PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

PROJETO:

IMPLEMENTAÇÃO DE UMA REDE SEGURA DE COMPUTADORES

GRUPO 03

André Souza
Brandon Henrique
Israel Oliveira
Júlio César

PUC Minas

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Sumário

OBJETIVO

Este trabalho visa apresentar um piloto da estrutura de rede, destacando as medidas de segurança atualmente adotadas no ambiente de computadores desenvolvido pelo Grupo 03.

Nosso objetivo é identificar tanto os pontos fortes quanto as possíveis fragilidades, oferecendo recomendações práticas e viáveis para fortalecer a postura de segurança da rede. O intuito é garantir a conformidade com os padrões estabelecidos de segurança

ESTRUTURA

Para simular um ambiente on-primesse, utilizamos o simulador PnetLab, alcançando assim o objetivo de implementar um ambiente completo.

Segmentação de rede por vlans setorizado por area.

Serviços de DNS, FILE SERVER e ACTIVE DIRECTORY – Servidores com o sistema operacional Windows Server 2022 e Linux Debian 12.

Políticas de grupos implementadas no FILESERVER, garantindo assim o acesso apenas a informações corretas.

Serviços habilitados - DNS, NTP e HTTP.

TOPOLOGIA

Centralização da rede através da implantação de um data center, o qual permite um melhor controle e segurança. Possuímos servidores, switchs, firewall e antivirus/endpoints para proteção dos dispositivos de usuários na rede.

A topologia demonstra a segmentação de rede estabelecida de acordo com cada setor, mantendo assim, o isolamento entre as redes/vlans liberando apenas as comunicações necessárias entre elas.

É possível também identificar que os serviços de Active Directory, Fileserver possuem redundância, trazendo mais segurança ao ambiente.

TOPOLOGIA

SUMARIO

VLANS:
200 (ADMINISTRAÇÂO)
IP: 10.11.200.0/24

201 (COMERCIAL)
IP: 10.11.201.0/24

202 (TI)
IP: 10.11.202.0/24

300 (SERVERS)
IP: 10.11.203.0/26

DEVICES NETWORK:

FIREWALL WAN
ISP1: 10.20.30.6
ISP2: 10.20.30.10

FIREWALL LANS
VLAN 200
IP: 10.11.200.1

VLAN201
IP: 10.11.201.1

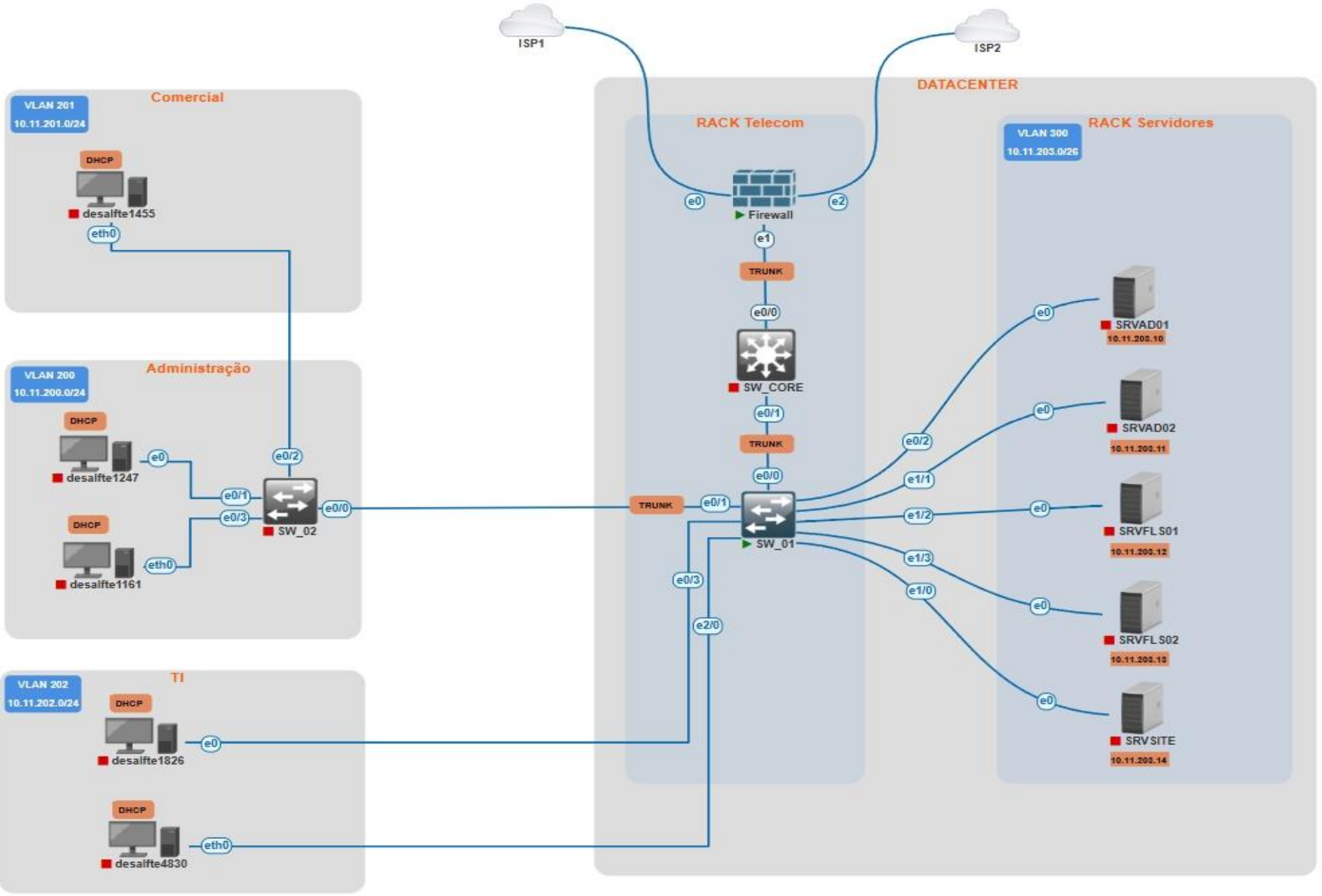
VLAN202
IP: 10.11.202.1

VLAN300
IP: 10.11.203.1

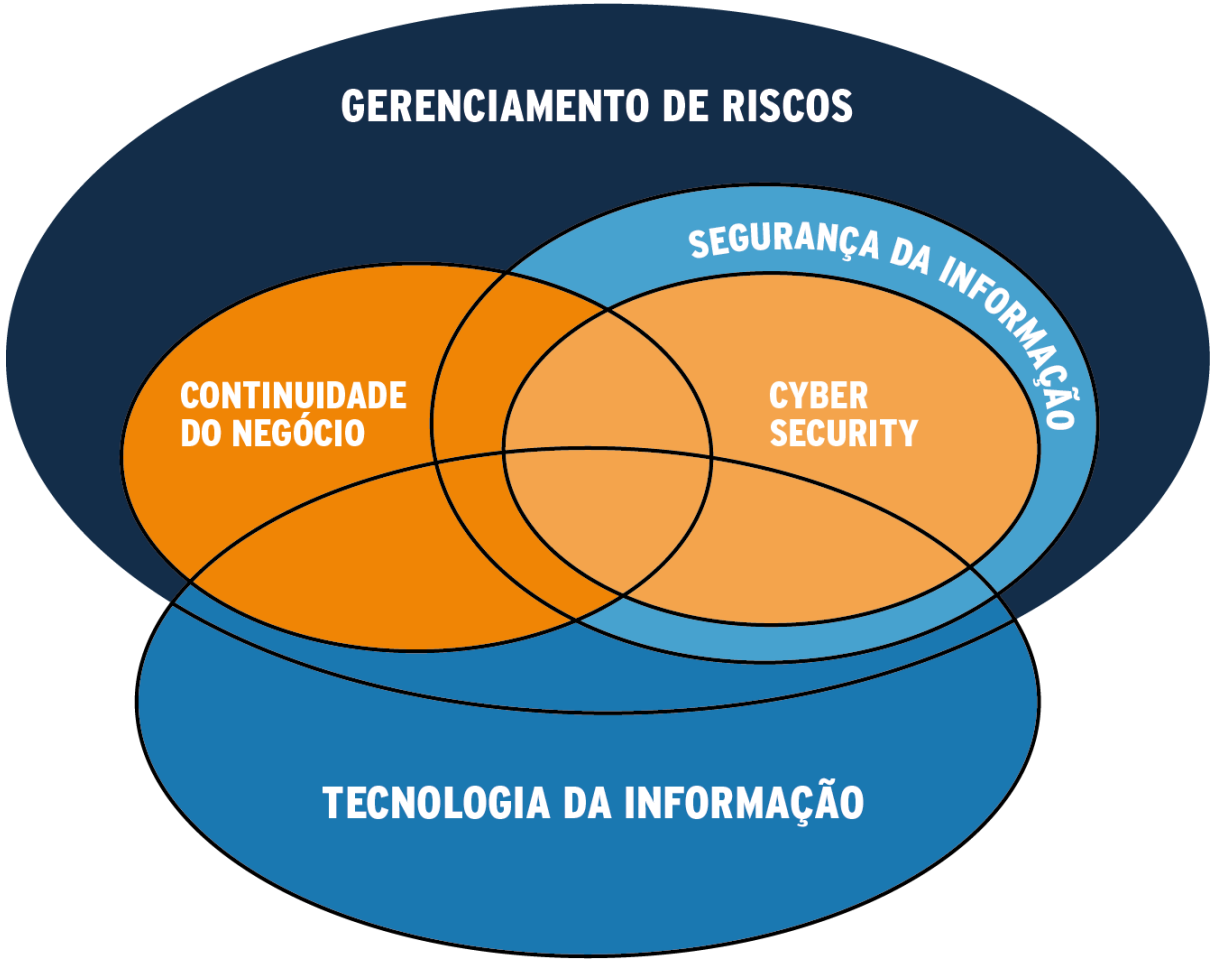
SW_CORE
10.11.200.2

SW_01
10.11.200.3

SW_02
10.11.200.4



GESTÃO DE RISCOS



METODOLOGIA

A análise de riscos é uma etapa fundamental para garantir a segurança e proteção das informações em uma organização. Para isso, é importante utilizar metodologias reconhecidas, tais como a **ISO 31000** e a **ISO 27001**.

- **ISO 31000** - É uma norma que estabelece princípios e diretrizes para a gestão de riscos. Ela fornece um processo sistemático e estruturado para identificar, analisar e avaliar os riscos, permitindo que a organização tome decisões informadas sobre como lidar com eles.

- **ISO 27001** - É uma norma específica para a gestão da segurança da informação. Estabelece requisitos para a implementação de um sistema de gestão de segurança da informação, incluindo a análise de riscos como parte integrante desse sistema.

NORMAS ISO 31000 e ISO 27001

- Utilizados estas normas como referências bem como framewoks e assessoria consultiva da Dvieira Consultoria para:
- Identificar riscos relacionados à segurança da informação (riscos cibernéticos).
- Escolha de riscos para aplicar Análise de Riscos, com base no contexto atualizado do ambiente interno objeto do trabalho.
- Realizar a Avaliação do risco escolhido, classificando seu impacto, probabilidade e conseguinte nível de risco.
- identificar vulnerabilidades e medidas recomendadas para atenuá-las.

DEFINIÇÕES

Risco: é efeito da incerteza nos objetivos. Risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Risco Inerente (Bruto): risco intrínseco ao negócio ou à atividade da Organização, sem considerar a execução de controles e ações para tratar sua exposição, também chamado de risco bruto.

Probabilidade: chance de algo acontecer ou possibilidade de um risco ocorrer. Isso pode ser expresso em termos de ocorrência de uma probabilidade ou frequência.

Agravantes: vulnerabilidades, fatores ou causas que aumentem a probabilidade do risco se materializar.

Impacto: resultado ou efeito de um risco, considerando os controles corretivos existentes para mitigá-lo. O impacto de um risco pode ser positivo ou negativo em relação à estratégia ou aos objetivos. Também denominado de severidade/criticidade para riscos operacionais ou ocupacionais.]

Atenuantes: medidas, controles ou ações que tem o potencial de impedir a materialização do risco ou atenuar seu impacto no caso de materialização.

Nível de Risco: magnitude de um risco resultante da combinação dos fatores de probabilidade e impacto.

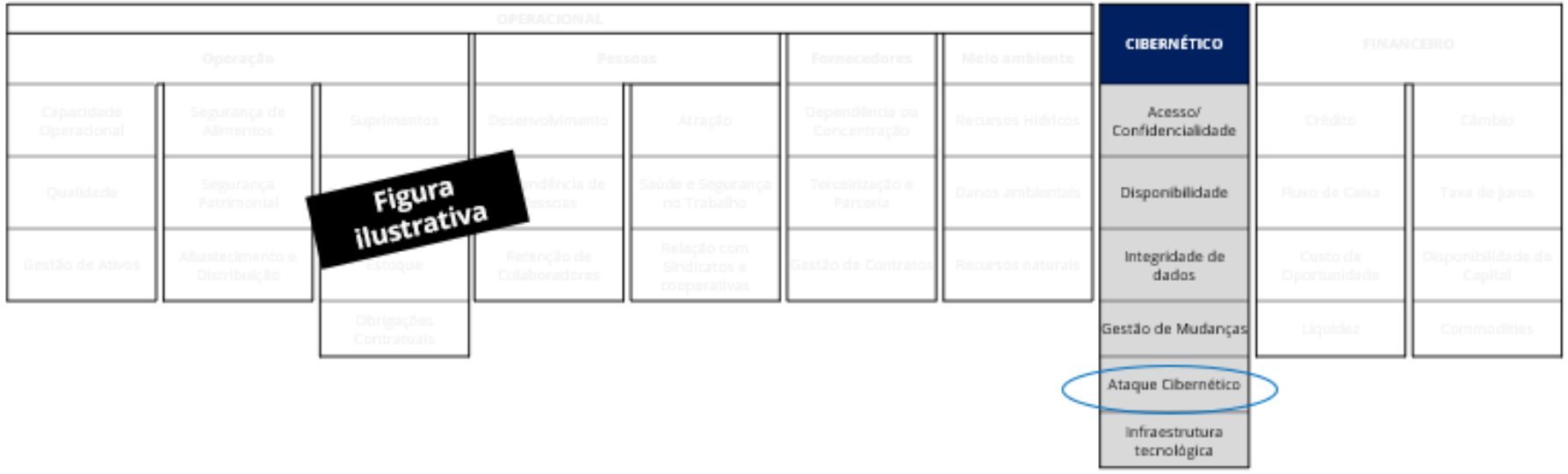
Gestão de Riscos: gerenciamento de riscos corporativos composto por estrutura, princípios e processo conduzido pelo conselho de administração, diretoria e demais empregados, aplicado para: (i) identificar em toda a organização eventos em potencial, capazes de afetá-la; (ii) administrar os riscos de modo a mantê-los compatíveis com o apetite de risco; e (iii) possibilitar garantia satisfatória do cumprimento dos seus objetivos.

IDENTIFICAÇÃO

O gerenciamento de riscos corporativos abrange pilares e categorias para distinguir a natureza dos riscos organizacionais e suas respectivas estratégias de tratamento, como por exemplo, riscos estratégicos, financeiros, riscos operacionais, de saúde e segurança, riscos legais, riscos de compliance etc. Este portifólio é desenvolvidos e personalizado para cada negócio e organização. Para fins deste trabalho escolheremos um risco do pilar Cibernético.

Riscos Cibernéticos: eventos que podem expor os ativos de informação, afetar a confidencialidade das informações e comprometer a integridade e disponibilidade de dados ou sistemas tecnológicos da Companhia.

Para aplicação da metodologia o risco de Ataque Cibernético foi escolhido.



Ataque Cibernético – Ficha de Riscos

Pilar	Categoria	Risco	Avaliação – Nível de Risco
Cibernético	Cibernético	Ataque Cibernético	

Definição	Principais consequências	Volumetria
Refere-se à tentativa de destruir, expor, alterar, desativar, roubar, obter acesso não autorizado ou fazer uso não autorizado de um ativo da Companhia.	• Indisponibilidade dos ambientes corporativos, e-commerce, financeiro e das ferramentas de comunicação com clientes, fornecedores e representantes comerciais. • Vazamento de informações estratégicas e confidenciais ao negócio, bem como dados sensíveis de clientes , fornecedores e funcionários	Tentativas de ataques cibernéticos e incidentes de segurança registrados x quantidade de vulnerabilidades classificadas como relevantes (médias, altas e críticas).

Análise do Ambiente Interno

Agravante	Atenuante
• Elevado número de tentativas de invasões • Ausência de monitoramento de ameaças contemplando todos os ativos tecnológicos . • Vulnerabilidade na Proteção de dados de clientes (LGPD) • Ausência de investimentos em Segurança da Informação • Equipe de segurança da informação reduzida • Acúmulo de funções no time de Tecnologia da Informação	• Firewalls: proteção de perímetro para entrada e saída de internet em todas as unidades. • WAF (Web Application Firewall): proteção contra ataques para todos os sites e sistemas publicados para internet. • Anti-Spam: proteção contra ameaças que podem se disseminar por e-mail. • Data center será migrado 100% para a AWS até agosto/2024 (atualmente está híbrido com Ativas e AWS). • Seguro para cobrir riscos cibernéticos • Utilização de solução de gestão de vulnerabilidades. • Utilização de solução de gestão de patchs (WSUS + System Center)

Impacto	Mínimo	Baixo	Moderado	**Alto**	Muito Alto

Probabilidade	Rara	Baixa	Possível	**Provável**	Quase Certo

Ataque Cibernético – Indicador de Risco

AC01 – Tentativas de Invasão, contenção e resposta a Incidentes de Segurança			
Tentativa de destruir, expor, alterar, desativar, roubar, obter acesso não autorizado ou fazer uso não autorizado de um ativo da Companhia.			
Objetivo do Indicador de Risco			
Aplicar corrigir e monitorar correções de versões, vulnerabilidades e atualizações em aderência às ferramentas e estratégias de Cyber Security definidas pela Companhia.			
Método do Indicador de Risco			
Quantitativo: 1- Apurar o volume atual de ofensas e ataques monitoradas através da plataforma Siem; 2- Apurar as vulnerabilidades identificadas no periodo, apuradas através da Plataforma de Gestão de vulnerabilidades; 3- Classificar as vulnerabilidades de acordo com nível de criticidade: crítica, alta, média e baixa. Fórmula: quantidade de ofensas|ataques registrados no mês x quantidade de vulnerabilidades classificadas como relevantes (críticas, altas e médias)			
Unidade de Medida	**Periodicidade**	**Responsável**	**Fonte**
Índice numérico	Mensal	Responsável primário pelo monitoramento (Gestor do risco): André Nascimento	Medição mensal de ofensas através da plataforma de Siem Vulnerabilidades apontadas na Plataforma de Gestão de vulnerabilidades
Avaliação do Indicador de Risco	**Meta**	**Faixas de Avaliação**	
Quanto maior o indicador de ataques/ofensas, maior a exposição da Companhia ao risco de vazamento, perda, extravio e roubo de informações eletrônicas.	Índice de ofensas/ataques destinadas ao ambiente sobre a quantidade de vulnerabilidade relevantes igual ou inferior à 800 **Nota da Dvieira Consultoria:** meta indicada para cenário otimista deve ser igual ou inferior à 800 para fins de exemplo aplicável a trabalhos científico.		Índice de ofensas/ataques x vulnerabilidades com resultado até 800
			Índice de ofensas/ataques x vulnerabilidades com resultado de De 801 a 1.000
			Índice de ofensas/ataques x vulnerabilidades com resultado acima de 1.000
Observação:			

RESULTADOS E RECOMENDAÇÕES

Com base na avaliação de risco realizada, identificamos que a probabilidade e o impacto de um ataque cibernético são altos. Isso se deve ao elevado número de tentativas de invasões, à ausência de monitoramento de ameaças contemplando todos os ativos tecnológicos, à vulnerabilidade na proteção de dados pessoais de clientes, empregados e terceiros (LGPD), à ausência de investimentos em segurança da informação, à equipe de segurança da informação reduzida e ao acúmulo de funções no time de Tecnologia da Informação.

Com base nesses resultados, recomendamos que a organização priorize as seguintes ações e medidas de segurança:

1. Investir em recursos humanos: contratar profissionais especializados em segurança da informação para fortalecer a equipe e reduzir o acúmulo de funções no time de Tecnologia da Informação.

2. Implementar um sistema de monitoramento de ameaças abrangente: é essencial ter visibilidade de todas as atividades e ameaças em tempo real, para identificar e responder rapidamente a possíveis ataques.

3. Realizar diagnóstico de maturidade e adequação à LGPD e fortalecer a proteção de dados pessoais: garantir que a organização esteja em conformidade com a LGPD e implementar medidas adicionais de proteção de dados, como classificação da informação, política, criptografia e controle de acesso.

RESULTADOS E RECOMENDAÇÕES

4. Realizar investimentos em segurança da informação: destinar recursos financeiros para aquisição de ferramentas e tecnologias de segurança, como soluções de prevenção de intrusões, detecção de malware e autenticação multifator.

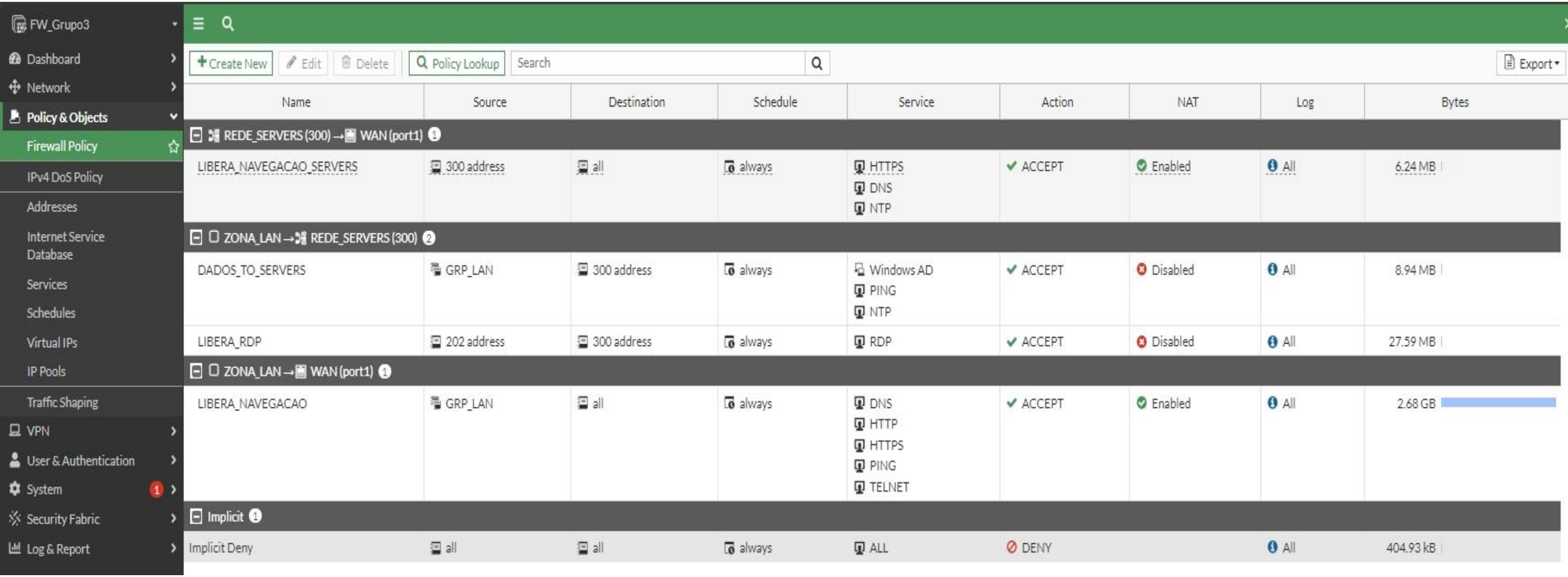
5. Realizar treinamentos e conscientização em segurança da informação: capacitar os colaboradores para identificar e evitar possíveis ameaças, como phishing e engenharia social.

6. Realizar testes de penetração e avaliações de vulnerabilidades: identificar e corrigir possíveis falhas de segurança antes que sejam exploradas por atacantes.

7. Revisar e atualizar regularmente as políticas e procedimentos de segurança da informação: garantir que as diretrizes estejam alinhadas com as melhores práticas e que sejam revisadas e atualizadas conforme necessário.

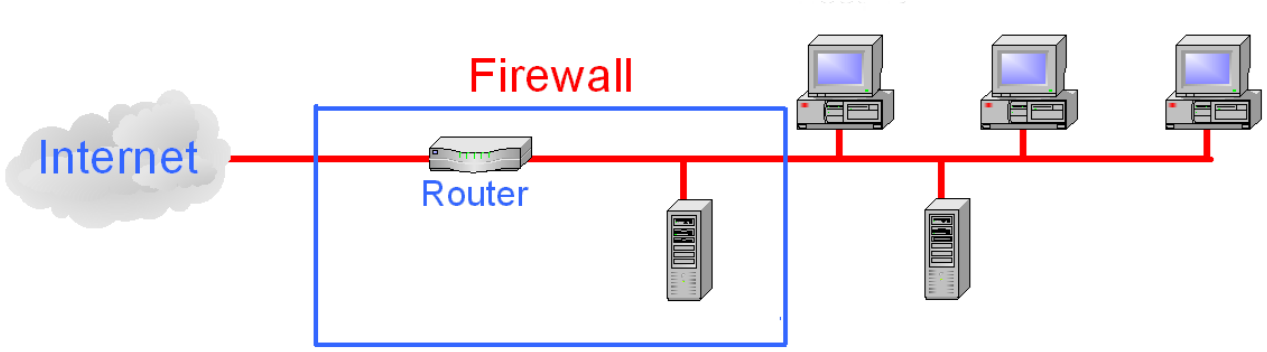
Ao implementar essas medidas em ordem de prioridade, a organização estará fortalecendo sua postura de segurança da informação e reduzindo os riscos de um ataque cibernético. É importante ressaltar que a segurança da informação é um processo contínuo e que deve ser revisado e atualizado regularmente para se adaptar às novas ameaças e vulnerabilidades.

FIREWALL FORTIGATE
POLÍTICAS DE SEGURANÇA



FIREWALL

Firewall - Estação Client



FIREWALL - Sistema de segurança para desempenhar um importante papel . Todas as conexões entre as rede, estão configuradas/autorizadas pelo Firewall.

MELHORIAS

Graylog
Inclusão de um servidor Linux Debian 12 com a solução Graylog, pois é uma ferramenta essencial para auditoria de dados, pois fornece um histórico de todas as atividades que ocorrem em uma rede ou sistema. Os registros de logs podem ser usados para detectar alterações nos dados, verificar a conformidade com regulamentos e investigar incidentes de segurança.

Antivirus
Inclusão de um antivírus de próxima geração (NGAVs), mantendo assim os endpoints seguros com uma proteção que combina segurança baseada em IA e Machine Learning, permitindo a aprendizagem contínua com as detecções do passado de modo a aperfeiçoar os recursos de prevenção do futuro.

Backup
Inclusão de uma ferramenta robusta de backup, pois é essencial para proteger os dados das empresas. Ele ajuda a garantir a continuidade dos negócios, reduzir custos e proteger contra perda de dados. Alguns exemplos de ações que podem comprometer os dados são: Falhas de hardware ou software, ataques cibernéticos e até mesmo desastres naturais. A escolha da melhor estratégia de backup depende das necessidades específicas da empresa. Para nosso cenário, escolhemos a ferramenta Veeam Backup & Replication

Firewall - HA
Inclusão de um segundo firewall, mantendo alta disponibilidade (HA), deste modo, se um dos firewalls falhar, o outro assumirá automaticamente o controle. Isso garante que a rede permaneça protegida e disponível, mesmo em caso de falha de hardware ou software.

CONCLUSÃO

É evidente que um projeto de rede, independentemente de seu porte, requer um planejamento e estruturação adequados para prevenir vulnerabilidades que possam impactar seu funcionamento e todo o ecossistema empresarial.

A implementação de diretrizes de segurança e treinamentos coletivos são passos frequentemente negligenciados no ambiente tecnológico. Nessa fase, concentramos nossa atenção na auditoria das diretrizes já implementadas, abrangendo a revisão completa da análise de riscos, planos de contingência, e na promoção de uma cultura de segurança de rede que permeie todos os setores da empresa, independentemente de sua área de atuação.

É crucial enfatizar que a revisão abrangente da análise de risco e a formulação de planos de contingência são passos fundamentais para garantir a segurança da rede e minimizar os riscos de vulnerabilidades. Além disso, a criação de uma cultura de segurança de rede é essencial para que todos os funcionários compreendam os riscos de segurança e estejam preparados para agir em casos de incidentes

OBRIGADO