UNIVERSIDADE FEEVALE

LUIZ HENRIQUE LISBOA

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Novo Hamburgo

2021

LUIZ HENRIQUE LISBOA

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale.

Orientador: Vandersilvio da Silva

Novo Hamburgo

2021

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram e me apoiaram para a realização desse trabalho de conclusão, em especial:

Aos amigos e às pessoas que convivem comigo diariamente - nos períodos mais difíceis do trabalho me incentivaram a continuar.

RESUMO

Este estudo foi elaborado com o objetivo demonstrar na prática a melhora que se obtém quando se utiliza de boas práticas em relação a segurança da informação e tecnologia da informação. O principal objetivo deste trabalho é a realização da análise de uma empresa e aplicação de técnicas e melhorias de segurança no ambiente. Os objetivos gerais são trazer essa visão aos gestores e responsáveis pela segurança da informação a terem o devido cuidado e proteção com seus ativos. Neste estudo foi realizado um levantamento junto com a empresa analisada a fim de identificar pontos onde poderiam evoluir visando sempre agregar melhorias e conhecimentos aos envolvidos. Em segundo momento foi elaborado um relatório onde constam os itens a serem trabalhados e por final foi realizado a aplicação destes itens. Ao se falar em gestão de risco, automaticamente se trabalha de cenários cujas consequências afetam a confidencialidade, integridade e disponibilidade. O gerenciamento de riscos pode ajudar as organizações a atingir seus objetivos com mais segurança, evitando possíveis problemas com perda de dados, economizando recursos e tempo.

Palavras-chave: Gestão de risco. Gestão de informação. ISO/IEC 27005. Segurança da Informação. CID.

ABSTRACT

This study was prepared with the objective of demonstrating in practice the improvement that is obtained when good practices are used in relation to information security and information technology. The main objective of this paper is to conduct an analysis of a company and apply safety techniques and improvements to the environment. The overall goals are to bring this insight to managers and information security officers to take due care and protection of their assets. In this study, a survey was carried out with the company analyzed in order to identify points where they could evolve, always aiming to add improvements and knowledge to those involved. The second step was to prepare a report containing the items to be worked on, and finally to apply these items. When talking about risk management, one automatically deals with scenarios whose consequences affect confidentiality, integrity and availability. Risk management can help organizations achieve their goals more securely, avoid potential data loss problems, and save resources and time.

Key words: Risk management. Information management. ISO/IEC 27005. Information security. CID.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ATP	Applicant Tracking System
AD	Active Directory
ACL	Access Control List
CRC	Cyclic Redundancy Check
DMZ	Zona Desmilitarizada
DDoS	Denial Of Service
DNS	Domain Service Name
DLP	Data Loss Prevention
EoL	End of Life
IEC	Comissão Eletrotécnica Internacional
IDS	Intrusion Detection System
ISO	Organização Internacional de Normalização
IPS	Intrusion Prevention System
LGPD	Lei Geral de Proteção de Dados
NAT	Network Address Translation
NBA	Análise do Comportamento de Rede
NBR	Norma Técnica brasileira
NIPS	Sistema de prevenção de intrusão baseado em rede
SI	Segurança da informação
SGSI	Sistema de Gestão de Segurança da Informação
SO	Sistema Operacional
SLA	Service Level Agreement
SSH	Secure Shell
SNMP	Protocolo Simples de Gerência de Rede
TCP	Transmission Control Protocol
TIC	Tecnologia da informação
TI	Tecnologia da Informação
TS	Terminal Service
VPN	Rede Privada Virtual
WAF	Web application firewall

WIPS	Sistema de prevenção de intrusão baseado em wi-fi
XSS	Cross-site Scripting

SUMÁRIO

INTRODUÇÃO

A segurança da informação pode ser entendida como um processo de proteger as informações das ameaças para sua integridade, disponibilidade e confidencialidade. (BAEL, 2005, p1). Bael (2008) ainda comenta que a segurança deve ser feita em diferentes camadas, com mais de uma alternativa de proteção. Uma vez que a proteção apresente alguma vulnerabilidade e seja superada, se esta for a única proteção, a informação já se torna exposta. A segurança em camadas abrange controles físicos, lógicos e manuais.

Segurança da informação é a proteção de informações, sistemas, recursos, e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança. (DIAS, 2001, p. 41).

Para Sêmola (2003, p43), a segurança da informação é uma área do conhecimento dedicada à proteção de ativos da informação, contra acessos indevidos e alterações indesejadas ou sua indisponibilidade.

Este trabalho tem como objetivo fazer uma análise detalhada da empresa a ser analisada, investigando pontos importantes para que se tenha uma gestão da segurança da informação funcional, minimizando os riscos que a empresa corre e mantendo o ambiente totalmente funcional.

A análise realizada se baseia especialmente na ISO 27005, os pontos analisados são trazidos para o ambiente de debate e verificado seus impactos na organização.

Posterior mente foi elaborado um plano de ação com metas e prazos, e os itens foram separados por níveis de criticidade, onde sempre foi procurado fazer os ajustes nos mais críticos por primeiro.

O propósito deste trabalho é trazer a tona a fragilidade de empresas que normalmente acreditam estar seguras, demonstrando como sempre se pode melhorar em vários fatores, outro ponto importante é trazer para os diretores e gerentes a atual necessidade de investimento em segurança da informação. Atualmente o maior bem de uma empresa é seus clientes e suas informações.

O objetivo é mostrar que apesar de aparentemente termos uma infraestrutura de rede bem montada e planejada sempre é possível melhorá-la, com o passar do tempo ir realizando análises para monitorar possíveis pontos críticos. O objetivo não é a aplicabilidade de segurança

em sistemas específicos, ou até mesmo em toda a empresa, mas sim destacar a importância e pontos relacionados a segurança do ambiente que precisam ter alguns cuidados especiais.

A PWC, uma *network* de firmas independentes que estão presentes em mais de 155 territórios, que presta serviços de auditoria. Realizou uma pesquisa com executivos de negócios de segurança e TI, onde apontou que 71% afirmam contar com um executivo sênior que faz a comunicação sobre a importância da segurança para a corporação. A comunicação interna é essencial para o sucesso das demais iniciativas, salientado por PWC (2014).

Para apenas 17% das organizações a segurança da informação é eficaz. A ineficácia na área de segurança atinge 83% das organizações (ERNEST; YOUNG, 2013).

1. REFERENCIAL TEÓRICO

A seção 1, traz o referencial teórico, onde é definido conceitos sobre diversos itens que fazem parte da gestão de risco de segurança da informação, entre eles, na seção 1.1 consta a definição de ameaça e seus tipos, na seção 1.2 se tem as vulnerabilidades, explicação e exemplos, já na seção 1.3 é apresentado métodos para avaliação dessas vulnerabilidades. A partir da seção 1.4 é apresentada a definição de risco, a seção 1.5 traz a gestão de risco com seus conceitos, para que na seção 1.6 se tenha critérios para identificação dos riscos. Na seção 1.7 é apresentado o processo de gestão de risco. A seção 1.8 ilustra o tratamento do risco de SGSI, suas ações, retenção, ação para evitar e fala sobre a aceitação dos riscos residuais ou que não puderam ser tratados.

Na seção 2 consta a metodologia, é explicado como foi elaborado este estudo. Na seção 3 é exibido a análise da empresa. Na seção 4 são exploradas as vulnerabilidades encontradas, a partir da seção 4.1 até a seção 4.14 é explicado sobre cada uma das vulnerabilidades encontradas.

A seção 5 traz se inicia as soluções propostas, na seção 5.1 são apresentadas as soluções a curto prazo, na seção 5.2 as soluções a médio prazo e na seção 5.3 as soluções a longo prazo. A seção 6 traz uma demonstração de acompanhamento dos itens.

Na seção 7 se inicia as correções que foram aplicadas na empresa demonstrando e explicando o que foi realizado, indo da seção 7.1 com o item de restrição de acesso à internet, até o item 7.13 com a ausência de centralizador de logs

1.1 AMEAÇAS

A norma ISO 27005 traz alguns exemplos de ameaças, conforme o quadro a seguir mostra. As ameaças podem ser intencionais, acidentais ou de origem ambiental (natural) e podem resultar, por exemplo, no comprometimento ou na paralisação de serviços essenciais. O quadro 1 lista as ameaças e identifica o tipo de origem para cada tipo de ameaça. A letra I é utilizada para ameaças intencionais; a letra A é usada para ameaças de origens humanas que podem comprometer acidentalmente os ativos; e a letra N é utilizada para todos os incidentes que não são provocados pela ação dos seres humanos.

1.1.1 Tipos de ameaça

A ISO 27005 traz alguns exemplos de ameaças e sua origem, conforme quadro 1.

Quadro 1 – Exemplos de ameaças e sua origem

Tipo	Ameaças	Origem
Dano físico	Fogo	A, I, N
	Água	A, I, N
	Poluição	A, I, N
	Acidente grave	A, I, N
	Destruição de equipamento ou mídia	A, I, N
	Poeira, corrosão, congelamento	A, I, N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno vulcânico	N
	Fenômeno meteorológico	N
	Inundação	N
Paralisação de serviços essenciais	Falha do ar-condicionado ou do sistema de suprimento de água	A, I, N
	Interrupção do suprimento de energia	A, I, N
	Falha do equipamento de telecomunicação	A, I
Distúrbio causado por radiação	Radiação eletromagnética	A, I, N
	Radiação térmica	A, I, N
	Pulsos eletromagnéticos	A, I, N
Comprometimento da informação	Interceptação de sinais de interferência comprometedores	I
	Espionagem à distância	I
	Escuta não autorizada	I
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A, I
	Dados de fontes não confiáveis	A, I

Continuação

Tipo	Ameaças	Origem
Comprometimento da informação	Alteração de *hardware*	I
	Alteração de *software*	A, I
	Determinação da localização	I
Fichas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Saturação do sistema de informação	A, I
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de *softwares* falsificadas ou ilegais	A, I
	Comprometimento dos dados	I
	Processamento ilegal de dados	I
Comprometimento de funções	Erro durante o uso	A, I
	Forjamento de direitos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, I, N

Fonte: ISO/IEC 27005, 2011.

1.1.2 Ameaças Humanas

Quadro 2 – Exemplos de ameaças humanas

Origem das ameaças	Motivação	Possíveis consequências
Hacker, *cracker*	Desafio	*Hacking*
	Ego	Engenharia social
	Rebeldia	Invasão de sistemas, infiltrações e entradas não autorizadas
	Status	Acesso não autorizado ao sistema
	Dinheiro	

Continuação.

Origem das ameaças	Motivação	Possíveis consequências
Criminoso digital	Destruição de informações Divulgação ilegal de informações Ganho monetário Alteração não autorizada de dados	Crime digital Ato fraudulento Suborno por informação *Spoofing* (fazer-se passar por outro) Invasão de sistemas
Terrorista	Chantagem Destruição Exploração Vingança Ganho político Cobertura da mídia	Bomba/terrorismo Guerra de informação Ataque a sistemas Invasão de sistemas Alteração do sistema
Espionagem industrial (serviços de inteligência, governos estrangeiros, empresas)	Vantagem competitiva Espionagem econômica	Garantir vantagem de posicionamento defensivo Garantir vantagem política Exploração econômica Furto de informação Violação de privacidade das pessoas Engenharia social Invasão de sistemas Acesso não autorizado ao sistema
Pessoal interno (funcionários mal treinados, insatisfeitos, negligentes, desonestos ou dispensados)	Curiosidade Ego Obtenção de informações úteis para serviços de inteligência Ganho monetário Vingança	Agressão a funcionário Chantagem Vasculhar informação de propriedade exclusiva Uso improprio de recurso computacional Fraude e furto

Continuação.

Origem das ameaças	Motivação	Possíveis consequências
Pessoal interno (funcionários mal treinados, insatisfeitos, negligentes, desonestos ou dispensados)	Erros e omissões não intencionais	Suborno por informação Entrada de dados falsificados ou corrompidos Interceptação Código malicioso

Fonte: ISO/IEC 27005, 2011.

1.2 IDENTIFICAÇÃO DE VULNERABILIDADES

O quadro 3 desenvolvido pela ISO 27005 fornece exemplos de vulnerabilidades, incluindo exemplos de ameaças que poderiam explorar tais vulnerabilidades.

Quadro 3 – Exemplos de vulnerabilidades e ameaças

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Manutenção insuficiente/instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento
	Inexistência de um controle eficiente de mudança de configuração	Erro durante o uso
	Sensibilidade a variação de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Falta de cuidado durante descarte	Furto de mídia ou documentos
	Realização de cópias não controladas	Furto de mídia ou documentos
Software	Procedimentos de teste de software insuficientes ou inexistentes	Abuso de direito

Continuação.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Software	Falhas conhecidas no *software*	Abuso de direito
	Não execução do logout ao se deixar uma estação de trabalho desassistida	Abuso de direito
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direito
	Atribuição errônea de direitos de acesso	Abuso de direito
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados	Comprometimento dos dados
	Interface de usuário complicada	Erro durante o uso
	Documentação inexistente	Erro durante o uso
	Configuração de parâmetros incorreta	Erro durante o uso
	Datas incorretas	Erro durante o uso
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para autenticação de usuários	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de direitos
	Gerenciamento de senhas mal-feito	Forjamento de direitos
	Serviços desnecessários que permanecem habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Inexistência de controle eficaz de mudança	Defeito de *software*
	Download e uso não controlados de software	Alteração de *software*
	Inexistência de cópias de segurança (*back-up*)	Alteração de *software*

Continuação.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Software	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
Rede	Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junção de cabeamento mal-feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Transferência de senhas em claro	Espionagem à distância
	Gerenciamento de rede inadequado (quanto a flexibilidade de roteamento)	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos Humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados

Continuação.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Recursos Humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos
	Inexistência de políticas para uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamento
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e aposentos	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registro e a remoção de usuários	Abuso de direito
	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direito
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Indisponibilidade de recursos humanos

Continuação.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Organização	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direito
	Inexistência de auditorias periódicas (supervisão)	Abuso de direito
	Inexistência de procedimentos para a identificação, análise e avaliação de riscos	Abuso de direito
	Inexistência de relatos de falhas de arquivos (logs) de auditoria das atividades de administradores e operadores	Abuso de direito
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Acordo de nível de serviço (SLA) inexistente ou insuficiente	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de procedimento de controle de mudanças	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de um procedimento formal para o controle da documentação do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a supervisão dos registros do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações
	Inexistência de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondência eletrônica (e-mail)	Erro durante o uso

Continuação

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Organização	Inexistência de procedimentos para a instalação de softwares em sistemas operacionais	Erro durante o uso
	Ausência de registros nos arquivos de auditoria (logs) de administradores e operadores	Erro durante o uso
	Inexistência de procedimentos para a manutenção de informações classificadas	Erro durante o uso
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções	Erro durante o uso
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos de funcionários	Processamento ilegal de dados
	Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação	Furto de equipamentos
	Inexistência de uma política formal sobre o uso de computadores moveis	Furto de equipamentos
	Inexistência de controle sobre ativos fora das dependências	Furto de equipamentos
	Política de mesas e telas limpas (clear des and clear screen) inexistentes ou insuficientes	Furto de mídia ou documentos
	Inexistência de autorizações para instalação de processamento de informações	Furto de mídia ou documentos
	Inexistência de mecanismos estabelecidos para o monitoramento de violação da segurança	Furto de mídia ou documentos
	Inexistência de análises críticas periódicas por parte da direção	Uso não autorizado de equipamento

Continuação.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Organização	Inexistência de procedimento para relato de fragilidades ligadas à segurança	Uso não autorizado de equipamento
	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	Uso de cópia de *software* falsificadas ou ilegais

Fonte: ISO/IEC 27005, 2011.

1.3 MÉTODOS PARA AVALIAÇÃO DE VULNERABILIDADES

A ISO 27005 aborda alguns métodos de avaliação de vulnerabilidades, tais como:

- Ferramentas automatizadas de procura por vulnerabilidades;
- Avaliação de testes de segurança;
- Teste de invasão;
- Análise crítica de código.

Ferramentas automatizadas tem como objetivo varrer um grupo de computadores ou uma rede em busca de vulnerabilidades e falhas na rede, por exemplo, serviços vulneráveis como o FTP, *sendmail*. Porém nem todas as vulnerabilidades significam realmente uma vulnerabilidade real.

Avaliação de testes de segurança (ATS) é uma técnica utilizada na identificação de vulnerabilidades em sistemas TIC, ela inclui roteiros de procedimentos e lista de resultados esperados. Seu propósito é testar a eficácia dos controles de segurança de um sistema TIC. O objetivo é assegurar que os controles aplicados satisfaçam as especificações de segurança do software e do hardware.

Testes de invasão, podem ser usados para complementar o processo de análise crítica dos controles de segurança, seu objetivo é assegurar que as diversas facetas do sistema TIC estejam protegidas. Este procedimento visa avaliar a capacidade do sistema de TIC de resistir a tentativas intencionais de se driblar a segurança do sistema testando assim a fonte da ameaça e identificando possíveis falhas no esquema de proteção do sistema.

Análise crítica de código é a mais minuciosa forma de avaliação de vulnerabilidades, tem como objetivo ajudar a identificar vulnerabilidades de um sistema.

Ferramentas e técnicas de invasão podem gerar falso positivo. Para que se possa testar vulnerabilidades especificas é preciso saber a configuração exata do sistema e das aplicações instaladas no sistema testado, caso contrário pode não ser possível explorar determinada vulnerabilidade com sucesso.

Entre os métodos existentes, podem ser incluídos os seguintes:

- Entrevista com pessoas e usuários;
- Questionários;
- Inspeção física;
- Análise de documentos;

1.4 RISCO

Risco é o efeito das incertezas nos objetivos, sendo um efeito de desvio ao resultado esperado. Os objetivos podem ter diferentes aspectos e podem aplicar-se em diferentes níveis. O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências ou em sua combinação.

O risco é inerente a toda atividade humana. A capacidade de definir o que acontecerá no futuro e optar entre várias alternativas é central às sociedades contemporâneas. A administração do risco nos guia por uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros e isto inclui a informação e a complexa tecnologia envolvida em seu processo (BERNSTEIN, 1997).

Para Wheeler (2001), risco em segurança da informação é a expectativa da perda da confidencialidade, integridade, disponibilidade e responsabilidade da informação.

O risco em segurança da informação é muitas vezes expresso em termos de uma combinação de consequências de um evento e a probabilidade associada de ocorrência.

A prevenção da perda, dano, destruição ou acesso não autorizado à informação processada por organizações é uma evolução contínua e a segurança da informação tem chamado cada vez mais a atenção de pesquisadores, profissionais, jornalistas, legisladores e cidadãos. Governos e organizações se sensibilizam e investem cada vez mais na segurança de seus ativos de informação, auxiliando não somente a tomada de decisões, mas também a melhoria e continuidade de suas operações (JOURDAN et al., 2010).

A tecnologia é um artefato geralmente visível na organização. Tal evidência é o resultado da implementação de componentes de segurança da informação tais como de riscos e política de segurança (SCHEIN, 1985).

Os sistemas de informação estão sujeitos a ameaças que podem tanto oferecer oportunidades como ter impactos negativos sobre as operações da organização, incluindo missão, funções, imagem, reputação, os ativos, os indivíduos, assim como comprometer a confiabilidade, integridade, autenticidade e disponibilidade de informações que estão sendo processados, armazenados ou transmitidos por esses sistemas (NIST, 2010).

1.5 GESTÃO DE RISCO

Influenciadas por suas necessidades, objetivos, exigências de segurança, processos, tamanho e estrutura, as organizações tendem a especificar e implementar estrategicamente um Sistema de Gestão de Segurança da Informação (SGSI) que atenda às necessidades da organização. Em sua recente atualização, a norma ISO/IEC 27001:2013 padroniza definições e estruturas de diferentes padrões ISO, alinhando-se com outros importantes padrões já existentes e propiciando uma gestão de riscos ainda mais efetiva ao incluir requisitos para a avaliação e tratamento de riscos de segurança da informação (ISO/IEC 27001, 2013).

Por mais que Moreira (2001, p. 3) comenta que “a informação vem sendo considerada como um dos principais ativos para as empresas, e, desta forma, a Segurança da informação vem se tornando uma real necessidade no dia a dia das organizações para proteger seus segredos de negócios ou suas estratégias comerciais, sendo considerada hoje fator de sobrevivência e competitividade para as corporações modernas”, as estatísticas demonstram que a fraude na informática é um problema em escala mundial, que tem custado bilhões de dólares às organizações. Apenas em 2002 nos Estados Unidos devido a funcionários insatisfeitos as perdas ultrapassaram a US$MM 372,00 (CSI, 2002, p. 2).

Para Sêmola (2003, p. 43) a Segurança da informação é uma área de conhecimento dedicada à proteção de ativos da informação contra acesso não autorizados, alterações indevidas, não-repúdio ou sua indisponibilidade.

Já a ABNT (2005, p. ix) definiu o termo Segurança da Informação (SI) como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Segundo a NBR ISO/IEC 27005/2013 a segurança da informação é consistida por

3 pilares, sendo eles confidencialidade, integridade e disponibilidade. MOREIRA (2001, p. 9), segue a mesma ideia quando diz que o objetivo da segurança da informação é a busca pela disponibilidade, confidencialidade e integridade de seus recursos e da própria informação. O risco pode ser baseado em uma equação, sendo ela:

Risco = Ativos x Ameaças x Vulnerabilidades

Para Landoll (2011), está simples equação é uma mera ilustração do princípio do cálculo do risco baseado no conhecimento do valor do ativo, estendido a ameaças e a probabilidade de tal ameaça explorar determinada vulnerabilidade existente.

Confidencialidade, integridade e disponibilidade de uma informação podem ser essenciais para a preservação da competitividade, faturamento, lucratividade, atendimentos aos requisitos legais e a imagem da organização. (NBR ISO/IEC 17799, 2001)

1.5.1 Confidencialidade

A NBR ISO/IEC 17799:2001 caracteriza a confidencialidade como “Garantia de que a informação é acessível somente por pessoas autorizadas”. Sêmola (2003, p. 44), diz que confidencialidade é a proteção da informação de acordo como grau de sigilo de seu conteúdo, de forma a restringir seu acesso somente a pessoas autorizadas.

Para Dias (2000, p. 42), o conceito de confidencialidade é associado ao conceito de privacidade onde tem a premissa de proteger as informações contra qualquer pessoa não autorizada pelo dono da informação.

1.5.2 Integridade

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 17799, 2001). Segundo Dias (2000, p. 42) a integridade está baseada em evitar que dados sejam apagados ou alterados sem permissão do seu proprietário. Beal (2005, p.1), coloca a integridade como sendo a garantia da criação legitima e da consciência da informação ao longo do seu ciclo de vida, mantendo como foco principal a prevenção contra criação, alteração e destruição indevidas dos dados.

1.5.3 Disponibilidade

Garantia de que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 17799, 2001). Wheller (2011) definiu a disponibilidade como em caso de necessidade, ela seja acessada em tempo útil, confiável por utilizadores autorizados.

Sêmola (2003, p. 44), disponibilidade é a garantia de que toda a informação gerada ou adquirida esteja disponível para as pessoas autorizadas quando forem requisitadas.

Alguns dos principais papéis e responsabilidades das organizações para o processo de gestão de risco de segurança da informação, de acordo com a ISO 27005, são:

- Desenvolvimento do processo de gestão de riscos de segurança da informação adequado à organização,
- identificação e análise das partes interessadas,
- definição dos papéis e responsabilidades de todas as partes, internas e externas à organização.

Ainda seguindo o que diz a ISO 27005, dependendo do escopo e dos objetivos da gestão de riscos, diferentes métodos podem ser aplicados. Convém que um método de gestão de riscos apropriado seja selecionado ou desenvolvido e leve em conta critérios básicos, como: avaliação de riscos, impactos e aceitação de risco.

Além disso, convém que a organização avalie se os recursos necessários estão disponíveis para então executar o processo de avaliação de riscos e estabelecer um plano de tratamento de riscos. Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados. Monitorar controles. Monitorar o processo de gestão de risco de segurança da informação.

Pode-se utilizar abordagens de segurança da informação no que se refere à implementação de controles de segurança e ameaças aos ativos de informação. A ISO/IEC 27002:2005, define uma série de controles necessários à maioria das situações que envolvem T.I. (DA VEIGA, 2010). Uma outra abordagem apresentada por Eloff e Eloff (2005) é denominada PROTECT, que é um acrônimo para Políticas, Riscos, Objetivos, Tecnologia, Execução, Conformidade e Time.

Tudor (2000), por sua vez, propõe uma abordagem abrangente e flexível de uma Arquitetura de Segurança da Informação para proteger os ativos de uma organização. Sua abordagem destaca cinco princípios fundamentais, listadas na Tabela 1, que são utilizadas para compreender o ambiente de risco em que as organizações operam, a fim de avaliar e implementar controles para mitigar tais riscos, assim como há também um foco na legislação do país para garantir que as informações confidenciais de cada organização estejam protegidas em conformidade.

Tabela 1 – Princípios da arquitetura da segurança da informação

1. **Organização de segurança e infraestrutura:** Papéis desempenhados pelas pessoas e responsabilidades são definidas e o suporte por parte da gerência executiva é estabelecido
2. **Políticas de segurança, normas e procedimentos:** Políticas, normas e procedimentos são desenvolvidos.
3. **Programa de segurança:** Um programa de segurança da informação é organizado tendo em conta a gestão de riscos.
4. **Conscientização para a segurança da cultura e da formação:** Os usuários são treinados e há reflexo da conscientização nas diversas atividades desenvolvidas. Há confiança entre os usuários, a gerência e os terceiros.
5. **Adequação:** Existe um controle interno e externo da segurança da informação.

Fonte: Tudor (2000) adaptado por Da Veiga e Eloff (2007).

Os princípios abrangem aspectos de processos e de tecnologia para direcionar necessidades de segurança das organizações. O primeiro princípio diz respeito à organização de segurança e infraestrutura com funções e responsabilidades definidas, bem como a apoio gerencial. O segundo princípio diz respeito às políticas de segurança, normas e procedimentos de gestão, destacando a importância de seu desenvolvimento e implementação.

Os requisitos de controle de segurança estabelecidos nas políticas de segurança não podem ser implantados de forma isolada, devendo considerar os riscos para a organização. Portanto, como um terceiro princípio, as avaliações de risco devem ser realizadas em todas as plataformas, bancos de dados, aplicativos e redes, assim como um processo deve ser instituído visando fornecer um orçamento adequado de recursos para enfrentar os riscos e implementar controles (SOUZA, J. *et al*, 2016).

Para que os controles atuem de forma eficaz, os usuários precisam estar cientes da sua responsabilidade e incentivados a participar de programas de treinamento. O quarto princípio visa estabelecer um ambiente de confiança entre os usuários, gestão e terceiros para permitir

transações e proteger a privacidade. O quinto e último princípio concentra-se na verificação da conformidade e auditorias por auditores internos e externos para monitorar a eficácia do programa de segurança.

1.6 IDENTIFICAÇÃO DE RISCOS

Segundo a ISO 27005, o propósito da identificação de riscos é determinar eventos que possam causar perda potencial e deixar claro como, onde e por que a perda pode acontecer.

A ISO 27005 ainda alerta para critérios referentes a aceitação de risco. Estes critérios devem ser desenvolvidos e especificados, estes critérios de aceitação do risco são relacionados frequentemente às políticas, metas e objetivos da organização, assim como dos interesses das partes interessadas.

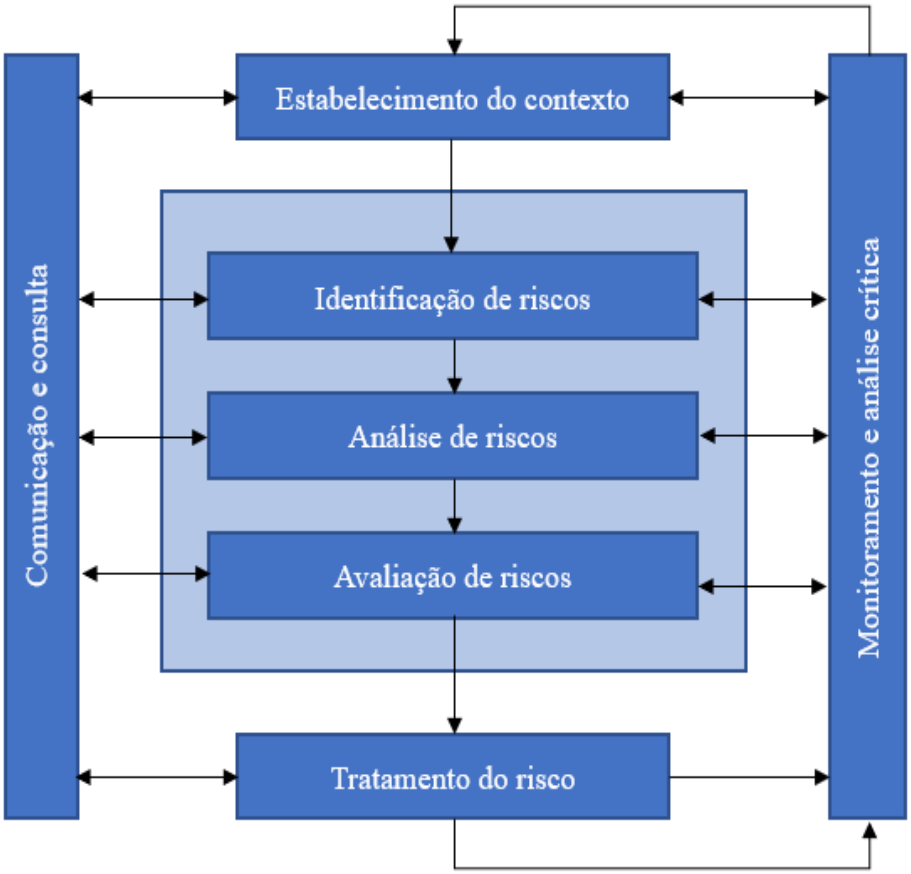
É recomendado que a organização defina sua própria escala de níveis de aceitação dos riscos. Alguns tópicos podem ser abordados, tais como:

- Critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas por gestores seniores para aceitar riscos acima deste nível;
- Critérios para a aceitação do risco podem ser expressos como a razão entre o lucro estimado (ou benefício ao negócio) e o risco estimado;
- Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, por exemplo, não conformidade de regulamentações ou leis, podem ser aceitos, enquanto riscos de alto impacto podem ser aceitos se isto for especificado como um requisito contratual;
- Critérios para aceitações do risco podem incluir requisitos para um tratamento adicional futuro, por exemplo, um risco ser aceito quando houver compromisso com ações futuras para reduzi-lo.

1.7 AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A ISO 27005 traz uma visão geral do processo de gestão de riscos de segurança da informação na Figura 1:

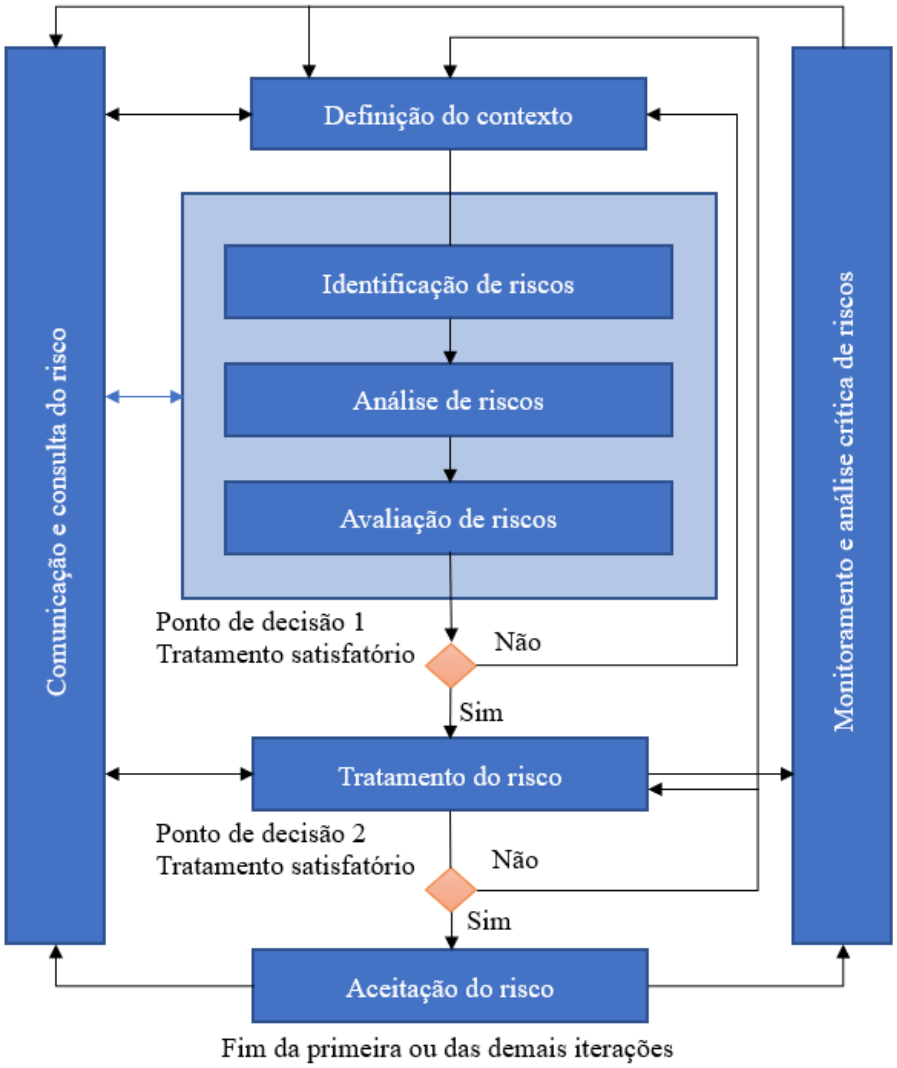
Figura 1 – O processo de gestão de riscos.



Fonte: NBR ISO/IEC 27005, 2011. p. 8

O processo de gestão de riscos de segurança da informação consiste na definição do contexto, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica dos riscos.

Figura 2 – Processo de gestão de riscos de segurança da informação.



Fonte: NBR ISO/IEC 27005, 2011. p. 9.

Na figura 2 é apresentado como esta norma se aplica ao processo de gestão de riscos. O processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento do risco.

Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. O enfoque iterativo permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidades possam ser adequadamente avaliados.

Primeiramente é estabelecido o contexto, em seguida, executa-se um processo de avaliação de riscos. Se o contexto fornecer informações suficientes para determinar de forma eficaz as ações a serem tomadas para minimizar os riscos a um nível aceitável a tarefa está completa e o processo de tratamento de riscos pode continuar. Caso contrário, se não houver

informações suficientes, é executada uma outra iteração do processo de avaliação de riscos, revisando-se o contexto, por exemplo, critérios de avaliação de riscos, de aceitação do risco ou de impacto.

Para a ISO 27005, a eficácia do tratamento do risco depende dos resultados do processo de avaliação de riscos.

Notar que o tratamento de riscos envolve um processo cíclico para:

- Avaliar um tratamento do risco;
- Decidir se os níveis de risco residual são aceitáveis;
- Gerar novo tratamento do risco se os níveis de risco não forem aceitáveis; e
- Avaliar a eficácia do tratamento.

Nem sempre o risco residual de um tratamento de risco será aceitável. Nessa situação, pode ser necessária uma nova iteração do processo de avaliação de riscos com mudanças no contexto, seguida por uma fase adicional de tratamento de risco (ver Figura 2, ponto de decisão 2).

Os riscos residuais precisam ser explicitamente aceitos pelos gestores da organização. Essa situação é especialmente importante em ambientes onde ocorre a situação em que a implementação de controles é omitida ou adiada.

A ISO 27005 ressalta que durante o processo de gestão de riscos as pessoas das áreas operacionais e os gestores sejam informados dos riscos e de como estão sendo tratados. Informações sobre os riscos identificados podem ser muito úteis para o gerenciamento de incidentes e pode ajudar a reduzir possíveis prejuízos.

A ABNT NBR ISO/IEC 27001:2006 especifica que os controles implementados no escopo, limites e contexto do SGSI devem ser baseados no risco. Este processo pode ser aplicado por vários métodos, convém que às organizações utilizem o método que se adeque melhor ao seu ambiente.

No SGSI, a definição do contexto, o processo de avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação compõe a fase de “planejar”. Na fase de “executar”, as ações e controles necessários para reduzir os riscos a um nível aceitável são implementados de acordo com o plano de tratamento de risco. Na fase “verificar”, a determinação de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas

circunstâncias são definidas pelos gestores. As ações tomadas são executadas na fase “agir”, incluem a replicação do processo de gestão de segurança da informação.

O quadro 4 exibe o alinhamento das 4 fases:

Quadro 4 – Alinhamento do processo do SGSI e do processo de SGSI

Processo do SGSI	**Processo de gestão de riscos de segurança da informação**
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Fonte: ISO/IEC 27005, 2011.

1.8 TRATAMENTO DO RISCO DE SGSI

A ISO 27005 traz as seguintes definições sobre tratamento do risco de segurança da informação.

Entrada: Uma lista de riscos priorizada, de acordo com o critério de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

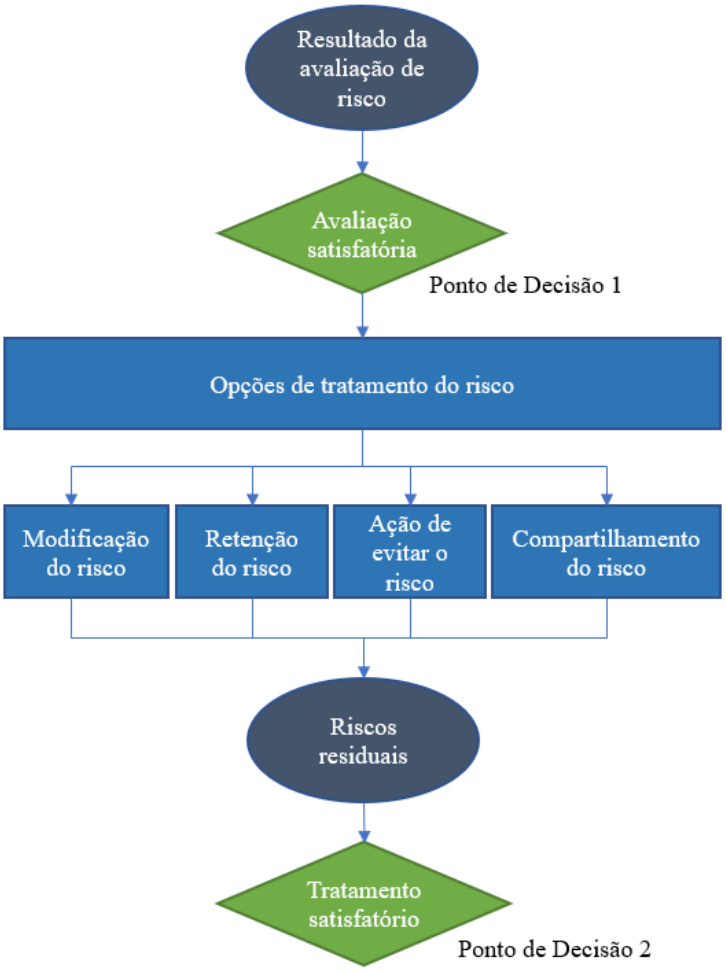
Ação: Convém que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e o plano de tratamento do risco seja definido.

Diretrizes para implementação:

Existem quatro alternativas para o tratamento de risco: modificação do risco, retenção do risco, ação de evitar o risco e compartilhamento do risco.

A Figura 3 ilustra o tratamento do risco dentro do processo de gestão de riscos de segurança da informação.

Figura 3 – A atividade de tratamento do risco.



Fonte: NBR ISO/IEC 27005, 2011. p. 26.

1.8.1 Ação de tratamento de risco

A ISO 27005 diz que o tratamento de risco deve ser baseado no resultado do processo de avaliação de riscos, levando em consideração o custo esperado, e os benefícios provenientes deste tratamento.

É levado em consideração quando se pode aplicar uma grande modificação com um custo menor e que traga benefícios para a organização, já, outras estratégias quando se tem um gasto muito elevado e um retorno não tão significativo podem ser aplicadas em outros momentos.

Independentemente de qualquer critério é essencial que seja leva em consideração que as consequências adversas do risco devem ser reduzidas ao mínimo possível, os gestores devem considerar também os riscos improváveis, porém graves. Nesta situação nem todas justificativas

são de ponto estritamente econômicas são aplicáveis, mas, podem ser necessários implementá-las.

Muitas vezes a combinação dos quatro fatores podem beneficiar a empresa, tais como, redução da probabilidade, redução das consequências e o compartilhamento ou retenção dos riscos residuais.

Se possível, é recomendado que seja definido um plano de tratamento de riscos, evidenciando de forma clara as prioridades para definir de forma específica como será implementado o tratamento de riscos. Os gestores têm a responsabilidade de avaliar e organizar os custos da implementação dos controles e o orçamento.

A ISO 27005, diz que "Convém que as opções de tratamento de risco sejam consideradas levando-se em conta:

- Como o risco é percebido pelas partes afetadas.
- As formas mais apropriadas de comunicação entre as partes

Após a identificação do tratamento de risco, os riscos residuais precisam ser determinados. Caso os riscos residuais não estejam de acordo com o esperado é pode ser necessário fazer uma nova iteração do tratamento de risco antes da aceitação.

1.8.2 Retenção do risco

Segundo a ISO 27005, as decisões sobre a retenção do risco, devem ser tomadas tendo como base avaliação de riscos. Ainda, a aceitação do risco, consciente e objetivamente, desde que claramente satisfaça as políticas da organização e os critérios para aceitação do risco.

Se o nível de risco atender aos critérios para a aceitação do risco, não há necessidade de implementar controles adicionais e pode haver retenção de risco.

1.8.3 Ação de evitar o risco

Definição de ação segundo a ISO 27005: a atividade ou condição que dá origem a um determinado risco seja evitada.

Diretrizes para implementação:

Quando os riscos são elevados e o custo de implementação de outras opções for exceder os benefícios, pode-se decidir evitar o risco completamente.

1.8.4 Aceitação do risco

O tratamento do risco e a avaliação do risco residual está sujeita à decisão dos gestores da organização como informado na ISO 27005. É indicado que a aceitação do risco seja feita de forma oficial, formalmente registrado tendo explicitamente a responsabilidade pela decisão.

Os riscos devem ser tratados observando os termos de aceitação de risco, para que eles sejam atendidos. É importante que o plano de tratamento juntamente com os riscos residuais seja registrado e aceito pelos responsáveis após uma análise crítica.

Nem sempre os riscos residuais vão estar de acordo com o esperado, isso ocorre pois os critérios aplicados não levam em conta as circunstâncias no momento. Em alguns casos os gestores podem ter que aceitar os riscos que não satisfaçam os critérios. Neste caso está ação deve ser incluída no termo de aceito para os riscos residuais.

2. METODOLOGIA

Este trabalho se iniciou com uma revisão sobre a gestão de riscos em segurança da informação. A partir desta revisão foi constituído o capítulo referencial teórico. Foi realizado uma iteração com a gestão de riscos, identificando o que são riscos, ameaças, vulnerabilidades, para posteriormente dar andamento colocando em prática os princípios da segurança da informação que foram identificados no referencial teórico.

Na elaboração do referencial teórico, foi identificado pontos que são fundamentais para uma boa gestão de segurança, e definição de conceitos para se ter como base de conhecimento. Após a revisão da literatura, as informações obtidas foram aplicadas na empresa que será trabalhada ao decorrer deste estudo.

A principal motivação para a realização deste trabalho é poder contribuir de alguma forma positiva para profissionais das mais diversas áreas, em especial a área de segurança da informação aos riscos que correm no mundo atual, analisar estabelecendo um contexto, identificar os riscos, analisá-los, fazer uma avaliação em cima de cada risco encontrado, e por fim tratá-lo. Está metodologia é baseada nas normas ISO 27001, ISO 27002 e ISO 27005 conforme figura 1.

Antes de iniciar este trabalho foi realizada uma reunião com os responsáveis pela empresa a ser analisada, e ficou definido que não seria divulgado nome da empresa nem dos responsáveis, juntamente com os dados sensíveis para a empresa nas figuras apresentadas.

Previamente essas informações foram relatadas aos gerentes e pessoas chaves do negócio, como programadores e suporte técnico, informando possíveis problemas que poderiam vir a acontecer caso algum item crítico fosse encontrado e corrigido, isso poderia de alguma forma afetar outras pessoas, inicialmente foi buscado a realização de tarefas onde o impacto ao usuário final fosse nula ou praticamente imperceptível, com o andamento do projeto, se foi encontrado algumas barreiras onde precisou ser colocado algum ajusta em *standby* e em outro momento dado continuidade.

Antes da realização de qualquer mudança significativa era realizada um teste, onde se verificava se ocorria tudo de acordo com o esperado e posteriormente colocado em ambiente de produção. Ao decorrer destas correções vários ajustes precisaram ser realizados.

3. ANÁLISE DE INFRAESTRUTURA DA EMPRESA

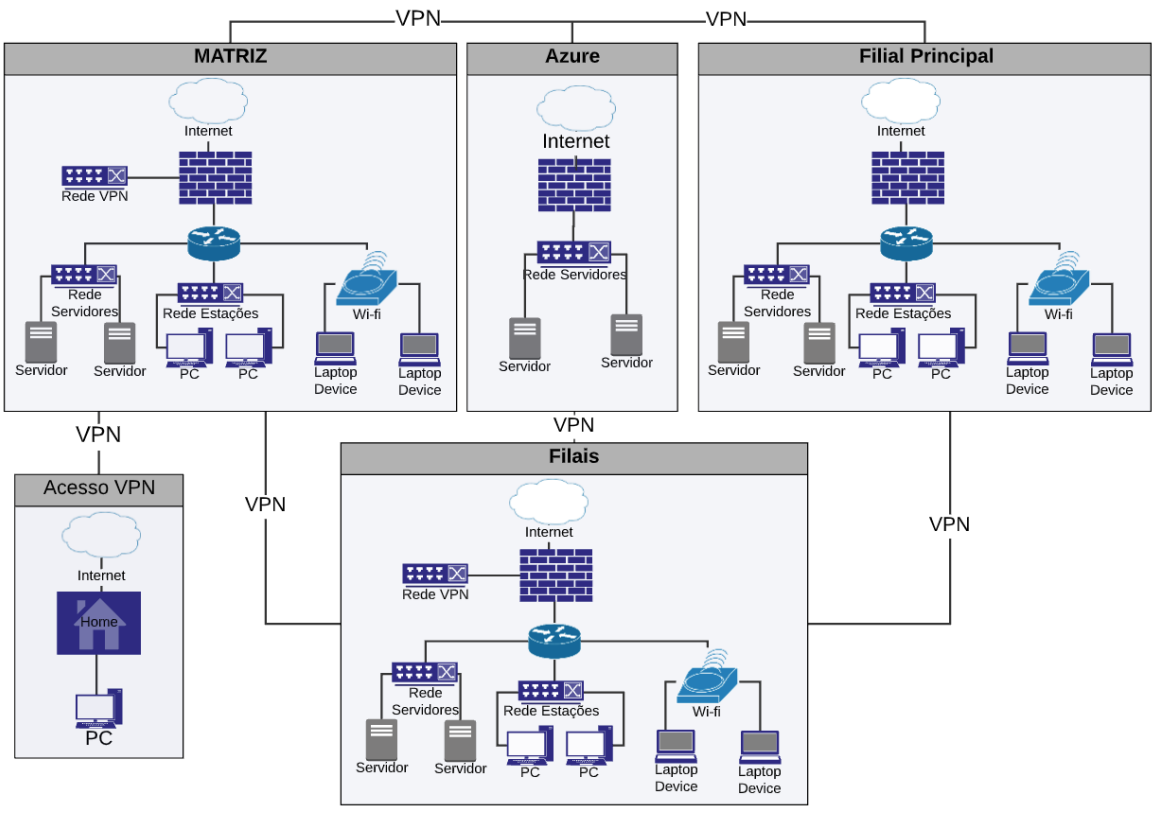
Inicialmente foi realizada uma análise na topologia da empresa buscando pontos onde poderiam serem aplicadas as devidas correções, sempre buscando o menor impacto para os funcionários e melhorando a segurança da organização, não apenas relacionado há segurança de vírus, ataques, mas também melhorando a infraestrutura como um todo, permissões de acessos, disponibilidade de serviços, sistemas e orientando funcionários a terem boas práticas.

É de suma importância salientar que nem todos os itens encontrados como vulnerabilidades puderam ser corrigidos, fatores como tempo, disponibilidade e impacto foram determinantes para a não correção.

Além das correções aplicadas será elaborado um projeto para implementação das demais correções e a criação de um novo mapa de risco demonstrando como seria o ideal para a empresa, e como ela se encontra durante este momento de evolução estrutural.

Cada item que foi identificado fora de conformidade na estrutura atual foi definido com um nível de criticidade, e foi buscado tratá-los de acordo com os mais críticos e que não tivessem tanto impacto nos funcionários e na empresa em geral.

Figura 4 – Topologia inicial da empresa.



Fonte: Elaborado pelo autor (2021).

4. VULNERABILIDADES DA TOPOLOGIA ATUAL

4.1 SEGREGAÇÃO DA REDE INTERNA

Segregação de rede se baseia no ato de dividir uma rede em partes menores, assim sendo chamadas de segmento de rede, desta forma as redes ficam separadas umas das outras e assim evitam que uma passa acessar a outra sem ter o devido acesso liberado.

A estratégia de restringir o acesso a rede pode ser feito em conjunto com a configuração de outros dispositivos de rede como roteadores, switches etc. e deve ser feita de acordo com o planejamento da segmentação da rede, potencializando a segurança da rede (KLOSTERBOER, 2008).

Conforme levantamento de estrutura da empresa, as redes corporativas possuem algumas restrições, a matriz é controlada por ACLs no *switchcore* e nas filiais por regras de firewall, entre as redes das filiais e a matriz não há bloqueios.

Desta forma caso alguma das redes de alguma filial seja comprometida facilmente poderá afetar até a matriz e assim chegar até as demais filiais, podendo levar a vazamentos de suas informações ou de seus clientes. Além de poder causar muitos outros transtornos internos e externos.

Nível de risco: Crítico

4.2 REDE PARA GERÊNCIA DE EQUIPAMENTOS

A empresa possui uma rede de gerência, porém não está em uso.

Com a falta deste controle usuários comuns tem acesso aos ativos da rede e servidores através das suas portas de gerenciamento remoto permitindo que um atacante efetue ataques de força bruta e obtendo acesso aos servidores e recursos de redes críticos.

Nível de risco: Alto

4.3 PUBLICAÇÃO NA REDE INTERNA

Durante o levantamento foi identificado que existem servidores de publicações no mesmo segmento dos outros servidores. Não possuem DMZ, mas fazem o controle de acesso as publicações pelo proxy-reverso e *features* de WAF e IPS no *firewall*.

O acesso, a partir da internet, a servidores instalados no segmento interno da rede representa grande risco para toda a rede, pois caso algum destes servidores venha a ser comprometido, através da exploração de alguma vulnerabilidade (vírus, *worms*, *trojans*, *ransomware*) ou qualquer que seja a forma da ameaça, toda a rede interna poderá ser prejudicada.

Isso é possível, pois após o comprometimento de um servidor qualquer instalado na rede interna, não haverá barreiras que impeçam que este equipamento seja utilizado como ponte para proliferação de ataques pelos demais dispositivos e estações, ou que seja, ele poderá ser usado para coleta de informações sigilosas através de ataques passivos, ou até mesmo ataques de destruição de informações.

Este tipo de acesso é normalmente caracterizado pela existência de um NAT estático, ou seja, tradução de endereço público para endereço da rede privada.

Em alguns casos o acesso não é possível apenas pela inexistência de uma regra que permita o tráfego, embora a tradução de endereços exista. Mesmo assim, é aconselhável a remoção da tradução de endereços, pois existindo o "caminho", alguma regra mal construída pode acidentalmente permitir que o acesso ocorra e acabe afetando a empresa.

O ambiente deve ser segmentado em várias faixas entre elas uma especificamente para servidores publicados para a internet (DMZ), desta forma caso um servidor seja atacado com êxito os demais não poderão ser atingidos, pois um servidor não consegue ter acesso a rede de outro servidor.

Nível de risco: Crítico

4.4 ACESSO LIVRE A INTERNET

O risco aponta para a liberdade de comunicação com à internet com pouca filtragem que controle o tráfego e os proteja de qualquer ação maliciosa. Nem todas as filiais possuem o mesmo controle sobre os acessos para a internet.

A empresa informou que todos os servidores têm acesso à internet, mas que possuem *features* de controle habilitados nas regras de *firewall*, tais como *webfilter*, *appcontrol*, IPS, IDS, antivírus.

Quando se trata de acesso à internet se deve adotar uma série de artifícios para ajudar na proteção do ambiente, servidores, estações de trabalho e outros equipamentos conectados à

internet, estão propícios a diversos riscos que vão desde contaminação por pragas, vírus, *worms* até mesmo à ataques e vazamento de informações sigilosas.

Vários servidores possuem acesso irrestrito para a internet, é de extrema recomendação que esses acessos não existam, caso seja necessário, devem ser liberados os acessos aos destinos específicos onde o servidor e seus serviços necessitem de conexão.

Utilizando controles de acessos a internet pode-se tratar o índice de controle de acessos conforme descrito na ISO 27001 (2006), proteger e controlar os acessos à informações e sistemas definindo acessos, competências e responsabilidades.

Nível de risco: Crítico

4.5 BLINDAGEM DE CREDENCIAIS ADMINISTRATIVAS

É recomendado que os acessos remotos aos servidores não sejam realizados diretamente das máquinas da equipe de TI, uma vez que, as senhas de *domain admin* ficam armazenadas no cache (memória) da máquina local apresentando o risco de serem capturadas por um atacante.

4.6 SEGMENTAÇÃO DA REDE DE BANCO DE DADOS

Existem servidores de banco de dados situados no mesmo segmento de rede que os demais servidores de aplicação e de serviços de rede. Este cenário permite que os servidores sejam facilmente mapeados e posteriormente sofram algum ataque por um usuário malicioso que já tenha acesso a algum outro servidor, pois as bases de dados não possuem um segmento de rede próprio.

Para amenizar qualquer risco de isso ocorrer é indicado a separação da rede de bancos de dados das demais redes, *workstations*, aplicativos, gerencia.

Nível de risco: Crítico

4.7 CENTRALIZADOR DE LOG REMOTO (*SYSLOG*)

Seguindo a ISO 27005 a inexistência de *logs* é uma vulnerabilidade e a ameaça pode ser caracterizada como abuso de direito. Em reunião com a empresa foi identificado que não possuem um servidor específico para armazenamento de logs, mas possuem o *Fortianalyzer* para os *firewalls* e dispositivos de rede.

Deixando os logs apenas localmente em seus equipamentos corre-se o risco de serem apagados por um atacante ou perdidos por falta de espaço no *buffer* conforme o tempo de utilização ou até mesmo causar transtornos por lotação de disco. Este cenário também pode dificultar o trabalho de identificação e compreensão dos eventos dos ativos de redes em casos de alterações indevidas no ambiente ou algum ataque à segurança.

Nível de risco: Baixo

4.8 IMPLEMENTAÇÃO DE IDS/IPS

Atualmente a *feature* de IPS/IDS está ativo em alguns hosts e em algumas regras de *firewall*. É recomendado que seja aplicado em todos os segmentos críticos ao negócio.

No cenário atual a equipe de infraestrutura pode ter dificuldades em identificar incidentes de rede ao ponto de tomar alguma ação e minimizar seus prejuízos.

Sistemas de prevenção de intrusão (IPS) tem como função principal parar os ataques detectados, tem função ativa na proteção contra tentativas de ataques, ele analisa a rede e se detectar algum movimento suspeito ele bloqueia a atividade.

Já o IDS tem como função principal identificar e alertar fornecendo dados sobre as atividades geralmente não toma nenhuma ação para parar o ataque, ele pode emitir alertas para o administrador, disponibilizar estatísticas e monitorar o tráfego.

Nível de risco: Crítico

4.9 SISTEMAS OPERACIONAIS OBSOLETOS

Foi realizado um levantamento com a ferramenta *lansweeper* e identificado que a empresa possui servidores *EOL* no ambiente, no mesmo segmento dos outros servidores. O risco aponta para existência de sistemas operacionais e ISOs descontinuados pelos fabricantes, não possuindo mais atualizações, suporte e consequentemente suscetível a falhas que não podem ser corrigidas.

Desse modo, tornando o ambiente vulnerável à ataques, potencializando ainda mais o risco caso existam servidores, dispositivos ou equipamentos com essas características expostas para internet.

Nível de risco: Alto

4.10 CONTROLE SOBRE VAZAMENTO DE INFORMAÇÕES - DLP

Data Loss Prevention (DLP), refere-se a sistemas que identificam, monitoram e protegem dados em uso, em movimento e em repouso, tem como objetivo detectar e prevenir o uso e a sua transmissão não autorizada de dados confidenciais (ROEBUCK, 2001).

Sistemas de prevenção de dados são sistemas centralizadores de gerenciamento de dados que monitoram e protegem as informações críticas relacionadas a empresa. Seu foco é baseado em dados confidenciais evitando violação dedados.

A empresa possui a *feature* de DLP somente nos hosts com antivírus e em algumas regras de *firewall*. O risco aponta para a falta de controle sobre vazamento de informações sensíveis da empresa, onde possa comprometer tanto no âmbito de informações e projetos intelectuais, quanto questões de valores e demais informações importantes para o negócio da empresa.

As ameaças de vazamento de dados, roubos, negligencias se dão por muitas vezes por não seguimento das normas e políticas de conformidades, para ajudar nesta situação é que a DLP uma solução contra vazamento de dados atua. DLP é um conjunto de soluções com foco na perda de dados, principalmente por fontes internas, através de definições de políticas dentro do sistema com o intuito de prevenir, detecta e barrar a evasão de dados importantes (ISACA, 2010).

Nível de risco: Crítico

4.11 VPN SEM DUPLO FATOR DE AUTENTICAÇÃO

A organização possui algumas VPNs *client-to-site*, para uso dos funcionários que tenham necessidade de acesso externo aos serviços e para fornecedores de serviços, ambos são autenticados no AD mas sem um segundo fator de autenticação (2 FA).

Recomenda-se a utilização de um duplo fator de autenticação para todos os usuários. A autenticação forte ou de múltiplos fatores é definida com a utilização de duas ou mais formas de diferentes de verificação de identidade, permitindo assim minimizar o risco associado ao roubo de identidades ou o uso indevido de credenciais por pessoas não autorizadas, aumentando o nível de segurança no ambiente.

Para Tanenbaum (2001), as ameaças à privacidade estão em constante crescimento, neste contexto, a autenticação convencional é considerada defasada para muitas aplicações

críticas, tais como, bancos online e sistemas online. A autenticação em dois fatores, eleva o nível de proteção ao exigir dois meios de autenticação, podendo ser por token, *hardware* ou em um *smartphone*.

Nível de risco: Médio

4.12 CONTROLE DE CAMADA DE ACESSO (REDE CABEADA)

A empresa informou que não existe controle de acesso na rede corporativa na camada de acesso (cabeada). Possibilitando acesso à rede interna onde estão conectados dispositivos de uso corporativo pelos funcionários, servidores e outros dispositivos de rede possibilitando ações maliciosas como mapeamento e escaneamento da rede ou tentativas de acesso a recursos de rede restritos que, caso sejam acessados, podem fornecer dados sensíveis a pessoas não autorizadas.

Possibilita também que os próprios colaboradores utilizem dispositivos pessoais na rede, podendo conter algum tipo de vírus e disseminando-os para a rede interna, comprometendo a segurança como um todo.

A ISO, menciona o controle de acesso somente a pessoas autorizadas

Nível de risco: Médio

4.13 AUTENTICAÇÃO DE DISPOSITIVOS DE REDE DESCENTRALIZADA

Atualmente alguns dispositivos se integram com o *active directory*, nos outros os usuários são criados localmente, dificultando o gerenciamento dos usuários que utilizam os equipamentos e seu processo de autorização dos recursos de rede que podem ser acessados, e principalmente um problema na identificação do administrador de rede que realizou alguma mudança no ambiente, uma vez que, todos acessam o equipamento com o mesmo usuário.

É indicado que sempre seja criado um usuário por funcionário que utilizará a máquina, desta forma se mantem uma gestão centralizada e de fácil controle, juntamente com melhorias para auditorias de usuários.

Nível de risco: Médio

4.14 REDUNDANCIA E ALTA DISPONIBILIDADE (HA)

A empresa possui redundância somente na matriz, nos outros ambientes não. Caso algum dos equipamentos das filiais desliguem indevidamente ou ficarem indisponíveis por falha interna ou um ataque proposital, toda a rede local ficará indisponível até que seja trocado o equipamento impactando no acesso aos serviços externos e internos e consequentemente no acesso dos usuários.

Aconselha-se que se tenha em pontos chaves estrutura para alta disponibilidade (HA). Esta forma o ambiente não ficará totalmente improdutivo.

Sêmola (2003), diz que toda informação é influenciada por três propriedades principais confidencialidade, integridade e disponibilidade. Este sentido a disponibilidade é um pilar chave na segurança da informação, fazendo uso de alta disponibilidade este princípio é tratado para não haver falta de disponibilidade.

Nível de risco: Médio

5. SOLUÇÕES TOPOLÓGICAS PROPOSTAS

Recomendações gerais propostas para mitigar vulnerabilidades no ambiente atual e soluções a serem expandidas ou implementadas no ambiente, a curto, médio e longo prazo. Sempre salientando que segurança da informação é algo que não pode parar, sempre é necessário estar em busca de novas soluções e melhorias nos ambientes.

5.1 ATUAÇÕES A CURTO PRAZO

5.1.1 Controle de acesso à internet

O simples fato de falarmos de acesso à internet já requer uma série de técnicas e artifícios que ajudaram a proteger a infraestrutura de rede bem como computadores antes mesmo de ter o acesso à internet. Das técnicas que precisam ser adotas para ajudar a mitigar os riscos suscetíveis no acesso à internet, vão desde a instalação de antivírus, proteção por *firewall*, *proxy* para controle da navegação, *webfilter*, IPS para controle de invasão.

Recomenda-se que seja implementado um controle mais restritivo de acesso à internet, de modo que, para os que realmente precisam ter conexão com a internet, esta deverá ser feita através de um filtro de conteúdo e regras de firewall que bloqueiem sites não permitidos pelas políticas de acesso interno e restringindo a navegação para destinos e/ou portas de serviços específicos, evitando a navegação livre e que possa permitir vazamento de informações sensíveis para a companhia.

A ISO/IEC 17799, define o controle de acessos como objetivo de controlar acessos a informações, os acessos devem ser controlados de acordo com os requisitos de segurança do negócio.

5.1.2 Blindagem de credenciais administrativas – *Jump Server*/TS blindado

Jump Server, com tradução livre pular servidor, ou seja, servidor de pular, serve como meio entre a rede normal e a rede de servidores, garantindo assim mais uma barreira para possíveis invasões no ambiente.

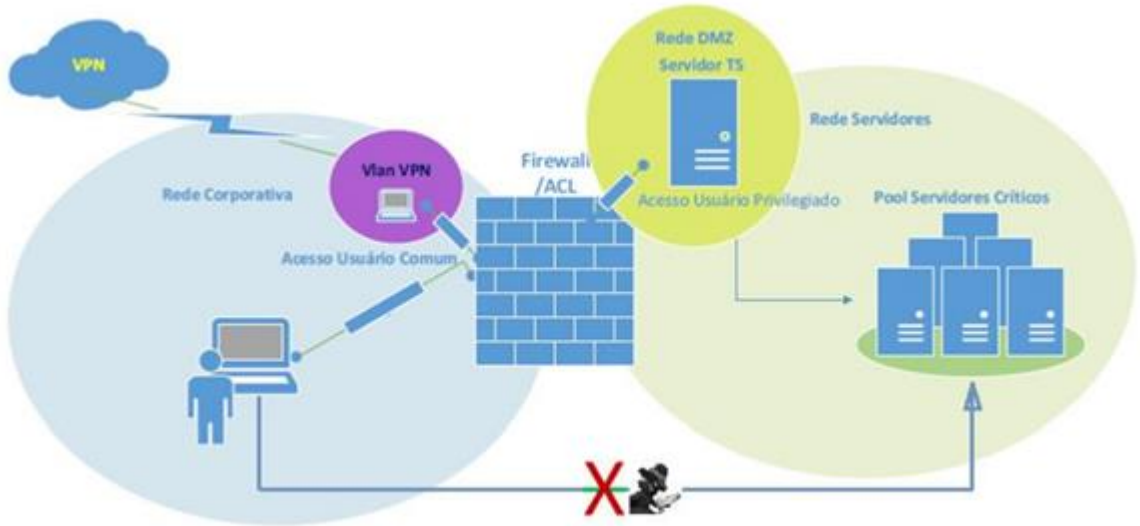
Este item pode gerar um grande conflito pois cria mais um processo para os responsáveis por administrar o ambiente, ou seja, fatores como dupla autenticação ou até

mesmo a mudança dos acessos, ferramentas e hábitos do dia a dia se tornam obstáculos para que esta mudança de mentalidade aconteça.

Para melhoria na segurança do ambiente recomenda-se como forma de proteção á credenciais administrativas a implementação de um servidor de acesso remoto (TS Seguro) para centralizar todo e qualquer acesso remoto aos ativos de rede ou servidor evitando que estas credenciais fiquem espalhadas pelos outros ambientes e centralizando em um ambiente seguro, controlado e monitorado pela equipe de TI da empresa.

Na figura 5 se tem o exemplo de como pode ser estruturado o posicionamento do *Jump Server* na rede.

Figura 5 – Exemplo de posicionamento de um *Jump Server* na rede.



Fonte: Elaborado pelo autor (2021).

Alcançar um nível de 100% de segurança é praticamente impossível, entretanto estas melhorias são fundamentais para evitar um *bypass* do conceito de TS Seguro. Então, para evitar que os usuários com credenciais administrativas administrem o ambiente de servidores críticos fora do conceito de TS Seguro.

Mesmo utilizando o conceito de *Jump Server*, é importante que tenha uma atenção especial para também manter o ambiente de *Jump Serve* seguro, adotando alguns critérios como:

- Manter o sistema operacional do *Jump Server* atualizado;
- Utilização de duplo fator de autenticação;
- Adotar uma política de acesso ao *Jump Server*;

- Restringir o acesso à internet através do *Jump Server*;
- Alta disponibilidade do servidor *Jump Server*;

5.1.3 Controle sobre Vazamento de Informações – DLP

A utilização de DLP (*Data Loss Prevention*), são ferramentas que atuam na camada de rede, o ideal é que essa solução seja aplicada para todo ambiente de acordo com sua necessidade. O DLP auxilia na descoberta, monitoração e no gerenciamento de dados confidenciais independentemente da localização e da utilização através de redes, dispositivos móveis ou *endpoints*. Os sistemas DLPs podem identificar a perda de dados através da identificação do conteúdo, monitoramento e bloqueio de dados sensíveis, ou seja, identificar, monitorar e proteger as informações confidenciais que podem estar em uso (máquinas dos usuários), em movimento (na rede corporativa) ou armazenadas (banco de dados, servidores).

- *Endpoint* DLP

É uma solução baseada em um agente que fica instalado nas estações de trabalho e laptops e permite o monitoramento e bloqueio para todos os dados sensíveis que saem através de dispositivos removíveis, como CDs e USBs. Este tipo de DLP também fornece a auditoria e proteção dos dados segundo as políticas de segurança da empresa.

- *Network* DLP

Pode ser uma solução em hardware ou software, sendo instalado em todos os pontos de saída dos dados da rede corporativa para Internet. Os dados serão analisados para identificar informações confidenciais que estão violando as políticas de segurança imposta pela empresa. As soluções de DLP analisam o tráfego de rede para detectar se dados sensíveis estão sendo enviados contrariamente às políticas de segurança da informação. Com base no conjunto de regras, a solução também pode colocar em quarentena ou criptografar os dados em questão.

Quando transmitidos pela rede, os arquivos normalmente são divididos em pacotes, para inspecionar as informações que estão sendo enviadas pela rede, a solução DLP precisa ser capaz de: monitorar passivamente o tráfego de rede, reconhecer os fluxos de dados corretos a capturar, montar os pacotes coletados e reconstruir os arquivos transportados no fluxo de dados, que devem ser descriptografados antes da inspeção realizada pela solução de DLP que após a inspeção dos dados deve criptografar novamente os dados. A solução DLP deve ter a capacidade de fazer isso por si só (tendo esse recurso e as chaves de criptografia necessárias)

ou deve haver um dispositivo na rede que descriptografe o tráfego antes da inspeção da solução de DLP e, então, criptografe-o novamente depois que os dados forem inspecionados e tenham a permissão para passar.

5.1.4 Implementação de IPS e IDS

É importante que a função de IDS/IPS ou também conhecido como Sistemas de Detecção/Prevenção de Intrusos, sejam habilitados em todos os pontos críticos do ambiente, pois são recursos de segurança de redes com a função de monitorar as atividades de redes e/ou sistemas procurando por atividades maliciosas.

As principais funções de IPS são:

- Identificar atividades maliciosas,
- Arquivar informações sobre estas atividades,
- Tentar bloquear/parar a atividade maliciosa,
- Reportar a atividade maliciosa.

Sistemas de Prevenção de Intrusos são considerados extensões dos Sistemas de Detecção de Intrusos, porque são colocados em linha, monitorando o tráfego de rede procurando atividades maliciosas, sendo capazes de trabalhar ativamente para prevenir/bloquear intrusões que são detectadas. Algumas soluções de IPS podem tomar medidas como o envio de um alarme, ignorar o pacote malicioso, reiniciando a conexão e/ou bloqueando o tráfego originário de um determinado endereço IP agressor. Um IPS também pode corrigir erros de *Cyclic Redundancy Check* (CRC), desfragmentação de pacotes *streams*, evitar problemas com a sequência dos pacotes TCP, e limpar opções indesejáveis nas camadas de transporte e rede.

Os Sistemas de Prevenção de Intrusos podem ser classificados em quatro tipos:

- Sistemas de Prevenção de Intrusos via Rede de Dados (NIPS): monitora toda a rede procurando tráfego suspeito, analisando as atividades dos protocolos.
- Sistemas de Prevenção de Intrusos via Rede Wireless (WIPS): monitora uma rede wireless procurando tráfego suspeito, analisando as atividades dos protocolos de rede wireless.

- Análise do Comportamento de Rede (NBA): analisa o tráfego de rede para identificar ameaças que geram fluxos de tráfego incomuns, tais como negação de serviço distribuída (DDoS), certas formas de *malware*, e violações de políticas.
- Sistemas de Prevenção em Host (HIPS): um pacote de *software* é instalado em um único host, procurando por atividades suspeitas, pela análise dos eventos que ocorrem neste host.

A rede de gerência do IPS deve ficar separada dos demais segmentos de rede da localidade onde serão implantados. Nesta rede de gerência deverá estar também o gerenciador dos equipamentos, e se necessário o servidor de *syslog* dedicado. O acesso a está rede deverá ser restrito as pessoas que farão a administração deste recurso.

5.1.5 Publicações na rede interna

Para os servidores nos quais estão instalados serviços que realmente necessitam ser publicados para a Internet, é recomendado a migração de seus serviços, ou de todo o servidor, para o segmento DMZ (Zona Desmilitarizada).

A não aplicação de uma rede segregada em VLAN´s pode ocasionar uma implementação da segurança geral menos imune às atividades maliciosas. As zonas desmilitarizadas (DMZs) são comumente implementadas sem a imposição das políticas apropriadas, o que facilita a atividade de um possível atacante.

Os servidores localizados na DMZ só devem processar solicitações de entrada da internet e, consequentemente, iniciar conexões com alguns servidores de *back-end*. Os servidores da DMZ não devem conversar entre si, e nem iniciar conexões com o ambiente externo. Isso define claramente os fluxos de tráfego necessários em um modelo de confiança simples. No entanto, muitas vezes esse tipo do modelo não é ser imposto adequadamente.

Usualmente se implementam DMZs usando um segmento comum de redes para todos os servidores sem qualquer controle sobre o tráfego entre eles. Por exemplo, todos os servidores são colocados em uma VLAN comum. Como nada está controlando o tráfego na mesma VLAN, se um dos servidores for comprometido, então o mesmo servidor poderá ser explorado para lançar um ataque a qualquer um dos servidores e hosts no mesmo segmento. Isto facilita claramente a atividade de um invasor potencial responsável por um redirecionamento de porta ou um ataque de camada de aplicativo.

Os *firewalls* e os filtros de pacote são usados para controlar as conexões recebidas, mas geralmente nada é feito para restringir as conexões provenientes da DMZ. A publicação de serviços via web tem como premissa a não exposição direta dos servidores envolvidos. Para isso, é utilizado o mecanismo de *Proxy* Reverso ou WAF, que impossibilita a exploração de possíveis falhas por parte de um usuário externo.

Abaixo seguem alguns riscos da publicação direta de servidores web:

- Na publicação direta do servidor web o usuário externo poderá explorar falhas neste servidor, nas bibliotecas ou no sistema operacional, pois estará diretamente conectado a esse servidor;
- Um simples *firewall*, trabalhando com filtro de pacotes, não será o suficiente para bloquear ataques mais elaborados, como requisições fora de padrão para explorar buffer overflow, uma vez que o protocolo precisa ser liberado para a Internet.

A função do *Proxy* Reverso/WAF é filtrar as requisições vindas da Internet e depois de realizar as requisições junto ao servidor web localizado na rede interna. Com isso, impede-se que o usuário externo tenha contato direto com o servidor web. Oferecem uma camada altamente escalável de proteção contra-ataques às aplicações web, estas aplicações visam emitir alertas e bloquear ataques antes de chegarem aos servidores nas camadas de rede e aplicação através de filtros do tráfego HTTP e HTTPS, ou seja, tem como principal objetivo verificar *strings* e assinaturas pré-definidas em sua base, a partir desta obter uma atitude, seja ela bloquear a ação ou emitir um alerta para o administrador para uma análise ou ação posterior.

Há um conjunto de diversas regras que detectam e previnem técnicas de exploração de vulnerabilidades como técnicas de *SQL Injection* e *Cross Site Scripting* – XSS.

As ferramentas permitem que o administrador possa definir todas as regras, alertas e ações a serem tomadas, dentre estas, é possível se configurar listas de endereços IPs que podem ou não acessar as suas aplicações web.

Principais Vantagens:

- Aumenta a confiabilidade, integridade e disponibilidade das aplicações web;
- Aumento da segurança nas aplicações web;
- Reduz tráfego de ataques;
- Reduz custos relacionados, como banda, infraestrutura e recursos operacionais;

- Mitiga os riscos de subdimensionamento de *firewalls* de aplicação web;
- Absorção de ataques DDoS através de escalonamento automático sob demanda;
- Reduz ataques à infraestrutura de origem aliviando a carga da arquitetura de segurança já existente;
- Fornece relatórios com a visualização das ocorrências de ataques e alarmes;
- Permite a criação de regras para bloqueio de acesso em função do volume de requisições vindas de um único endereço IP em um período predefinido;
- Inclui padrões já estabelecidos e aceita a criação de outras regras para controle do cliente;

5.2 ESTRATÉGIAS DE PRIORIZAÇÃO DE MÉDIO PRAZO

5.2.1 Segregação de Rede através de *firewall*

É recomendado que as segmentações lógicas presentes no ambiente sejam separadas entre si, principalmente em relação aos segmentos críticos para o negócio seja realizado em um firewall específico para a rede interna pois este possui *features* voltadas para o controle de acesso do tráfego entre as vlans e demais *features* de segurança necessárias para este tipo de controle.

Deve ser realizada uma análise criteriosa das necessidades das comunicações entre as VLANs verificando quais são as origens e destinos, em seguida verificar as restrições dos serviços que serão liberados. É importante levar em conta o conceito de privilégios mínimos (*Least privilegies*), e restringir ao máximo cada acesso que for disponibilizado.

A segregação de redes, contribui na prevenção de acessos não autorizados a um serviço de rede e melhora a monitoração de grupos de usuários e sistemas de informação. (NBR ISO/IEC 27001:2006).

5.2.2 Papel de VPN na segregação

Outra segregação recomendada é definir claramente quem é e quais são as origens esperadas para trafegarem em tuneis VPN a realizar ações administrativas. Como administradores usam conexões remotas para prestar suporte ao ambiente, deve ser implementada uma forma de segregá-los dos usuários comuns, permitindo que a autorização

para acesso a serviços de gestão de ativos críticos da empresa seja feita apenas para o grupo correto de usuários que necessitam do acesso.

5.2.3 Segmentação de rede por Ambientes:

A criação da segmentação de rede por ambientes tem como principalmente objetivo blindar o Ambiente de Produção (negócio do cliente). De modo que o acesso ao ambiente seja cada vez mais restritivo, diminuindo consideravelmente os incidentes e acessos não permitidos.

Alguns exemplos de melhorias para segmentação do ambiente:

5.2.4 Segmento de rede para usuários:

Criação de rede específica para hospedar os usuários. Exemplo: Usuário do departamento de RH, Usuário do departamento Financeiro, Usuários do departamento de diretoria etc.

5.2.5 Segmento de Gerência:

Criação da rede específica para administração de equipamentos de rede, servidores, *jump servers*, dispositivos, *firewalls* etc.

O ideal é que somente essa rede tenha acesso as interfaces de gerenciamento desses equipamentos. Incluir nessa rede somente os funcionários que irão prestar o suporte e gerenciamento.

5.2.6 Segmentos de rede para Servidores Administrativos:

Criação de rede exclusiva para hospedar os Servidores denominados de Administração.

Exemplo: DHCP, *Syslog*, Monitoramento, DNS, Servidor de arquivos etc.

5.2.7 Segmento de rede para Servidores de Aplicação:

Criação de rede exclusiva para hospedar todos os servidores de Aplicações do Negócio da Empresa.

Exemplo:

Sistema de Folha de pagamento, SAP, Sistema Jurídico etc.

5.2.8 Segmento DMZ:

Criação de rede para hospedar os servidores que possuem aplicações e/ou sites com acesso externo. Esses servidores são os mais vulneráveis a ataques e por isso é importante que sejam isolados dos outros.

5.2.9 Segmento DMZ EoL:

Criação de rede para hospedar os servidores EoL e Legado que não possuem mais atualizações de segurança do fabricante.

5.2.10 Segmento Jump Server:

Criação de uma rede específica para agregar os servidores de *Jump server*, com essa rede fica mais fácil e segura a administração e controle dos acessos aos outros servidores.

5.2.11 Segmento de rede para Servidores de Banco de Dados:

Criação de rede exclusiva para hospedar todos os Servidores de Banco de Dados. De forma a restringir e proteger melhor o acesso a eles.

5.2.12 Segmento de rede para backup:

Criação de rede exclusiva para hospedar os Servidores denominados responsáveis por efetuar o backup dos Ambientes.

Exemplo: Backup do Servidor de Banco de Dados, Backup do Servidor de Aplicação, Backup de servidores Administrativos etc.

5.2.13 Ambiente de Homologação:

Consiste no ambiente criado para efetuar todos os testes, validações, atualizações etc. para certificar que entrem no ambiente de Produção corretamente e sem impacto.

5.2.14 Segregação e controle de comunicação entre as redes:

Após a segmentação das redes, é imprescindível que aplique controles e restrições de acessos entre elas. Sendo assim, é recomendado a implementação de *firewall* interno para efetuar precisamente o controle entre as redes.

5.2.15 Ambiente de banco de dados – Arquitetura de rede

É recomendado que seja realizado um trabalho de mapeamento e segregação dos ambientes de banco de dados a nível de arquitetura de rede, levando em consideração as necessidades atuais e tentando provisionar crescimentos futuros.

Os servidores de banco de dados devem estar alocados em segmentos de redes apartados dos demais servidores e seu acesso tanto para gerência quanto para utilização de seus serviços sejam feitos através de liberação de regras de *firewall* restringindo o acesso a estes servidores críticos ao máximo dificultando a ação de invasão, forçando o invasor a passar novamente pelo firewall antes de tentar acesso ao banco de dados das aplicações.

Outro fator importante é que estes servidores sejam segmentados por ambientes:

5.2.16 Ambiente de produção

O ambiente de produção é onde deverá ser alocado o servidor de banco de dados da produção, onde o seu acesso e o *input* de informações deveram ser controlados, a fim de que, nenhuma informação sensível seja perdida ou alterada sem um critério definido.

O acesso a este servidor deverá ser feito somente pela equipe autorizada via TS seguro.

5.2.17 Ambiente de homologação

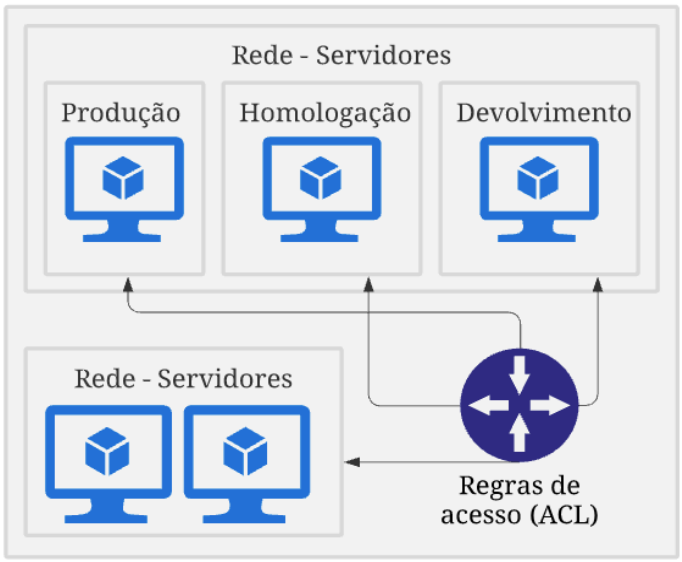
O ambiente de homologação é onde deverá ser alocado os servidores de homologação. Aqui serão testados os sistemas, tabelas e quaisquer aplicações que entrarão em produção no ambiente.

A perda de dados nesse nível do sistema como um todo não gera grandes prejuízos a corporação, porém é necessário que este ambiente esteja segregado logicamente no ambiente de produção.

5.2.18 Ambiente de desenvolvimento

O ambiente de desenvolvimento é onde deverá ser alocado os servidores de desenvolvimento. Este servidor é submetido a várias alterações até que a aplicação e sistema seja considerado em fase de testes, a perda de dados nesse nível do sistema como um todo não gera grandes prejuízos a corporação, porém é necessário que este ambiente esteja segregado logicamente no ambiente de produção.

Figura 6 - Segmentação lógica da rede de banco de dados.



Fonte: Elaborado pelo autor (2021).

A recomendação é migrar esse modelo de acesso do usuário diretamente ao banco (*client-server*) para o modelo de três camadas de aplicação (*client-aplication-server*), onde a aplicação do usuário final não precisará comunicar diretamente com o Banco de Dados. Dessa maneira, assim como mencionado no item anterior, restringindo o acesso através de *firewall* interno e segmentando os servidores de banco de dados de rede diferente da vlan (rede) de usuário.

Uma alternativa, caso não seja possível a migração da aplicação para modelo três camadas (*client-aplication-server*). Seria segmentar esse servidor de banco de dados do modelo de duas camadas de aplicação, dos demais servidores de banco de dados existentes no modelo de três camadas de aplicação. Criando uma estrutura de rede (segmento de rede diferente/subredes) específico para hospedar esse ambiente.

5.2.19 Implementação de Protocolo de autenticação Lógica

O padrão 802.1x define os modelos de controle de acesso e autenticação, restringindo dessa maneira que acessos não autorizados consigam entrada a rede LAN de uma empresa, através de qualquer ponto de rede, seja ele em uma sala de reunião, hall de acesso ou em qualquer departamento onde um usuário visitante consiga acesso a um ponto de rede.

O padrão 802.1x realiza a autenticação de cada usuário conectado a uma porta do switch, definindo a VLAN onde o usuário será conectado e os acessos que ele poderá realizar. Até que seja autenticado, a porta do switch onde o usuário se conectou trafega apenas informações essenciais para a autenticação deste.

Após a autenticação, esta porta permitirá que tráfego passe normalmente. O 802.1x é uma solução para controle de acesso à rede com base em portas, para isso o 802.1x utiliza-se do recurso de validação de certificados de máquina e de usuário através de um servidor externo (*Radius*), que trata as requisições informando aos Switches de rede se devem direcionar o acesso para a rede corporativa (caso certificados validados) ou para rede de visitantes (caso certificados inválidos ou inexistentes).

Entre a utilização das duas tecnologias, concluímos que o 802.1x possui diversos recursos de segurança complementares em comparação a utilização do *Port Security* conforme os itens abaixo:

- Toda autenticação é realizada de maneira centralizada no servidor, assim como seu gerenciamento, independentemente da quantidade de máquinas e o local em que o dispositivo está situado;
- Gerenciamento do usuário permitindo o direcionamento para a VLAN especifica da rede, segmentando de maneira correta o acesso, aumentando a segurança do ambiente e evitando captura de informações que não é destinado ao respectivo colaborador;
- Cada usuário tem suas credenciais, tanto para acessar a rede cabeada como sem fio. Assim não é necessário a configuração equipamento por equipamento e em caso de troca de máquina não é necessário refazer toda a configuração para o novo endereço MAC como no caso do *Port Security*;
- Como o *Port Security* não utiliza um servidor externo para autenticação tal como um servidor de autenticação *RADIUS*, e utiliza endereços físicos para identificar os dispositivos confiáveis, é possível utilizar softwares que “mudam” o endereço físico da

interface de rede, e com isso, caso o atacante consiga o endereço físico de um dispositivo devidamente cadastrado naquele switch, ele pode infiltrar-se na rede utilizando tal endereço e burlando a política de segurança deste ambiente.

A desvantagem deste modelo de segmentação seria a complexidade inicial na implantação deste novo conceito de segmentação da rede.

5.2.20 Produtos Obsoletos/EoL

É recomendado a empresa efetuar um levantamento de seu parque tecnológico para identificar todos os itens que estão em situação caracterizada como tecnologia obsoleta, descontinuadas, a fim de atualizá-las e elevar o nível de segurança para essa questão.

Tecnologia obsoleta significa que o produto (seja ele: *hardware*, *software*) foi categorizado pelo seu fabricante como descontinuado e não possuirá mais suporte, onde o próprio fabricante recomenda a atualização.

Recomenda-se ainda, que o cliente efetue uma força tarefa para atualizar principalmente os equipamentos que fazem conexão com à Internet, pois estão mais expostos a ataques. Caso não seja possível a atualização ou substituição desses equipamentos, a recomendação é segmentá-los numa rede DMZ e controlar os acessos a essa rede pelo *firewall* interno.

5.2.21 Rede de Gerência

É recomendado a criação de um escopo de rede específico para a gerência dos equipamentos de rede e servidores. Através deste escopo o controle de acesso remoto, monitoração e gerência dos equipamentos poderá ser feito através de regras de *firewall* interno liberando apenas este segmento para acessos SNMP, SSH e *Terminal Service* nos ativos de rede.

Nesta rede deveram estar somente as máquinas da equipe de TI do cliente, eliminando o acesso de usuários comuns a portas de gerência de equipamentos de rede e servidores, a fim de eliminar tentativas de conexões por pessoas não autorizadas.

5.3 ESTRATÉGIA DE PRIORIZAÇÃO DE LONGO PRAZO

5.3.1 Redundância e Alta Disponibilidade

O conceito de redundância é utilizado para aumentar o nível de desempenho e continuidade do negócio, é importante utilizar uma estratégia de tolerância a falhas e traçar caminhos alternativos.

Caso algum dos equipamentos sem redundância falhe, comprometerá o bom desempenho do negócio.

É recomendado que o cliente mapeie os principais equipamentos e serviços do ambiente, com intuito de definir uma estratégia afim de criar redundância para eles, de modo a manter a continuidade do negócio.

5.3.2 Servidor de autenticação de dispositivos de rede

Através de uma base de autenticação centralizada, será possível mitigar o risco apontado na autenticação local dos ativos de rede e elevando o nível segurança do ambiente.

De modo que todo e qualquer forma de acesso aos dispositivos de rede serão validados através de base centralizada, proporcionando rastreabilidade e auditoria de acessos, possibilitando adotar políticas de troca de senha, melhor administração e facilitando o diagnóstico de possíveis incidentes.

A utilização do *FortiManager* oferece diversos benefícios, entre eles:

- Padronização das formas de autenticação. Todos os seus usuários podem ser autenticados através de um método único e centralizado, diminuindo a complexidade e facilitando o gerenciamento da rede.
- Gerenciamento aprimorado. O *FortiManager* reduz os esforços para a configuração dos métodos de autenticação e controle de acessos aos equipamentos de rede. Toda a configuração poderá ser executada de forma centralizada.

5.3.3 Duplo fator de autenticação – Acesso à VPN

Deve-se estudar a melhor forma de implementação do duplo fator de autenticação no ambiente para acesso de administrador de domínio para que haja um alinhamento entre a utilização confiável e sem estar engessada com um nível de segurança alto.

Para tanto, vale-se informar que existem três categorias de autenticação, baseadas no conhecimento, na propriedade ou na característica.

Conhecimento: Login e Senha

A autenticação baseada em conhecimento é a mais comum. Simples “segredos” que são fornecidos pelo usuário mediante a uma solicitação.

Propriedade: *Token*, *Smart Cards*, Certificados Digitais entre outros

A autenticação baseada em propriedade eleva o nível de segurança, requisitando que o usuário utilize um *smartcard*, ou um conjunto de códigos gerados por um token, a presença de um certificado digital próprio.

Característica: Biometria, reconhecimento facial, voz entre outros

A autenticação baseada em característica possibilita que o nível de segurança seja mais complexo perante os métodos anteriores se bem implementado, possuir criptografia no canal de comunicação entre o SO e o hardware. Já que são utilizadas características próprias da pessoa. Como leitura da digital, reconhecimento da face ou da voz, *scan* da íris entre outros.

Proteger dados sensíveis online usando múltiplos fatores de autenticação é a melhor política para garantir a segurança e a integridade dos dados. Deve-se notar que, enquanto os dois fatores autenticação podem oferecer maior proteção, existem dois tipos de ataques (mascaramento e sequestro de sessão) quem podem minar qualquer tipo de autenticação.

Um ataque de mascaramento é exatamente o que parece, um ataque que é capaz de assumir uma identidade digital que foi falsamente reivindicada e, portanto, o mecanismo de autenticação é ignorado. Já o sequestro de sessão acontece quando um atacante obtém um ID de sessão e assume o controle de uma sessão já autenticada. Garantindo que todos os dados são transmitidos usando SSL e HTTPS é possível reduzir as chances de sequestro de sessão ocorrer.

Prós:

- Segurança extra caso seu usuário e senha seja comprometido.
- Fácil configuração.
- Possibilidade de utilização do aplicativo mesmo sem sinal de telefone e internet.
- Impede que um usuário malicioso utilize sua conta caso não tenha acesso ao seu celular.
- Possibilidade de efetuar backup no caso de perder ou extraviar o aparelho.

- Possibilidade de gerar alguns códigos de utilização única para emergências em situações que o acesso ao celular esteja impossibilitado (falta de bateria e afins).

Contras:

- Para usuários, pode ser um importuno a necessidade de entrar com um passo a mais no processo de login.

5.3.4 Configuração do Servidor de Logs (*Syslog*)

A organização é orientada a realizar a configuração do Servidor de Logs para que todos os logs sejam centralizados.

Logs são essenciais para preservar informações sobre eventos e problemas que venham a ocorrer na rede. Armazenar estes logs em dispositivos externos asseguram que estes não possam ser apagados ou modificados por uma pessoa não autorizada caso tenha acesso direto à console do equipamento.

Basicamente, o processo de centralização pode ser definido em reunir os arquivos e entradas de log em uma estrutura específica, protegida do resto do ambiente. Existem várias ferramentas disponíveis no mercado que fornecem esta solução, incluindo soluções baseadas em padrões livres como o *Syslog*.

A ideia principal aqui é garantir que os eventos dos ativos críticos da rede sejam constantemente enviados para um local seguro, pois caso um ataque ao ambiente corporativo ocorra, os eventos gerados estarão protegidos e acessíveis, mesmo que a sua cópia original no dispositivo tenha sido comprometida, excluída ou adulterada.

Os acessos aos dispositivos de centralização de log devem ser restritos somente às pessoas autorizadas, garantindo assim a segregação e a proteção necessária dos logs.

6. ACOMPANHAMENTO DO MAPA DE RISCO

Com base na discussão realizada com a empresa foi realizado um levantamento para aplicação dos itens discutidos.

Neste momento não foram realizadas ações especificas para tratamento da Lei Geral de Proteção de Dados Pessoais (LGPD). Porém, os itens trabalhados auxiliam na segurança do ambiente como um todo, assim, contribuem para a proteção de dados pessoais, ferramentas de IPS, IDS e DLP auxiliam na gestão, proteção e vazamentos de informações. Outros pontos abordados como restrições de acessos tem o objetivo de impedir que pessoas não autorizadas tenham acessos a dados sensíveis.

As fases são identificadas por cores para a estratégia de priorização conforme figura 7, tendo itens que podem levar até três meses e itens com maior nível de dificuldade para aplicação podendo levar até um ano.

Figura 7 – Acompanhamento de priorização.

Fonte: Elaborado pelo autor (2021).

7. APLICAÇÕES E RESULTADOS

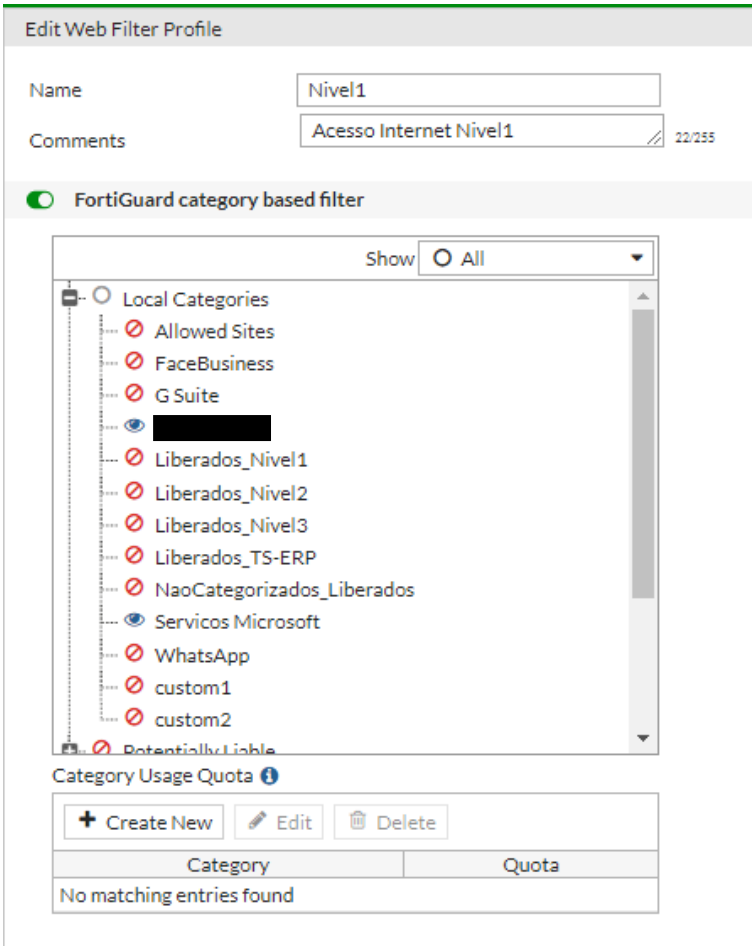
Após a análise de infraestrutura e o estabelecimento de metas e melhorias, foi definido os principais itens junto com os setores da empresa para que fossem afetados da menor maneira possível, fora definidas formas de aplicação.

7.1 RESTRIÇÕES DE ACESSO À INTERNET

Foi elaborado em conjunto com as gerencias níveis de acessos a internet.

Foram criados quatro níveis de acordo com a necessidade de acesso de cada funcionário, esses níveis são baseados em categorias e em casos mais extraordinários são liberados sites específicos para acessos, por exemplo: Usuários do nível 1 tem acesso nas categorias de sites do grupo da empresa e serviços Microsoft, vide figura 8.

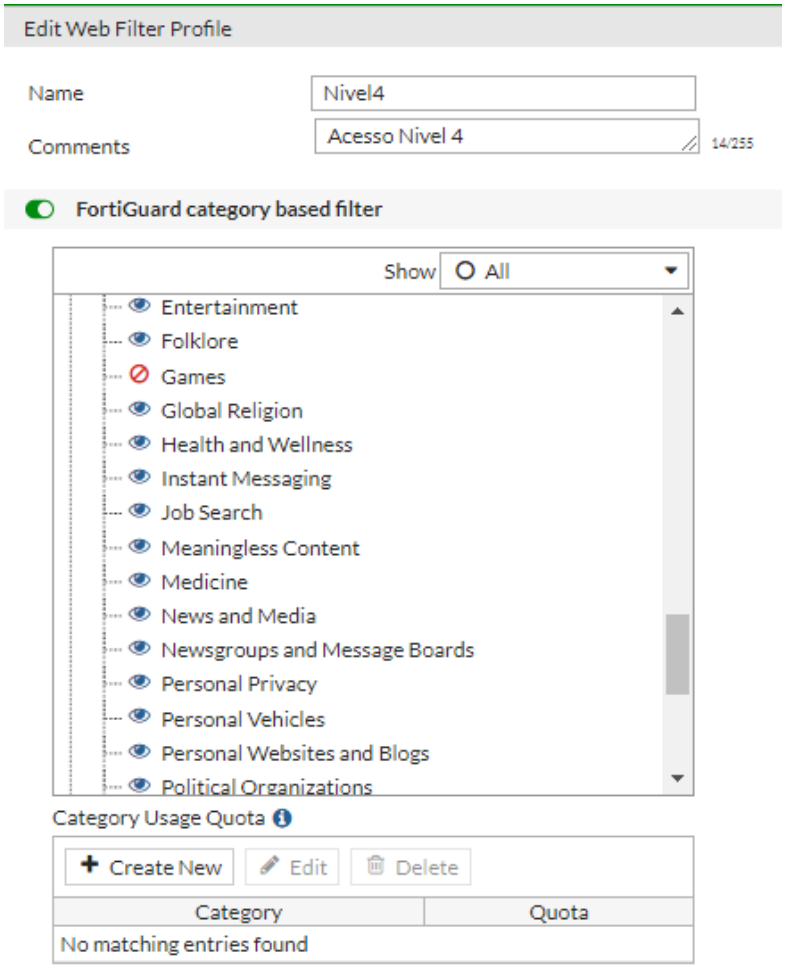
Figura 8 – Nível mais básico de acesso à internet.



Fonte: Elaborado pelo autor (2021).

E usuários que requerem maiores acessos, como sites de bancos, *storage*, notícias, pesquisas, entre outros, foram adicionados a uma nova categoria nível 4, porém de qualquer forma nenhum destes níveis possui acesso irrestrito para a internet, todas as categorias liberadas possuem filtragem e armazenamento de logs, conforme figura 9.

Figura 9 – Nível mais alto de acesso à internet.



Fonte: Elaborado pelo autor (2021).

7.2 BLINDAGEM DE CREDENCIAIS ADMINISTRATIVAS (*JUMP SERVER*)

Para a aplicação destes itens, foram identificados vários pontos que ainda estão em análises, o principal deles é repassar essa ideologia para os funcionários que precisaram se adaptar a esta nova forma de funcionamento.

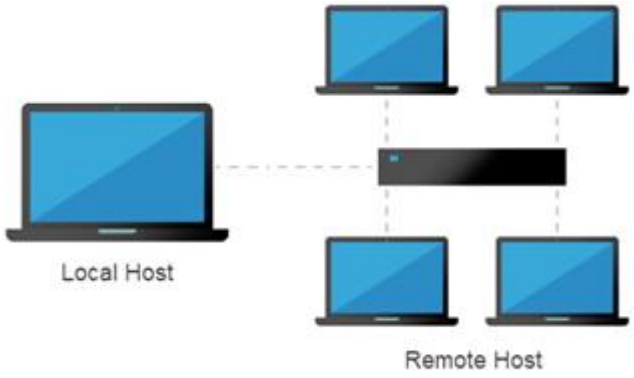
Da forma atual, qualquer usuário que tenha acesso a algum servidor de aplicação para realizar ajustes e manutenções pode acessar diretamente da sua máquina, o que acaba tornando

a rede vulnerável neste ponto, pois caso o usuário seja afetado por alguma ameaça, facilmente o atacante poderá atingir este servidor utilizando a máquina do usuário afetado.

Com a nova política de segurança o usuário que possui acesso a algum servidor precisará acessar um servidor de administração para então poder acessar o servidor de destino, desta forma é colocado mais uma barreira entre a estação e o servidor final.

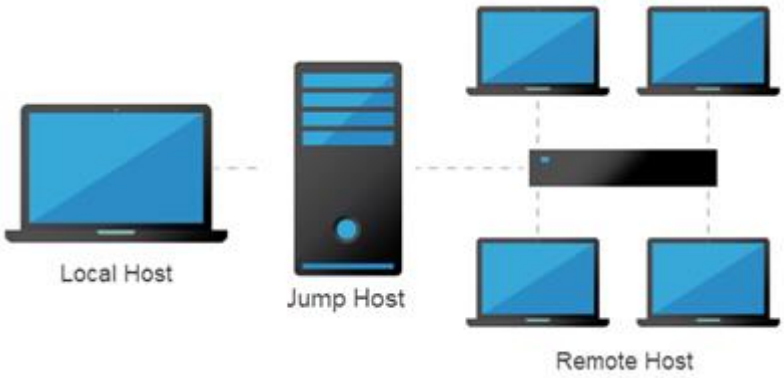
Para os usuários que necessitam este acesso é criado um usuário com poderes administrativos e removido este poder do usuário comum.

Figura 10 – Acesso sem *jump server*.



Fonte: Elaborado pelo autor (2021).

Figura 11 – Acessos com *jump server*.



Fonte: Elaborado pelo autor (2021).

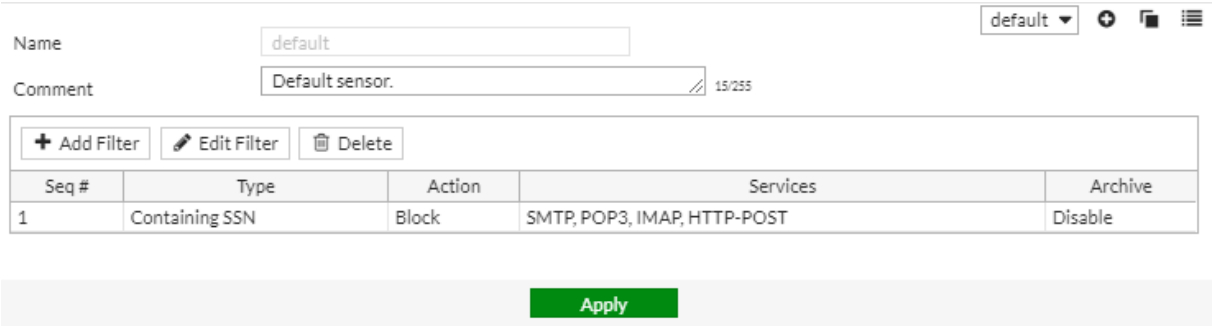
7.3 IMPLEMENTAÇÃO DE DLP

Após a análise e identificação de que a rede não possui DLP, foi realizado a inclusão dessa *feature* nas regras de *firewall*.

O *firewall* utilizado da empresa Fortinet, NGFW, ou seja, *firewall* de próxima geração, possui diversas opções de seguranças, entre elas a opção de DLP, possui opções de inspeção profunda em pacotes, aplicativos, protocolos e portas.

Esta implementação inspeciona os serviços de SMTP, POP3, IMAP, HTTP-POST

Figura 12 – Implementação de DLP em regras de *firewall*.



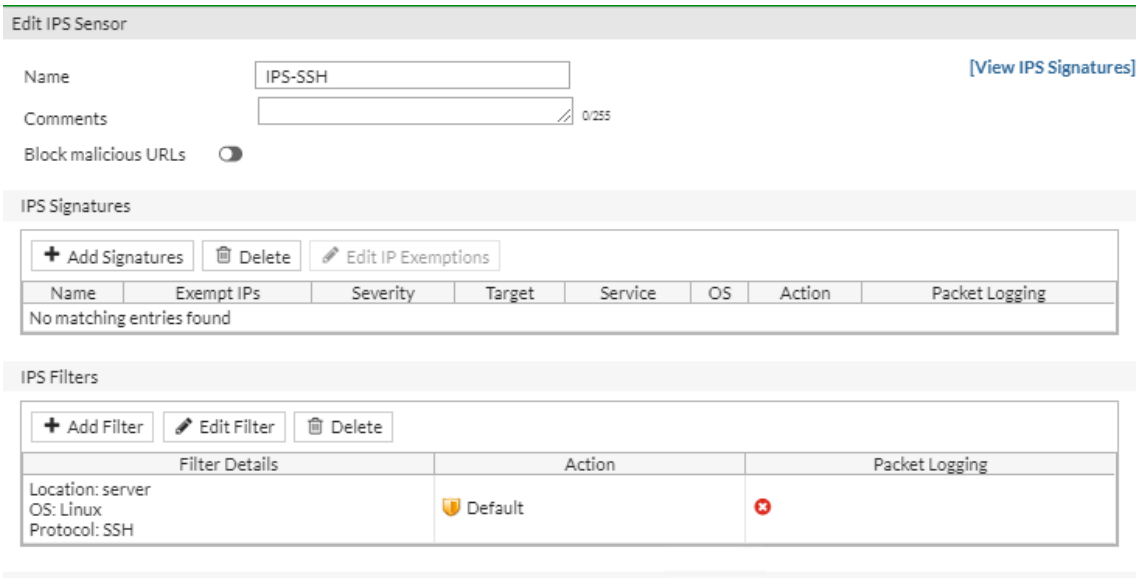
Fonte: Elaborado pelo autor (2021).

7.4 IMPLEMENTAÇÃO DE IPS E IDS

Do mesmo modo em que o serviço de DLP foi implementado no *firewall* o serviço de IPS também foi realizado nas regras de firewall e ainda foi instalado um firewall interno na rede (PFSense), onde foi configurada a ferramenta de IDS *SNORT* para monitoramento entre as redes internas da empresa.

A figura 13 mostra um exemplo implementado de assinatura para o protocolo SSH.

Figura 13 – Assinatura IPS para protocolo SSH.



Fonte: Elaborado pelo autor (2021).

7.5 PUBLICAÇÕES NA REDE INTERNA

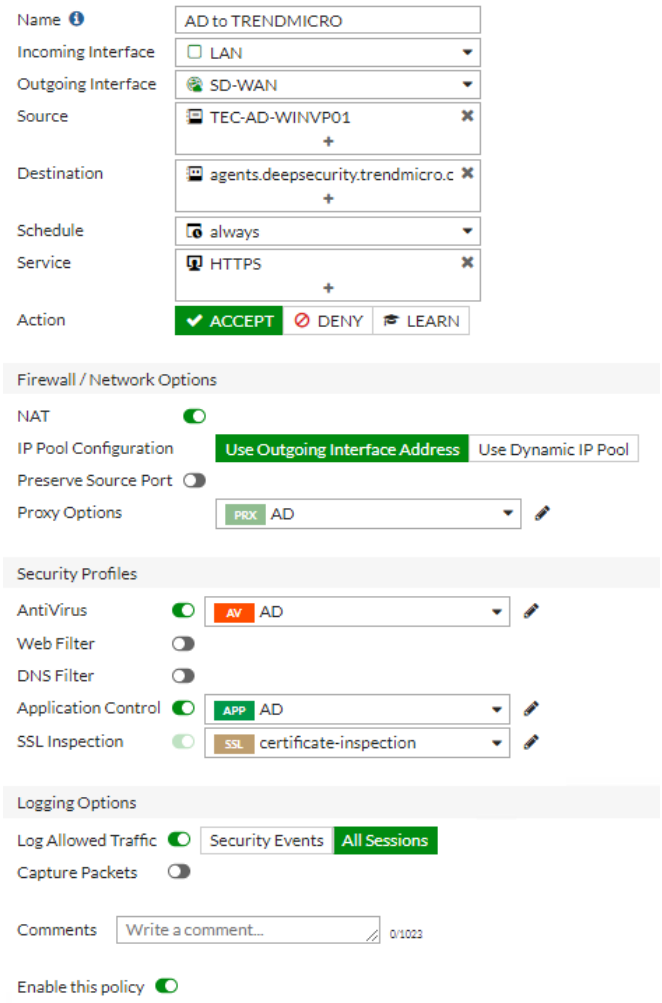
Este item não foi possível o ajuste de imediato. Inicialmente foi ajustado os servidores necessários para novas aplicações de acordo com o recomendado, os servidores mais antigos que estão atualmente na mesma rede dos demais servidores e não em uma DMZ estão sendo gerenciados por regras de conexões e ACLs em switch core interno, onde ficam definidos os protocolos e portas que se terá acessos.

7.6 SERVIDORES COM ACESSO A INTERNET

Os servidores que necessitam possuir acesso para a internet foram migrados para uma nova estrutura, desta forma passaram a possuir dois controles de acessos, além do firewall de borda, também serão monitorados pelo firewall interno. No firewall interno possuem acessos a protocolos e portas especificas e no firewall de borda possuem os acessos a destinos pré-definidos, normalmente são sites de ferramentas de gerenciamento onde precisam ter o acesso para atualizações e monitoramento.

Conforme figura 14 o servidor especificado na opção *source* pode acessar apenas o site de destino utilizando o serviço HTTPS, esta mesma regra possui perfil de antivírus e *application control*, o que garante um monitoramento das aplicações que o site acesse.

Figura 14 – AD com acesso restrito a serviços essenciais.



Fonte: Elaborado pelo autor (2021).

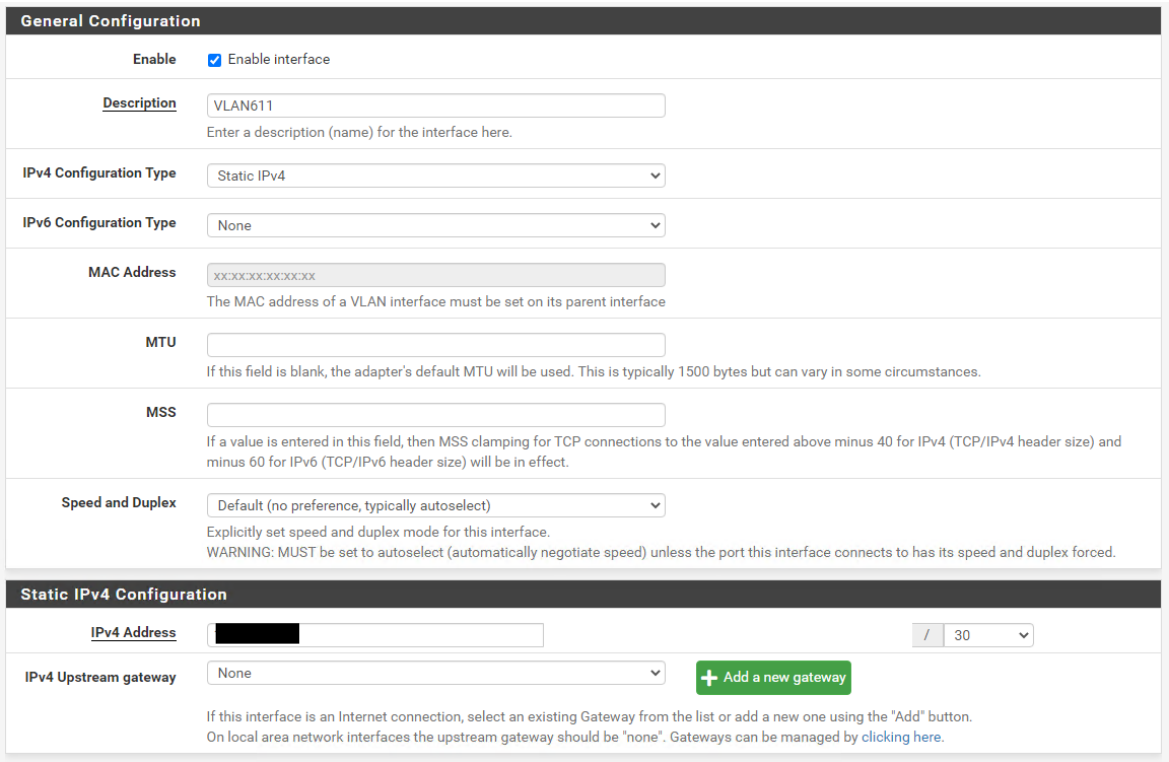
7.7 SEGREGAÇÃO DA REDE INTERNA

Possuindo uma rede com poucas segregações, a empresa corre um grande risco de que alguma máquina do ambiente seja infectada, dado o fato de se comunicar sem nenhuma ou restrição quase nula com outras redes.

Por este item ser de grande impacto para os negócios da empresa foram realizados os ajustes por etapas. Inicialmente os novos ambientes que foram surgindo durante este período foram automaticamente direcionados para esta segmentação, onde cada segmentação da rede possui exatamente a quantidade necessária de hosts para seu funcionamento, por exemplo, se um novo ambiente terá apenas um servidor de aplicação, foi segmentado uma rede com quatro hosts, sendo eles: *subnet*, *gateway*, *host* para aplicação e *broadcast.*

Desta forma foi possível deixar a rede restrita para os hosts já conhecidos e isolados dos demais segmentos. Estes segmentos são gerenciados por um *firewall* interno onde é liberado o acesso a eles somente do que se é de conhecimento, este controle é feito da mesma maneira para acessos que esse host precisa fazer.

Figura 15 – Segmentação da rede com apenas 4 hosts disponíveis.



Fonte: Elaborado pelo autor (2021).

Desta forma caso essa rede seja afetada por alguma invasão não conseguira se comunicar com as demais redes. Esta rede também e protegida por *firewall* interno e de borda.

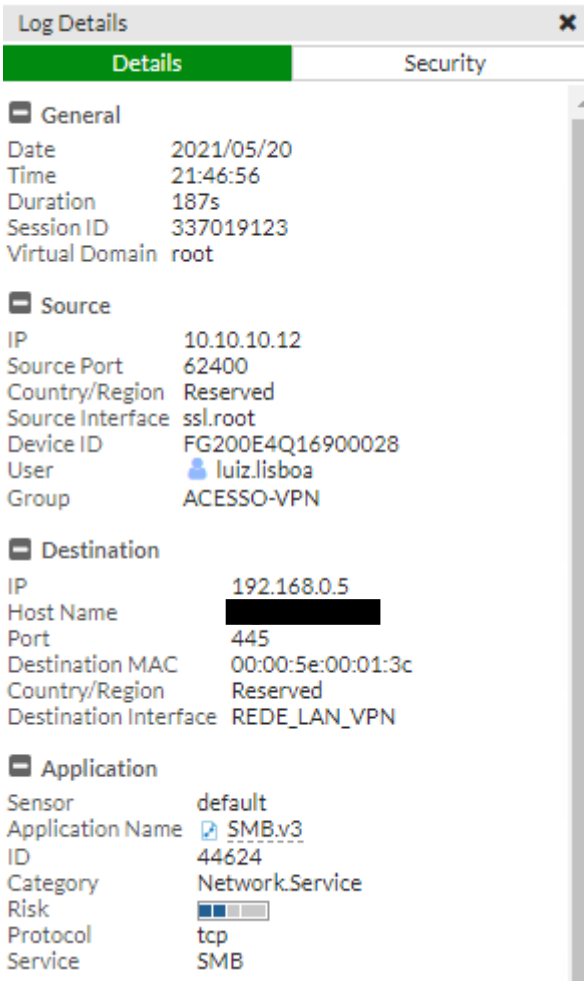
Os servidores antigos estão sendo movidos para esta nova estrutura, com previsão para finalização até o final do ano de 2021.

A segmentação da rede de VPN é controlada diretamente no *firewall* onde se tem criado uma rede específica para usuários que fazem uso da VPN, estes usuários ao se conectarem não são inseridos na rede geral da empresa.

Para cada nível de acesso é criado um perfil, onde é agregado a este perfil os servidores ou até mesmo redes que terão acesso, além de definição de protocolos e portas. Os perfis de acesso são monitorados por *application control* e WAF (*Web Application Firewall*) com essas ferramentas é possível fazer os monitoramentos de aplicações acessadas.

Nos logs de acesso da figura 16, é possível identificar no item risck o nível de risco que está conexão representa, ao receber acesso SMB.

Figura 16 – WAF analisando conexão SMB/SAMBA.



Fonte: Elaborado pelo autor (2021).

7.8 SEGMENTAÇÃO DA REDE DE BANCO DE DADOS

Para este ambiente foi necessário a criação de uma nova estrutura, separando a aplicação do banco de dados. Desta forma se obteve além da segmentação dos servidores, também a segmentação do banco de dados, permitindo assim um melhor controle de acessos, gerenciamento e manutenção.

Anteriormente os servidores ficavam na mesma segmentação que os bancos de dados, permitindo que quem tivesse acesso a um possivelmente conseguiria acessar o outro, com os novos ajustes este acesso não ocorre mais, apenas a aplicação consegue se conectar ao banco

de dados e os responsáveis pela manutenção fazem uso de um servidor separado somente para esta finalidade.

Este controle se faz necessário pois caso a aplicação seja afetada por algum tipo de vírus, os dados da empresa não são afetados, e o reestabelecimento das funcionalidades se tornam muito mais práticas, simples e rápidas.

7.9 PRODUTOS OBSOLETOS – EOL

Os produtos obsoletos são todos os softwares que não possuem mais suporte nem garantia da fabricante, para esta situação foi elaborado um plano de ação visando a atualização, substituição ou até mesmo a simples remoção destes itens do ambiente corporativo.

Tendo em vista que se possuía muitos equipamentos nesta situação os mesmos primeiramente foi analisado sua necessidade na empresa, se havia a necessidade de se ter a versão atual que representa um risco para o ambiente, não sendo necessária foi realizado a atualização, em outros casos onde se mostrou necessário a utilizado de sistemas *EoL* foi realizado configurações especificas por dispositivos, assim, restringindo seu uso no ambiente e impossibilitando que o mesmo se comunique com as demais maquinas da rede.

Desta forma se criou um ambiente mais seguro, evitando que possíveis vulnerabilidades que afetem estas máquinas se distribuam pela rede afetando o ambiente de forma geral.

7.10 REDE DE GERÊNCIA

Um dos itens que foi bastante trabalho foi a criação de uma rede de gerenciamento, uma rede apartada das demais, que tem a finalidade única e exclusivamente de ser utilizada para gerenciar.

Nesta nova estrutura criada se tem acesso aos dispositivos da empresa, tais como, servidores, switches, firewall, entre outros equipamentos que são de acesso crítico, estes dispositivos aceitam acessos e comandos somente da rede de gerenciamento, desta forma impossibilitando que máquinas de usuários comprometidas consigam de alguma forma acesso a estes equipamentos.

7.11 REDUNDÂNCIA E ALTA DISPONIBILIDADE

Por se tratar de um ambiente grande e não se possuir documentação de todos os pontos, existem lacunas onde não se possui redundância de equipamentos, muitas vezes se um equipamento apresenta problemas é necessário realizar a troca, desta forma causando um certo transtorno e parada dos serviços.

Um projeto de melhoria deste quesito foi criado para garantir uma menor parada dos serviços caso seja necessário, equipamentos antigos foram substituídos por novos, assim evitando não se ter garantia e procurando minimizar os riscos de estragos.

Outro ponto que está sendo implementado é a alta disponibilidade para *firewalls*, com esta melhoria não se terá o problema de ficar sem acessos aos serviços disponibilizados de forma geral.

7.12 DUPLO FATOR DE AUTENTICAÇÃO NA VPN

Com o presente cenário vivido na atualidade, com cada vez mais os sistemas podendo ser acessados remotamente, muitas vezes funcionários trabalhando de forma remota utilizando o próprio computador, foi aplicado uma ferramenta para funcionamento do duplo fator de segurança para acessos via VPN.

Foi realizada a instalação de um servidor com a finalidade de autenticação de usuários, é necessário que o usuário instale um aplicativo autenticador de sua preferência no seu smartphone cadastre a conta informada pelos administradores da rede.

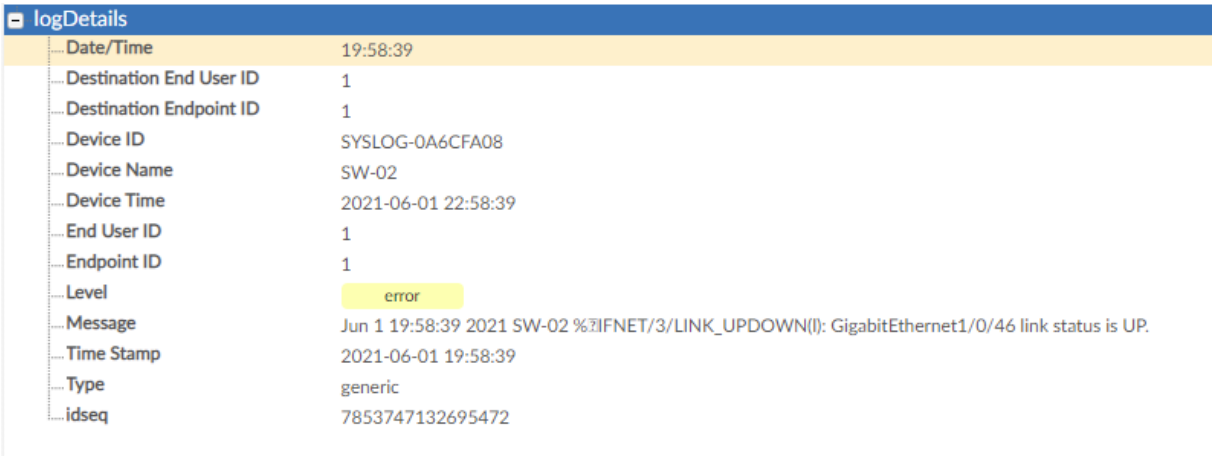
A cada conexão VPN é gerado uma sequência de 6 dígitos aleatoriamente no aplicativo instalado no *smartphone* do funcionário, estes dígitos precisam ser inseridos juntamente com a senha do usuário ao acessar a VPN, desta forma o acesso indevido é dificultado.

7.13 AUSÊNCIA DE CENTRALIZADOR DE LOGS (*SYSLOG*)

A existência de logs se torna fundamental quando se necessita de informações mais profundas e detalhadas sobre problemas, ferramentas, sistemas, ou até mesmo para conhecimento de acessos e configurações. Desta forma foi realizada a ampliação do dispositivo de armazenamento de logs e efetuado as configurações dos equipamentos que foram definidos como principais para se ter essas informações, como switches, servidores e *firewalls*.

Os dispositivos configurados enviam os dados para o *FortiAnalizer* que disponibiliza esses dados por uma interface web de fácil utilização, permitindo assim que quando necessário seja realizado as checagens.

Figura 17 – Exemplo de log de um switch.



Fonte: Elaborado pelo autor (2021).

A figura 18 traz um exemplo de log, onde é exibido que o switch de nome SW-02 apresentou um log do tipo *error* na porta 1/0/46 às 19:58:39 horas. É possível identificar que a porta mencionada estava com status de DOWN e logo em sequência ficou UP.

A próxima etapa será a ampliação do servidor de logs remoto para atender as máquinas do domínio, desta forma atingindo este item em 100%.

Com as análises realizadas e posteriormente as correções aplicadas, foi possível se obter o quadro 5, onde se tem as informações relacionadas aos itens que foram descritos durante este trabalho, a ideia inicial foi que a empresa conseguisse finalizar os itens em 100%, porém com todos os imprevistos que passados durante este período de aplicação não foi possível alcançar este índice.

Quadro 5 - Quadro comparativo status inicial e status final

ID	Risco	Classificação	Inicial	Final	Status
#1	Acesso à internet	Crítico	40%	90%	Em andamento
#2	Blindagem de credenciais administrativas	Crítico	0%	10%	Em andamento
#3	Controle de vazamento de informação (DLP)	Crítico	0%	70%	Em andamento
#4	Implementação de IDS e IPS	Crítico	10%	70%	Em andamento
#5	Publicações na rede interna	Crítico	0%	25%	Em andamento
#6	Segregação da rede interna	Crítico	20%	70%	Em andamento
#7	Segmentação da rede de banco de dados	Crítico	0%	20%	Em andamento
#8	Produtos obsoletos / EoL	Alto	75%	90%	Em andamento
#9	Rede de gerência	Alto	60%	85%	Em andamento
#10	Redundância e alta disponibilidade	Alto	10%	50%	Em andamento
#11	Implementação de duplo fator de autenticação na VPN	Médio	0%	60%	Em andamento
#12	Ausência de centralizador de logs remotos	Baixo	0%	30%	Em andamento

O quadro 5 traz o ID do risco na coluna um, a coluna dois representa a descrição da vulnerabilidade identificada, a coluna três mostra a classificação dos itens, a coluna quatro representa o percentual em que o risco se encontrava quando o estudo foi iniciado, vale ressaltar que apesar de alguns itens já possuírem um valor inicial eles não eram trabalhados isoladamente pela empresa. A coluna cinco mostra o percentual final que o risco se encontra até a finalização

deste documento, e por final a coluna seis mostra o status em que as melhorias se encontram, enquanto não atingirem a meta esperada estipulada de 100% estarão em andamento.

A segurança da informação é algo que deve ser monitorada e melhorada constantemente mesmo estando em conformidade deve-se manter análises periódicas sobre a infraestrutura.

Os itens representados e descritos no quadro 5 são apenas alguns itens que devem ser trabalhados.

CONSIDERAÇÕES FINAIS

Com o mapa de riscos foi possível o levantamento de algumas vulnerabilidades no ambiente da empresa.

Através das recomendações que indicam quais são os padrões a serem seguidos para correção de segurança no ambiente, será possível remover os problemas detectados e manter um alto nível de segurança. As correções descritas nesse documento deverão ser estudadas cuidadosamente por cada um dos responsáveis pelas aplicações das melhorias de segurança.

Além deste processo de análise e correção ficou definido a realização de mais análises voltadas para a segurança, procurando sempre por novas soluções tecnológicas e procurando sempre elevar o nível de segurança da rede proporcionando um ambiente mais seguro e mais organizado, pois com definições de padrões a serem seguidos fica mais fáceis possíveis correções e identificação de eventuais problemas que possam ocorrer.

Outro fato importante que deve ser destacado é o envolvimento das equipes em relação a estas correções, mesmo aplicando correções de maneira o mais transparente possíveis, evitando mudanças drásticas foram obtidos alguns conflitos pois em alguns momentos essas melhorias acabam gerando um passo a mais para realização de algumas tarefas do dia a dia, como por exemplo a criação de uma senha mais forte.

Os objetivos principais deste trabalho, era a realização de uma análise de uma empresa e aplicação de técnicas e melhorias de segurança no ambiente e conscientização os envolvidos, estes objetivos propostos no início do trabalho foram atingidos por completo. Estas melhorias não podem parar e foi possível passar este pensamento adiante, levando esta conscientização para os envolvidos.

Este foi o primeiro passo na busca de uma empresa mais segura, a segurança da informação é uma área onde nunca se deve parar de procurar soluções e melhorias.

Para trabalhos futuros se tem como objetivo trazer uma abordagem mais focada em servidores, segurança de usuário e ambiente físico.

Outros trabalhos focados na LGPD são de grande contribuição, podendo utilizar este como base para implementação de melhorias que colaboram na segurança da informação.

REFERÊNCIAS

ALEXANDRIA, J. C. S. **Gestão de segurança da informação – uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica.** Tese de Doutorado, Universidade de São Paulo, São Paulo, SP, Brasil, 2009.

DA VEIGA, Adéle; ELOFF J.H.P.. An information security governance framework. Information Systems Management. África do Sul, 2007.

DA VEIGA, Adéle; MARTINS, Nico. Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 2015.

ERNEST & YOUNG. Crimes Cibernéticos são a maior ameaça à sobrevivência das empresas, aponta estudo da EY, 2013.

FREITAS, Eduardo Antônio Mello; AMOUZOU, Koffi Djima. Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação. V13, 2009.

GABBAY, Max Simon. **Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte**. 2006.

ISACA. Considerações essenciais para a proteção do vazamento de dados confidenciais através de ferramentas de prevenção de perda de dados, 2014.

ABNT NBR ISO/IEC 17799:2001. Tecnologia da informação – Código de prática para a gestão da segurança da informação, 2001.

ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements. 2005

ISO/IEC 27002:2005. Information technology – Security techniques – Information security management systems – Requirements. 2005

ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. 2013

SOUZA, J. G. S. *et al*. MANAGEMENT OF INFORMATION SECURITY RISKS IN A FEDERAL PUBLIC INSTITUTION: A CASE STUDY. 2016.

LANDOLL, Douglas J. The Security Risk Assessment Handbook: a complete guide for performing Risk Assessment, CRCwhe Press, 2011

LAUREANO, Marcos AP; MORAES, Paulo Eduardo Sobreira. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, 2005.

LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação**. Senac, 2018.

LUFTMAN, J. N. Assessing IT-Business alignment. Information Systems Management, 2003.

KLOSTERBOER, LARRY. Implementing ITIL Configuration Management. Massachusetts, USA: IBM Press, 2008.

PWC. Principais resultados da Pesquisa Global de segurança da informação, 2014.

Tanenbaum, A.S.: Modern Operating Systems. Prentice Hall Press, 2001

ROEBUCK, K. Data loss prevention (DLP) -high-impact strategies.Brisbane:Emereo Pty Limited, 2011.

Santos, R. **O Bê-a-Bá da Gestão de Risco e Governança**, 2008.

SÊMOLA, M. Gestão da Segurança da Informação: visão executiva da segurança da informação, 2003.

SILVA NETTO, Abner da; SILVEIRA, Marco Antônio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM Universidade Federal do Rio Grande do Norte **Journal of Information Systems and Technology Management**, 2007.

POSTHUMUS, S., VON SOLMS, R. A Framework for the Governance of Information Security. Computers & Security, 2004.

TUDOR, J. K. Information Security Architecture – An integrated approach to security in an organization. Boca Raton, FL: Auerbach, 2000.

Wheeler, Evan. Security Risk Management Building an Information Security Risk Management Program from the Ground Up, Elsevier, Inc. 2011.