são utilizados para reduzir o impacto sobre a organização. Pode ser obtido com um plano de *backup*, plano de contingência, etc.

Reduzir a probabilidade: Realizar alterações na estrutura para conseguir reduzir a possibilidade de exploração em uma vulnerabilidade. Pode ser obtido com a implementação de firewalls, treinamento dos usuários, etc.

² Nesse contexto a palavra refere-se à forma de manifestação de um *software*. Seus objetivos incluem a liberdade aos usuários de controle de execução e processamento dos dados através da disponibilização do código fonte para alterações.

A figura 2 mostra o processo de tratamento inserido na gestão de riscos, ocorrendo após uma avaliação satisfatória do cenário.

Figura 2 - Atividade de tratamento do risco



Fonte: ISO/IEC 27005

A escolha pelo tipo de tratamento que caberá a cada um dos riscos, tem a função de oferecer diretrizes para o plano de ação que será efetuado posteriormente. Os riscos serão classificados para simplificação na retomada dos mesmos posteriormente.

A - Elo com a internet relativamente exposto, política de acesso permissiva possibilitando ataques externos que prejudiquem todos os princípios de segurança do local: Será implementado um *firewall*, com interface amigável, facilidade de gerenciamento e de aplicações de regras que auxiliarão a manter maiores controles sobre os dados que entram e saem da escola, o risco teve sua probabilidade reduzida.

B - Falta de controle de acesso a conteúdo *web*, oferecimento de disponibilidade total que pode abrir precedente para acesso à sites maliciosos que danifique o equipamento e posteriormente toda a rede: Será realizada a implementação de um *proxy* para controlar o acesso aos conteúdos *web*, também serão obtidos relatórios de todo acesso realizado na instituição, foi reduzida a probabilidade do risco e a consequência.

C - Inexistência de um plano de *Backup*, que gera receio pela perda acidental ou não dos dados impossibilitando a restauração dos arquivos e retomada das atividades: Foi proposto a implementação de um plano de backup onde foram indicados os locais e as datas que seriam feitas as cópias de segurança, portanto foi reduzida a consequência.

D - Ações desnecessárias disponíveis aos usuários na rede, propiciando a ataques mal-intencionados ou exclusão de arquivos acidentalmente: Optaram por aceitar este risco, pela baixa incidência deste tipo de ocorrência historicamente.

E - Execução de serviços e recursos sobre hardwares não indicados para tal atividade, ocasionado na danificação dos equipamentos e consequente indisponibilidade dos recursos dispostos: Com o argumento de que não poderiam fazer a aquisição de equipamento apropriados para os determinados sistema, o risco foi aceito.

F - Acesso físico livre aos dispositivos de rede, possibilitando à terceiros a modificação e dos equipamentos: Este risco também foi aceito, como consequência da impossibilidade de compra de equipamentos (*racks*) para resguardá-los.

G - Ausência de controle às mudanças físicas de estrutura e configuração dos dispositivos de rede, podendo gerar a alteração indevida e causar indisponibilidade da rede: Houve a justificativa de que as mudanças constantes eram necessárias, visto que a instabilidade dos equipamentos ocasionava isso. O risco foi aceito.

H - Imaturidade do sistema acadêmico, e falta de planejamento do mesmo que abre precedente para a exploração de vulnerabilidades no software ainda não identificadas: Este risco foi transferido, comunicando o desenvolvedor dos riscos existentes.

I - Ausência de controle à mudanças e atualizações nos servidores realizadas nos equipamentos, que pode gerar indisponibilidade de algum recurso de software que não tem compatibilidade com o hardware após a atualização: O risco foi aceito, considerando suficiente o controle já existente, ou seja, a auditoria do sistema operacional.

J - Rede única com informações de diferentes interesses, trafegando sobre a mesma arquitetura sem qualquer tipo de restrição física ou lógica, possibilitando a subtração de informações confidenciais da instituição: Pretende-se reduzir a probabilidade das ocorrências dividindo o domínio de broadcast, aplicando separação para a rede sem fio.

K - Falta de documentação dos equipamentos e das mudanças realizadas podendo impossibilitar a reestruturação da configuração anterior em caso de dano: Foi indicado a utilização de uma base de dados compartilhada já existente para integração e controle das atividades realizadas. Reduziu-se sua probabilidade.

L - Falta de segurança física nos ambientes que proporciona acesso à indivíduos não autorizados aos computadores: Aconselhou-se a contratação de pessoal para fazer a segurança física do local, portanto o risco foi transferido.

Este capítulo conclui a fase de avaliação do ambiente, considerando todas as alternativas e as variáveis, agora um plano de ação pertinente pode ser pautado sobre o conteúdo levantado, entramos na fase de implantação.

4 IMPLANTAÇÃO DE CONTROLES

Nesta etapa do trabalho, serão propostas e aplicadas algumas mudanças para conter os riscos escolhidos na etapa anterior do trabalho. Com base nas necessidades da instituição, foi proposta a implantação de uma aplicação, o *Netdeep Firewall* que abrangeria dois dos principais riscos, em seu índice de prioridade de tratamento. Estes são os riscos que são afetados com a solução:

1. *Elo com a internet relativamente exposto, política de acesso permissiva possibilitando ataques externos que prejudiquem todos os princípios de segurança do local.*
2. *Falta de controle de acesso a conteúdo web, oferecimento de disponibilidade total que pode abrir precedente para acesso à sites maliciosos que danifique o equipamento e posteriormente toda a rede.*
3. *Rede única com informações de diferentes interesses, trafegando sobre a mesma arquitetura sem qualquer tipo de restrição física ou lógica, possibilitando a subtração de informações confidenciais da instituição.*

Foi tida como uma boa opção pela sua simplicidade, fácil instalação, interface amigável, variadas opções de configuração e gratuidade. O *Netdeep Firewall* é uma solução da empresa *Netdeep*, onde o cliente pode optar pela versão gratuita do *software* ou uma assinatura com recursos a mais. A versão grátis da aplicação foi implementada na escola, entre os recursos disponíveis estão:

- *Firewall* de aplicação.
- *Proxy* HTTP.
- Filtro URL
- Captive Portal.
- Antivírus
- Monitor de rede.

O *software* oferece integração de quatro tipos diferentes das interfaces de rede que por sua vez atribui o nome de cores a elas para melhor identificação da sua configuração:

Red (Vermelho): Essa interface estará exposta à internet ou outra rede não confiável, o intuito é usá-la para fazer roteamento e proteger as demais interfaces.

Green (Verde): É atribuída aos computadores da rede local cabeada, possui restrições pré-definidas que garantem sua segurança.

Blue (Azul): Os dispositivos desta rede não podem se comunicar com a rede *Green*, é recomendada para o uso em redes sem fio.

Orange (Laranja): Esta interface é opcional e foi feita para o uso em DMZ³. Não existe comunicação desta rede com as demais.

Com isso foram preparados um computador com as seguintes configurações:

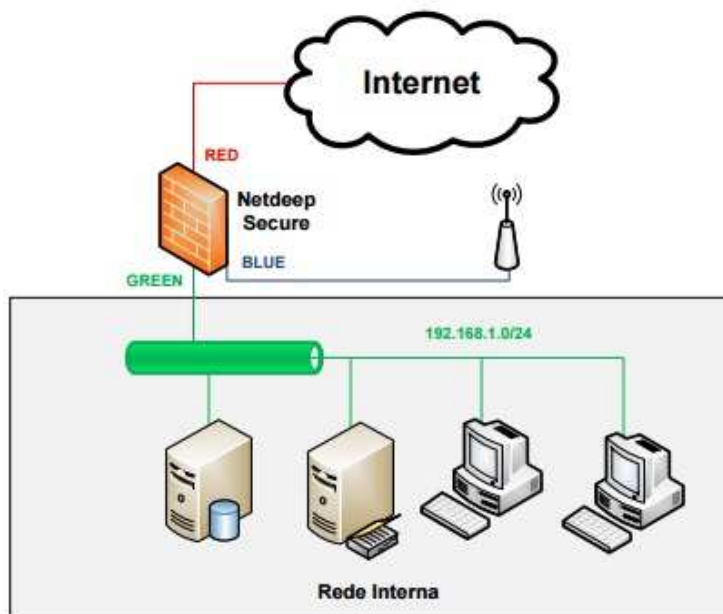
- Processador: Intel Core2Duo.
- Memória RAM: 4 GB
- Espaço de armazenamento: 500 GB.
- Três placas de rede Ethernet.

O *hardware* escolhido atende as recomendações da empresa. A figura 3 mostra o novo *layout* escolhido, utilizando três das quatro configurações de interface que o *Netdeep* oferece. A primeira interface (*Red*) está configurada como DHCP, portanto caracteriza sua autoconfiguração de IP, é conectada ao modem da provedora contratada, é a interface que tem acesso direto à internet. A segunda placa de rede (*Green*) foi configurada com um IP de classe C, este será o endereço de *Gateway* padrão dos computadores inseridos nessa rede. A terceira (*Blue*), foi configurada com um IP de classe B e designada aos dispositivos sem fio, este endereço será o *gateway* dos dispositivos móveis e *notebooks*. Com essa mudança de arquitetura a instituição ganha segurança no que diz respeito à separação das redes, reduzindo a probabilidade de ocorrência do risco 3, apresentado neste capítulo. A instalação é simples e tem seu manual

³ Do inglês Demilitarized Zone (em português Zona Desmilitarizada), refere-se ao seguimento da rede onde são alocados os Servidores que precisam estar expostos à Internet, como servidores FTP ou Web.

disponível em: <<http://www.netdeep.com.br/secure/wp-content/uploads/2015/05/Guia-de-Instala%C3%A7%C3%A3o-NETDEEP-SECURE-3.pdf>>

Figura 3 - Diagrama de proposta da estrutura de rede



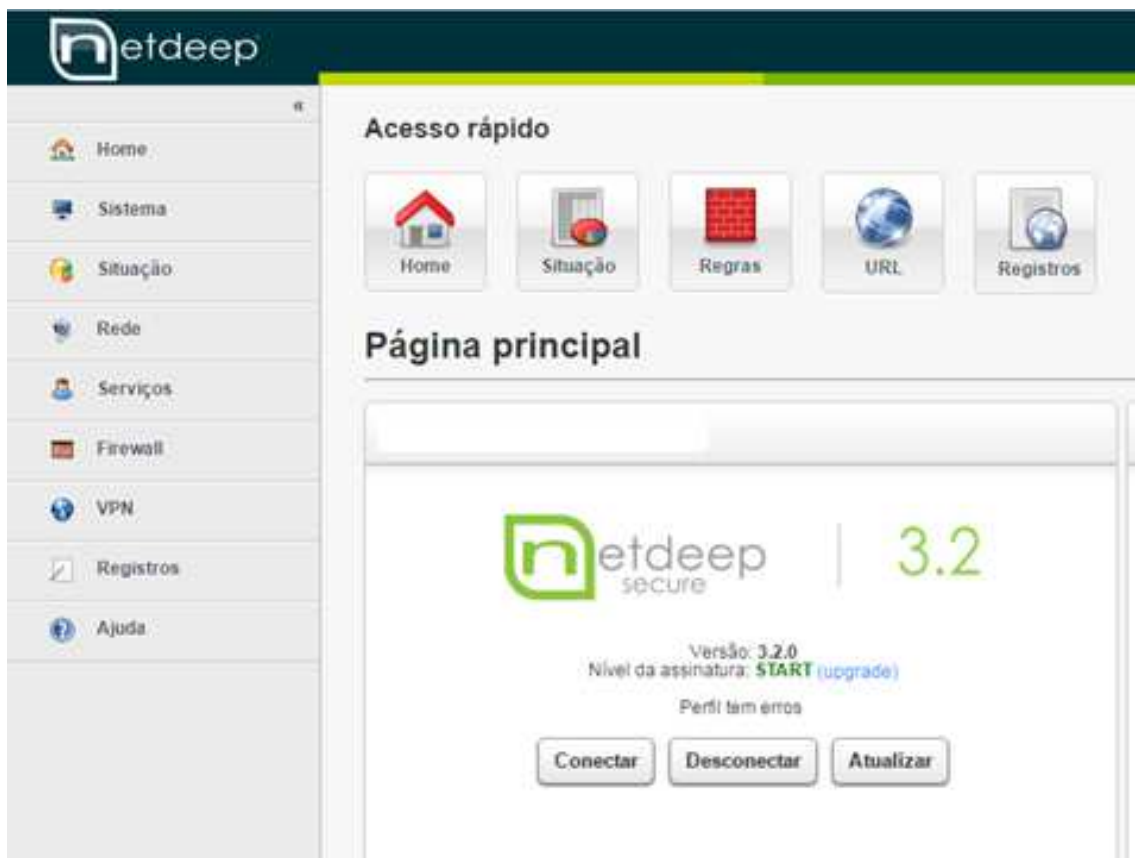
Fonte: Adaptação ao manual de instalação do Netdeep Firewall.

Após a instalação, é possível ver uma interface não muito amigável, com um fundo preto e linhas de texto. Será necessário acessar o IP da interface *Green* mais a porta padrão da aplicação, no caso 8443, de um computador da própria rede via navegador. Exemplo:

- <http://192.168.0.1:8443>

Ao acessar será necessário fazer a autenticação inserindo o usuário e senha configurados no momento da instalação. Na figura 4, é possível ver a tela encontrada após a realização da autenticação. Pode ser observado já na tela inicial a versão do *software*, monitores de consumo de *hardware*, da movimentação nas interfaces de rede, os serviços disponíveis e se estão ativos ou não, além de um menu lateral com opções disponíveis.

Figura 4 - Tela principal do Netdeep Firewall



Fonte: Netdeep Firewall da escola técnica em estudo.

Neste trabalho, o foco será a observação das regras de *firewall* e as configurações do serviço de *proxy* e filtro URL.

Para a configuração do *proxy*, duas opções são possíveis, a habilitação do *proxy* transparente que funciona basicamente imperceptível, todo pacote com destino à internet passa pelo filtro do *proxy*, sem que seja preciso fazer a configuração individual em cada estação. Porém, o Netdeep Firewall em sua versão gratuita não oferece suporte ao *proxy* transparente para *sites* que usam o protocolo HTTPS, excluindo assim boa parte de *sites* que deveriam ser bloqueados, uma vez que este protocolo é uma realidade na *Web*.

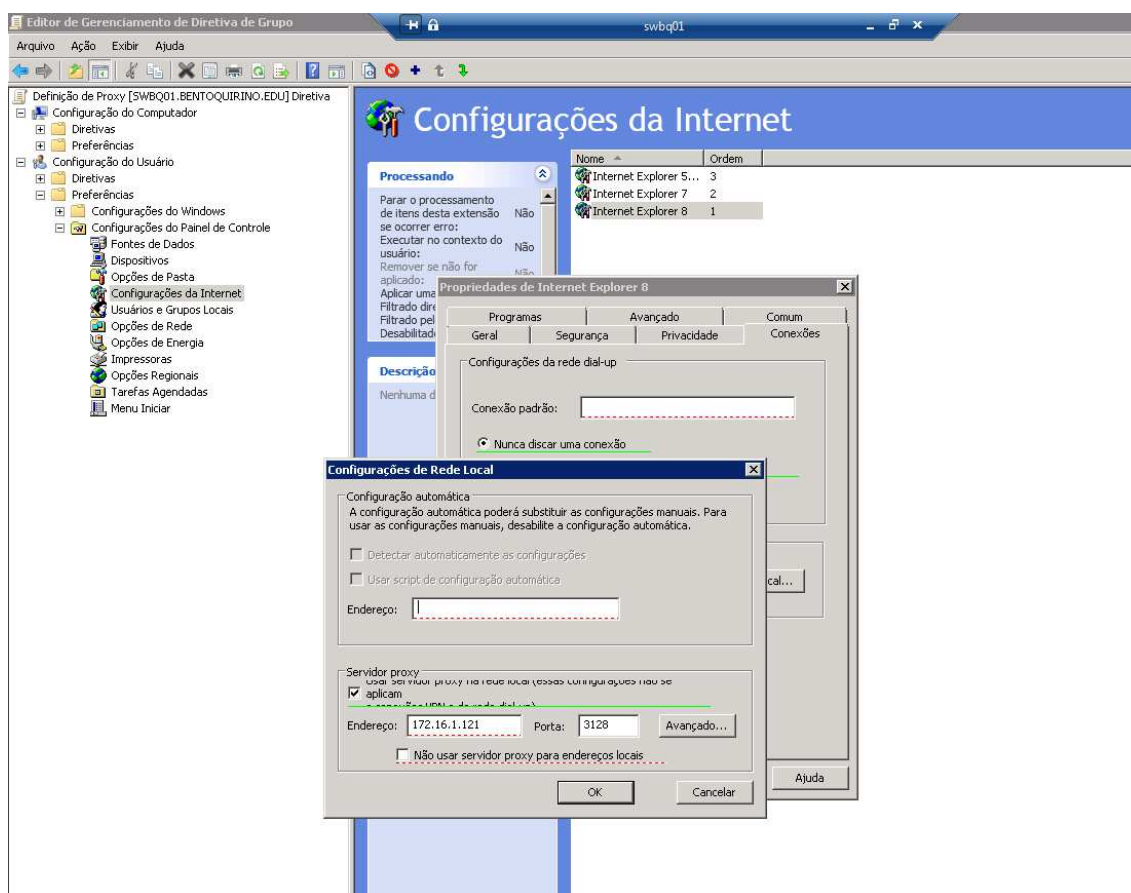
Com este problema, foi sugerido que o *proxy* transparente não fosse habilitado, ao invés disso foi feita a criação de uma Diretiva de Gerenciamento de Grupo, também conhecida como GPO. A GPO é um recurso disponível nos sistemas operacionais da Microsoft, esta permite a aplicação de políticas e regras a diferentes usuários da rede simultaneamente, como todos os

computadores do ambiente são executados sobre Windows, a utilização do recurso foi vista como uma boa solução. Então quando um usuário incluído na GPO efetuar o *login* em qualquer computador do ambiente, o *proxy* será automaticamente configurado e não poderá ser alterado. A configuração foi feita, após a criação da GPO (como criar uma GPO: [https://technet.microsoft.com/pt-br/library/cc772538\(v=ws.11\).aspx](https://technet.microsoft.com/pt-br/library/cc772538(v=ws.11).aspx). Disponível em 14/11/2016), da seguinte forma:

Configurações do Usuário > Preferências > Configurações do Painel de Controle > Configurações da Internet.

Nesta etapa são adicionados os navegadores que são passíveis às regras e a configuração que será aplicada neles, como é exibido na figura 5:

Figura 5 - Configuração de Política de Grupo no Windows Server 2008



Fonte: Servidor Windows 2008, da escola técnica estudada.

Todas configurações só poderão ser aplicadas em versões do Internet Explorer. No Google Chrome serão absorvidas por padrão, já o Firefox, terá de ser configurado manualmente e poderá ter as configurações alteradas, estes são os navegadores utilizados na escola. Para evitar o uso indevido dos recursos, foi definida a autorização de apenas os navegadores que recebem as regras, essa restrição também pode ser realizada pelo Netdeep Firewall, como pode ser observado na figura 6.

Figura 6 - Menu de seleção para restrição de navegadores

Firefox:	<input type="checkbox"/>	FrontPage:	<input type="checkbox"/>
Go!Zilla:	<input type="checkbox"/>	Google Chrome:	<input checked="" type="checkbox"/>
Internet Explorer:	<input type="checkbox"/>	Java:	<input type="checkbox"/>
MacOSX Update:	<input type="checkbox"/>	Media Player:	<input type="checkbox"/>
Safari:	<input type="checkbox"/>	WGA:	<input type="checkbox"/>
apt-get:	<input type="checkbox"/>		

Fonte: Netdeep Firewall da escola técnica em estudo.

Depois de realizada a configuração, é preciso decidir o que filtrar. Como configuração inicial foi definido o bloqueio de alguns temas para fins de teste. A aplicação oferece a possibilidade de importação de *blacklists* para facilitar as restrições, figura 7 pode ser observado o campo para seleção de bloqueio após a importação da lista.

Figura 7 - Seleção de categorias para bloqueio no proxy

finance/realestate:	<input type="checkbox"/>	models:	<input type="checkbox"/>
finance/trading:	<input type="checkbox"/>	movies:	<input type="checkbox"/>
fortunetelling:	<input type="checkbox"/>	music:	<input type="checkbox"/>
forum:	<input type="checkbox"/>	news:	<input type="checkbox"/>
gamble:	<input type="checkbox"/>	podcasts:	<input type="checkbox"/>
government:	<input type="checkbox"/>	politics:	<input type="checkbox"/>
hacking:	<input checked="" type="checkbox"/>	porn:	<input checked="" type="checkbox"/>
hobby/cooking:	<input type="checkbox"/>	radiotv:	<input type="checkbox"/>
hobby/games-misc:	<input checked="" type="checkbox"/>	recreation/humor:	<input type="checkbox"/>
hobby/games-online:	<input checked="" type="checkbox"/>	recreation/martialarts:	<input type="checkbox"/>
hobby/gardening:	<input type="checkbox"/>	recreation/restaurants:	<input type="checkbox"/>
hobby/pets:	<input type="checkbox"/>	recreation/sports:	<input type="checkbox"/>

Fonte: Netdeep Firewall da escola técnica em estudo.

A implementação do *proxy* será fundamental para o controle dos conteúdos dentro da instituição e a identificação dos registros para garantir o não-repúdio ao local. Os bloqueios e restrições aplicadas pelo sistema são baseados em sistemas como Squid e SquidGuard. O Netdeep oferece uma interface intuitiva e visualmente simples ao administrador. O resultado dos testes será abordado no próximo capítulo.

As configurações de *firewall* do sistema é intuitivo e pode oferecer um melhor gerenciamento para o administrador da rede. A segurança básica para as redes já está pré-definida conforme a atribuição das interfaces. Na figura 8 são exibidas algumas regras configuradas automaticamente pelo programa.

Figura 8 - Regras atribuídas automaticamente após definição das interfaces

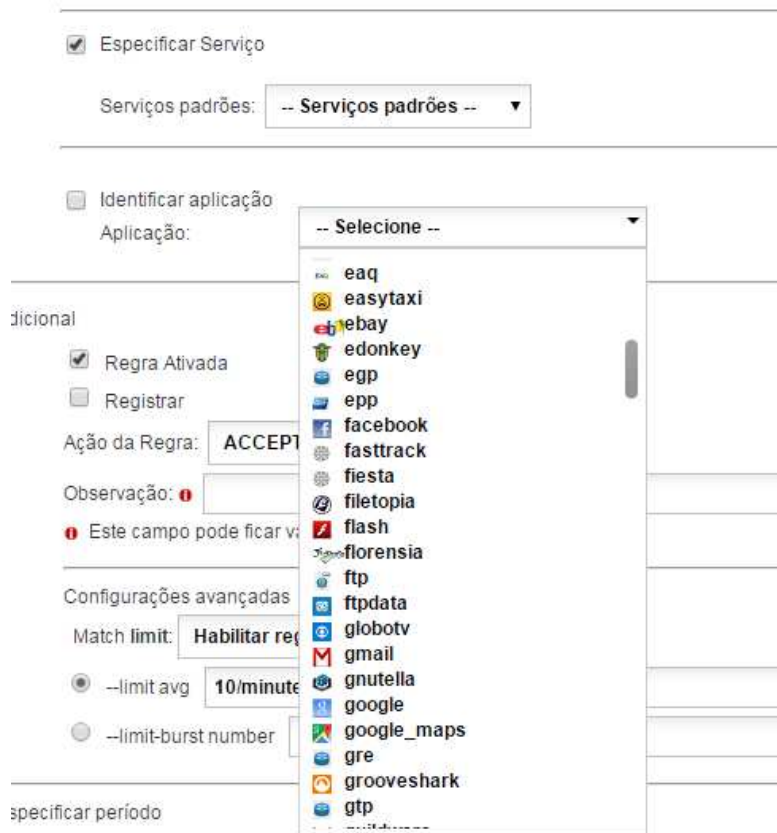
FORWARD (policy DROP 0 packets 0 bytes)							
num	pkts	bytes	target	prot	opt in	out src	dest
1	0	0	BADTCP	all	-- *	* 0.0.0.0/0	0.0.0.0/0
2	0	0	ACCOUNT_FORWARD_IN	all	-- *	* 0.0.0.0/0	0.0.0.0/0
3	0	0	ACCOUNT_FORWARD_OUT	all	-- *	* 0.0.0.0/0	0.0.0.0/0
4	0	0	TCPMSS	tcp	-- *	* 0.0.0.0/0	0.0.0.0/0 tcp flags:0x06/0x02 TCPMSS clamp to PMTU
5	0	0	FW_MARK_IPSEC	all	-- *	* 0.0.0.0/0	0.0.0.0/0
6	0	0	CUSTOMFORWARD	all	-- *	* 0.0.0.0/0	0.0.0.0/0
7	0	0	FW_OUTGOING	all	-- *	* 0.0.0.0/0	0.0.0.0/0
8	0	0	FW_NDS_FORWARD	all	-- *	* 0.0.0.0/0	0.0.0.0/0
9	0	0	ACCEPT	all	-- *	* 0.0.0.0/0	0.0.0.0/0 ctstate RELATED ESTABLISHED
10	0	0	ACCEPT	all	-- !o	* 0.0.0.0/0	0.0.0.0/0 ctstate NEW
11	0	0	DROP	all	-- *	* 127.0.0.0/8	0.0.0.0/0 ctstate NEW
12	0	0	DROP	all	-- *	* 0.0.0.0/0	127.0.0.0/8 ctstate NEW
13	0	0	PORTFWACCESS	all	-- *	* 0.0.0.0/0	0.0.0.0/0 ctstate NEW
14	0	0	FW_LOG	all	-- *	* 0.0.0.0/0	0.0.0.0/0

OUTPUT (policy ACCEPT 18038 packets 3504K bytes)							
num	pkts	bytes	target	prot	opt in	out src	dest
1	18106	3508K	ACCOUNT_OUTPUT	all	-- *	* 0.0.0.0/0	0.0.0.0/0
2	18106	3508K	CUSTOMOUTPUT	all	-- *	* 0.0.0.0/0	0.0.0.0/0

Fonte: Netdeep Firewall da escola técnica em estudo.

As regras mostram políticas de encaminhamento, na linha 9 por exemplo, é habilitada a transmissão de pacotes orientados a conexão, na linha 11 são gerados os logs de acesso. Toda a configuração baseada em comandos é íntima do sistema, isso não é gerenciado pelo administrador, a seleção e aplicação de regras é feita através de menus e botões, e no processamento da requisição a conversão é feita e são interpretados os comandos. A figura 9 mostra um exemplo do menu de configuração apresentada ao administrador da rede.

Figura 9 - Menu de seleção para criação de regras no firewall



Fonte: Netdeep Firewall da escola técnica em estudo.

No menu Serviços Padrões pode ser feita a política baseada em protocolos, no menu Identificar a aplicação, podem ser configuradas regras baseadas em site ou programas específicos, um diferencial oferecido pelo Netdeep Firewall, comparado aos seus concorrentes gratuitos, como o PFSense e o IPFire. Todos os comandos utilizados pela aplicação são baseados em NetFilter, filtro de pacotes nativo de muitas distribuições do Linux. O Netdeep oferece uma interface agradável e um gerenciamento intuitivo baseando-se em IPTables⁴, aplicação robusta, que utiliza o Netfilter.

⁴ Nome da ferramenta da interface do usuário que permite a criação de regras de firewall.

5 TESTES E RESULTADOS

É esperado que toda implementação realizada na instituição tenha seu benefício comprovado. Neste capítulo serão exibidos os testes realizados e um comparativo dos riscos que abrangiam a instituição, após propostas e postas as mudanças. Nas figuras seguintes pode ser observado a tentativa de acesso à sites que tiveram seu tema bloqueado no *proxy*. O bloqueio à conteúdo de jogos (Figura 10) e o bloqueio à *sites* de pornográficos (Figura 11). Com isso comprova-se a eficácia do controle implementado, reduzindo a probabilidade de acesso indevido à conteúdos maliciosos.

Figura 10 - Bloqueio a site de conteúdo de jogos



Fonte: Computador aleatório da instituição de ensino.

Figura 11 - Bloqueio a site de conteúdo pornográfico



Fonte: Computador aleatório da instituição de ensino.

Após os acessos bloqueados, podemos garantir o registro dos *logs*, fornecendo o não-repúdio para a instituição. Na figura 12, os registros dos acessos são exibidos, com data, hora, IP de origem e *site* acessado.

Figura 12 - Registro dos bloqueios realizados no proxy

172.16.3.87	11/11/2016	15:38:37	http://e-poker.net/...
172.16.3.87	11/11/2016	15:39:12	http://videosexo.blog.br/...
172.16.3.87	11/11/2016	15:39:12	http://videosexo.blog.br/favicon.ico...
172.16.3.87	11/11/2016	15:39:12	http://videosexo.blog.br/favicon.ico...
172.16.3.87	11/11/2016	15:39:27	blocklist.addons.mozilla.org/443...
172.16.3.87	11/11/2016	15:39:29	facebook.com/443...

Fonte: Netdeep Firewall da escola técnica em estudo.

Após a implementação dos controles, alguns riscos consequentemente tiveram seus valores alterados, na Tabela 4, são exibidos apenas os riscos que sofreram algum tipo de alteração e o novo controle implementado. Estes podem ser considerados os riscos residuais.

Tabela 4 – Riscos Residuais

ID	ATIVO	VULNERABILIDADE	AMEAÇA	CONTROLE EXISTENTE	PROBABILIDADE	CONSEQUÊNCIA	I.P.T
A	SERVIDORES	Elo com a internet exposto, política permissiva, controles de acesso escassos	Ataques externos que podem causar prejuízo a integridade e disponibilidade da rede	Firewall, com gerenciamento simplificado e facilidade de alteração e aplicação de regras	Improvável	Grande	6
B	COMPUTADOR	Sem controle de acesso na camada de aplicação, ou seja, todo conteúdo web está disponível	Acesso à conteúdos maliciosos que podem infectar o equipamento e toda a rede	Proxy para controle de conteúdos e relatórios dos acessos realizados	Rara	Grande	5
C	SISTEMA ACADÊMICO	Ausência de planejamento de backup da base de dados	Perda da base de dados, por ataque mal intencionado ou exclusão acidental	Plano de Backup	Possível	Pequena	5
H	SISTEMA ACADÊMICO	Imaturidade do software, falta de planejamento no desenvolvimento	Exploração de vulnerabilidade no software ainda não identificadas	Atualizações constantes, contato rápido com o desenvolvedor	Possível	Pequena	5
J	DISPOSITIVOS REDE	Falta de segmentação do ambiente, ocasionando em domínios de broadcast desnecessários	Subtração de dados confidenciais de setores restritos da instituição	Controle de tráfego por portas de um único switch gerenciável da instituição, definição prioridade aos domínios principais	Rara	Pequena	3

K	SERVIDORES	Falta de documentação dos equipamentos e das mudanças realizadas	Dano a um sistema e impossibilidade de retorno ao estado anterior	Quadro usado para informes de atividades realizadas no ambiente	Improvável	Pequena	4
L	COMPUTADOR	Falta de segurança física nos ambientes	Acesso de indivíduos não autorizados aos computadores	Usuários individualizados e controlados quando entram e saem da instituição	Rara	Moderada	5
I.P.T = ÍNDICE DE PRIORIDADE DE TRATAMENTO							

Fonte: Autoria Própria.

Por fim o gráfico 1 mostra o resultado prático dos controles implementados os números de referência no gráfico representam a seguinte fórmula, baseada de obra Segurança de Computadores (STALLINGS e BROWN, 2014):

PARA CADA ATIVO:

(PROBABILIDADE RISCO1 + CONSEQUÊNCIA RISCO1)

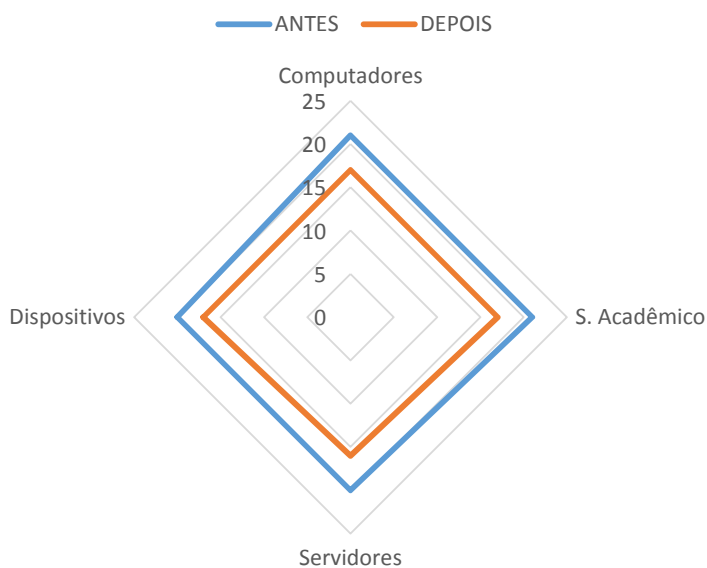
+

(PROBABILIDADE RISCO2 + CONSEQUÊNCIA RISCO2)

+

(PROBABILIDADE RISCO3 + CONSEQUÊNCIA RISCO3)

Gráfico 1 – Nível de risco antes da implantação e riscos residuais



Fonte: Autoria Própria.

Ao fim da análise pode ser destacada a eficácia dos controles implementados uma vez que cumpriram com o objetivo inicial de melhoria do nível de segurança da instituição, o gráfico exposto poderia ter sua linha ainda mais centralizada, o que representaria um risco residual ainda menor, caso recursos fossem dispendidos para o tratamento dos riscos

6 CONSIDERAÇÕES FINAIS

Entre os ensinamentos do trabalho, pode-se destacar a importância de uma análise de riscos para auxiliar um projeto de segurança da informação. Ao mesmo tempo é notada a dificuldade da resolução de alguns riscos, diante da escassez de recursos. Anteriormente destacado, o cenário que se encontrava era repleto de inconsistências e falta de controles. A análise dos riscos trouxe o direcionamento necessário para a identificação dos mesmos, através da análise pessoal do ambiente e sempre em conjunto com os responsáveis pelo setor em questão. Com a base de conhecimento construído, foi possível aplicar os recursos já disponíveis nas atividades que apresentaram o maior índice de prioridade, além de sugerir uma aplicação gratuita que sana em partes alguns dos riscos elencados.

A partir da sugestão feita, todo restante o trabalho destina-se à configuração desta aplicação, procurando realiza-la da melhor maneira possível, suprimindo suas deficiências com a atrelarão a outros serviços anteriormente disponíveis no local. A configuração executada não pretende orientar terminantemente o que será bloqueado ou permitido, e sim fornecer uma base de ambiente na qual as melhores alterações possam ser definidas em conjunto com os funcionários da escola.

É importante destacar o capítulo de Testes e Resultados, este comprova o sucesso das realizações exibindo no gráfico a diminuição do nível dos riscos em todos os ativos, mesmo com os poucos recursos disponíveis.

Este trabalho foi importante para a melhoria da segurança de uma instituição e pode ser usado como base para referência em outros cenários, aplicando os conceitos de segurança da informação e análise de riscos, a fim de otimizar os processos desenvolvidos no negócio.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27002**: tecnologia da informação: técnicas de segurança : código de prática para controles de segurança da informação. Rio de Janeiro, 2013. 99 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27005**: tecnologia da informação: técnicas de segurança : gestão de riscos de segurança da informação. Rio de Janeiro, 2011. 87 p.

DANTAS, Marcus Leal. **Segurança da Informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. (Capítulo 1)

FERUZA, Sattarova; KIM, Tao-hoon. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. **International Journal of Multimedia and Ubiquitous Engineering**, vol. 2, n. 2, 2007.

HAFFERMAN, Leonardo. **Segmentação de Redes com VLAN**. Trabalho de Pós-Graduação em Redes e Segurança de Sistemas Pontifícia Universidade Católica do Paraná. 2009. Disponível em: <<http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Hafferman%20-%20Artigo.pdf>>. Acesso em: 21 Nov. 2016.

LAUREANO, Marcus Aurelio Pchek. **Gestão de Segurança da Informação**. 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 21 Nov. 2016. (Capítulo 2)

NETDEEP SECURE. **Guia de Instalação: Netdeep Secure 3**. Disponível em: <<http://www.netdeep.com.br/secure/wp-content/uploads/2015/05/Guia-de-Instala%C3%A7%C3%A3o-NETDEEP-SECURE-3.pdf>> Acesso em: 10 Nov. 2016.

OSCARSON, Per. Information Security Fundamentals: graphical conceptualisations for understanding. **Security Education and Critical Infrastructures**: IFIP — The International Federation for Information Processing, Nova York, vol. 125, p. 95-107, 2003. Disponível em <http://link.springer.com/chapter/10.1007%2F978-0-387-35694-5_9#page-1>. Acesso em: 21 Nov. 2016.

STALLINGS, William; BROWN, Laurie. **Segurança de Computadores**: princípios e práticas. 2ª ed. Rio de Janeiro: Elsevier, 2014.

ROSA, Adriano Justino; TAMAE, Rodrigo Yoshio; SPINOLLA, Diego de Castro. A importância da utilização de controle de conteúdo no acesso à web. **Revista Científica Eletrônica de Sistemas de Informação**: Faculdade De Ciências Jurídicas e Gerenciais de Garça /FAEG, ano II, n. 3, 2005. Disponível em: < http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/3nnbVkJNsrPRen4H_2013-5-24-17-15-59.pdf>. Acesso em: 21 Nov. 2016.

TREASURY, HM. **The Orange Book**: Management of Risk – Principles and Concepts. 2004. Disponível em: < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf >. Acesso em: 21 nov. 2016.