SOFTWARE DE SEGURANÇA PARA PEQUENAS EMPRESAS: OTIMIZANDO A ESCOLHA COM O MÉTODO AHP

SECURITY SOFTWARE FOR SMALL BUSINESSES: OPTIMIZING THE CHOICE USING THE AHP METHOD

Carlos Ricardo Bifi
Fatec Araraquara
carlos.bifi@fatec.sp.gov.br

Mary Kodato Okabe
Universidade de Taubaté - UNITAU
mary.okabe@gmail.com

Ronald Adomaitis da Silva
Universidade de São Paulo – USP
ronald.aldomaitis@usp.br

Resumo

Este artigo apresenta um estudo de caso sobre a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) para pequenas empresas de desenvolvimento de *software*. Estas empresas, com recursos limitados, precisam priorizar as medidas de segurança a serem implementadas. Para o desenvolvimento do trabalho foi utilizado um método de Pesquisa Operacional chamado de *Analytic Hierarchy Process* (AHP), no qual foram definidos três critérios de segurança: confidencialidade, integridade e disponibilidade. As alternativas consideradas foram: implementação de um *firewall*, implantação de um sistema de controle de acesso, treinamento de conscientização em segurança e aquisição de um *software* antivírus. A análise dos resultados, baseado nas informações coletadas, indicou que a implantação de um sistema de controle de acesso e a implementação de um *firewall* são as medidas mais eficazes para proteger as informações da empresa.

Palavras-chave: Segurança da Informação, Pequenas Empresas, *Analytic Hierarchy Process* (AHP), Medidas de Segurança

Abstract

This article presents a case study on the implementation of an Information Security Management System (ISMS) for small software development companies. These companies, with limited resources, must prioritize which security measures to implement. For this study, an Operational Research method called Analytic Hierarchy Process (AHP) was applied. Three security criteria were defined: confidentiality, integrity and availability. The alternatives considered were implementing a firewall, deploying an access control system, conducting security awareness training and acquiring antivirus software. The analysis of the results, based on the collected data, indicated that deploying an access control system and implementing a firewall are the most effective measures to protect the company's information.

Keywords*:* Information Security, Small Businesses, Analytic Hierarchy Process (AHP), Security Measures

1. Introdução

Chegamos a uma época em que a tecnologia e a informação tornaram-se uma preocupação para empresas de todos os portes, quando se tratando da segurança da informação (SI). Para o sucesso e a continuidade dos negócios e para a proteção de dados mantendo-os confidenciais, a garantia da integridade dos sistemas e a disponibilidade dos serviços tornaram-se prioridades. No entanto, a complexidade dos ambientes de Tecnologia da Informação (TI) e a variedade de ameaças existentes, exigem uma abordagem estruturada e eficiente para a tomada de decisões nesta área. É nesse contexto que a técnica da Pesquisa Operacional, por meio do método *Analytic Hierarchy Process* (AHP), surge como ferramenta confiável e eficaz para auxiliar na análise e priorização de medidas de segurança cibernética.

A Segurança da Informação (SI) é um campo que evolui rapidamente, impulsionado pelo avanço tecnológico e pela crescente sofisticação das ameaças cibernéticas. Segundo Whitman e Mattord (2011), a segurança da informação refere-se às medidas adotadas para proteger informações e os sistemas que as manipulam, armazenam e transmitem, buscando garantir a confidencialidade, integridade e disponibilidade frente a possíveis ameaças. Essa definição destaca a tríade *Confidentiality, Integrity, Availability* - CIA, que é fundamental para qualquer estratégia de segurança.

Na Pesquisa Operacional (PO), o método AHP, desenvolvido por Thomas L. Saaty na década de 1970, é uma metodologia que facilita a tomada de decisões complexas, permitindo que os gestores avaliem múltiplos critérios de forma estruturada. Saaty (1980) argumenta que o AHP é uma metodologia de medição que utiliza comparações em pares e baseia-se nos julgamentos de especialistas para estabelecer prioridades. Essa abordagem é particularmente útil na área da segurança da informação, onde as decisões devem considerar uma variedade de fatores, desde a vulnerabilidade dos sistemas até o impacto potencial de uma violação de dados.

A aplicação do AHP na segurança da informação permite que as organizações priorizem suas iniciativas de segurança com base em critérios claramente definidos e ponderados. Por exemplo, uma empresa pode usar o AHP para determinar quais ativos de Tecnologia da Informação (TI) são mais críticos e, portanto, merecem maior proteção. Para isso, ela pode comparar a criticidade de diferentes ativos, como servidores de dados, sistemas de e-mails e dispositivos móveis, considerando critérios como confidencialidade das informações, impacto

financeiro em caso de indisponibilidade e custo de recuperação. O AHP ajuda a determinar a importância relativa de cada ativo e a priorizar os investimentos em segurança.

De acordo com Gordon e Loeb (2002), os investimentos em segurança da informação devem ser alinhados ao valor dos ativos protegidos e ao grau de ameaça a que estão expostos. Essa perspectiva reforça a importância de uma abordagem baseada em risco, onde o AHP pode ser instrumental na avaliação e diminuição dos riscos de segurança. O método AHP, por meio da estruturação hierárquica do problema, da realização de comparações paritárias entre os critérios e alternativas, e do cálculo das prioridades, permite que os gestores avaliem os riscos de forma sistemática e transparente, direcionando os investimentos em segurança de forma mais eficiente.

Não podemos negar que a segurança da informação é uma preocupação crescente para as empresas modernas, e a complexidade do ambiente de TI exige ferramentas robustas para a tomada de decisões. Dito isto, o método AHP oferece uma solução estruturada e baseada em critérios para a priorização das medidas de segurança, ajudando as organizações a protegerem seus ativos mais valiosos e a garantir a continuidade dos negócios.

2. Questão de Pesquisa e Objetivos

2.1. Questão de Pesquisa

Considerando o contexto que será apresentado no estudo de caso da empresa Tech Solutions, a pesquisa busca responder à seguinte questão:

Como uma pequena empresa de desenvolvimento de *software* com recursos limitados pode priorizar a implementação de medidas de segurança da informação de forma eficiente para proteger suas informações e atender aos requisitos de conformidade?

2.2. Objetivos

a) Objetivo Geral

Analisar a aplicação do método *Analytic Hierarchy Process* (AHP) na priorização de medidas de segurança da informação em uma pequena empresa de desenvolvimento de *software*, considerando os critérios de Confidencialidade, Integridade e Disponibilidade.

b) Objetivos Específicos

- Descrever o contexto da segurança da informação em pequenas empresas de desenvolvimento de *software*.
- Apresentar o método AHP e sua aplicação na tomada de decisão em segurança da informação.
- Definir os critérios de Confidencialidade, Integridade e Disponibilidade no contexto do estudo de caso.
- Avaliar as alternativas de segurança (*Firewall*, Controle de Acesso, Treinamento e Antivírus) utilizando o método AHP.
- Analisar os resultados da aplicação do método AHP e discutir as implicações para a tomada de decisão na empresa.

3. Referencial Teórico

3.1. O Método *Analytic Hierarchy Process* (AHP)

O AHP é um método de tomada de decisão multicritério que permite decompor um problema complexo em uma hierarquia de critérios e alternativas. Por meio de comparações par a par, o AHP permite determinar a importância relativa de cada critério e, posteriormente, a prioridade de cada alternativa em relação aos critérios estabelecidos.

3.2. Fundamentos do AHP

O AHP baseia-se na ideia de que a mente humana é capaz de fazer julgamentos comparativos de forma mais precisa do que atribuir valores numéricos diretamente. Ao comparar pares de elementos, o decisor expressa sua preferência ou a importância relativa de um elemento em relação ao outro, utilizando uma escala numérica predefinida. Essas comparações são então organizadas em matrizes, que são processadas matematicamente para obter pesos que representam a importância de cada elemento na hierarquia.

3.3. Etapas do Método AHP

A aplicação do AHP envolve as seguintes etapas:

- **Definição do problema e do objetivo:** O primeiro passo é definir claramente o problema de decisão e o objetivo a ser alcançado. No contexto da segurança da informação, o problema pode ser, por exemplo, "como alocar recursos de segurança de forma eficiente?" ou "qual a melhor solução de segurança para proteger um determinado ativo?".
- **Construção da hierarquia:** O problema é decomposto em uma hierarquia, com o objetivo no topo, seguido pelos critérios de decisão e, por fim, pelas alternativas a serem avaliadas.
- **Comparações par a par:** Para cada nível da hierarquia, são realizadas comparações pares entre os elementos, utilizando uma escala numérica para expressar a importância relativa de um elemento em relação ao outro.
- **Cálculo dos pesos:** As matrizes de comparação são processadas para obter os pesos de cada elemento em relação ao seu nível hierárquico superior.
- **Síntese dos resultados:** Os pesos são agregados ao longo da hierarquia para determinar a prioridade global de cada alternativa.

3.4. Vantagens e Limitações do AHP

O AHP apresenta diversas vantagens, como a sua capacidade de lidar com problemas complexos e subjetivos, a sua estrutura hierárquica que facilita a organização do problema e a

sua flexibilidade para incorporar diferentes tipos de critérios. No entanto, o AHP também possui algumas limitações, como a subjetividade inerente ao processo de comparação par a par e a possibilidade de inconsistência nas avaliações.

3.5. AHP na Segurança da Informação

A aplicação do AHP na segurança da informação permite uma abordagem estruturada e analítica para a tomada de decisões, auxiliando na seleção e priorização de medidas de segurança, destacando-se os seguintes pontos:

a) **Definindo Critérios de Segurança:** A primeira etapa na aplicação do AHP é a definição dos critérios de segurança que serão considerados na análise. Esses critérios podem ser derivados de *frameworks* de segurança da informação, como o ISO 27001, ou ser definidos de acordo com as necessidades específicas da organização. Alguns critérios comuns incluem:
   - **Confidencialidade:** Garantir que as informações sejam acessíveis apenas a pessoas autorizadas.
   - **Integridade:** Assegurar que as informações sejam precisas e completas e que não sejam modificadas de forma não autorizada.
   - **Disponibilidade:** Garantir que as informações e os sistemas estejam disponíveis para os usuários autorizados quando necessário.

b) **Construindo a Hierarquia de Decisão:** Após definir os critérios, a próxima etapa é construir a hierarquia de decisão. O objetivo, no topo da hierarquia, pode ser, por exemplo, "selecionar a melhor solução de segurança para proteger os dados da empresa". Os critérios de segurança (confidencialidade, integridade, disponibilidade) ocupam o nível intermediário. No nível inferior, são listadas as alternativas de segurança a serem avaliadas, como *firewall*, *software* antivírus, criptografia, etc.

c) **Priorizando Medidas de Segurança:** Com a hierarquia definida, o próximo passo é realizar as comparações par a par entre os critérios e as alternativas, utilizando uma escala numérica para expressar a importância relativa de cada elemento. Após a realização das comparações, o método AHP calcula os pesos de cada critério e de cada alternativa, permitindo a priorização das medidas de segurança.

4. Metodologia

O estudo de caso é uma metodologia de pesquisa valiosa para investigar fenômenos complexos em seus contextos reais, proporcionando uma análise aprofundada e rica em detalhes. Neste capítulo, exploramos a fundamentação teórica do estudo de caso e justificamos sua aplicação na pesquisa em segurança da informação, com ênfase na utilização de casos fictícios.

4.1. Definição e Característica de um Estudo de Caso

De acordo com Yin (2014), o estudo de caso é uma investigação empírica que examina um fenômeno contemporâneo dentro de seu contexto real, especialmente quando as fronteiras entre o fenômeno e o contexto não são claramente evidentes. Essa metodologia é particularmente útil quando se busca responder a questões do tipo “como” e “por que”, permitindo uma compreensão abrangente e detalhada do objeto de estudo.

Stake (1995) complementa essa definição ao destacar que o estudo de caso é uma estratégia de pesquisa que se concentra na singularidade e na complexidade de um caso particular, proporcionando uma visão holística e contextualizada. Ele enfatiza que essa abordagem é ideal para explorar situações em que o pesquisador tem pouco controle sobre os eventos e onde o foco está em fenômenos contemporâneos dentro de contextos da vida real.

4.2. Justificativa para o Uso de Estudo de Caso e o Uso de Casos Fictícios

A escolha do estudo de caso para este artigo justifica-se pela complexidade da implementação de um Sistema de Gestão de Segurança da Informação (SGSI) em pequenas empresas de desenvolvimento de *software*, um fenômeno com múltiplos fatores e interações. O estudo de caso permite analisar essas interações em seus contextos específicos, proporcionando uma compreensão mais profunda do tema.

Além disso, o estudo de caso possibilita a exploração de questões práticas e contextuais, como a priorização de medidas de segurança em empresas com recursos limitados. Investigar as decisões e ações dos gestores em tempo real oferece *insights* sobre as melhores práticas e os desafios enfrentados.

É importante destacar que a utilização de um estudo de caso fictício é um recurso para modelar e simular cenários complexos, testando diferentes variáveis e explorando possíveis resultados. Schiavon (2019) argumenta que o estudo de caso fictício permite a criação de cenários ideais para a aplicação de métodos e modelos, como o AHP, facilitando a compreensão e o aprendizado. Essa abordagem permite analisar a aplicação do método em um ambiente controlado, explorando suas potencialidades e limitações de forma didática.

Dessa forma, o estudo de caso fictício contribui para a construção de conhecimento e para o desenvolvimento de soluções eficazes em segurança da informação, servindo como modelo para futuras implementações em cenários reais.

4.3. O caso e processos do AHP

a) Descrição do Cenário

A Tech Solutions, empresa de desenvolvimento de *software* localizada em São Carlos - SP, fundada em 2010, busca implementar um SGSI para proteger suas informações e atender aos requisitos de conformidade. Com 35 funcionários, incluindo 5 gestores, a empresa atua no desenvolvimento de aplicativos *mobile* e *web* para pequenas e médias empresas.

A Tech Solutions armazena dados sensíveis de clientes, como informações pessoais e financeiras, além de propriedade intelectual relacionada aos seus *softwares*. Devido a recursos limitados, a empresa precisa priorizar as medidas de segurança a serem implementadas, considerando as seguintes alternativas:

1) Implementação de um *firewall*: Para proteger a rede da empresa contra acessos não autorizados.
2) Implantação de um sistema de controle de acesso: Para gerenciar o acesso de usuários a informações e sistemas.
3) Treinamento de conscientização em segurança: Para educar os funcionários sobre as melhores práticas de segurança da informação.

4) Aquisição de um *software* antivírus: Para proteger os computadores da empresa contra *malware*.

A Tech Solutions reconhece a importância de proteger suas informações, mas enfrenta o desafio de otimizar seus investimentos em segurança da informação. Para tomar a decisão mais adequada, a empresa utilizará o método AHP para priorizar as alternativas, considerando os critérios de Confidencialidade, Integridade e Disponibilidade.

b) Aplicação do AHP

Para determinar quais medidas de segurança devem ser priorizadas, a empresa decidiu utilizar o método de *Analytic Hierarchy Process* (AHP). Este modelo ajuda a tomar decisões complexas, considerando múltiplos critérios e alternativas.

Os critérios de segurança definidos pela empresa são:

1) **Confidencialidade**: Garantir que as informações sejam acessíveis apenas por pessoas autorizadas.
2) **Integridade**: Assegurar que as informações sejam precisas e completas.
3) **Disponibilidade**: Garantir que as informações estejam disponíveis quando necessário.

A seguir, realizamos comparações par a par entre os critérios e, posteriormente, entre as alternativas. Nesta etapa os especialistas decisores utilizarão uma escala de 1 a 9, onde 1 indica igual importância e 9 indica extrema importância.

c) Comparação Par a Par dos Critérios para cálculo dos pesos

A Tabela 1 apresenta a comparação par a par dos critérios de Confidencialidade, Integridade e Disponibilidade, utilizando a escala fundamental de Saaty. Os valores demonstram a importância relativa de cada critério em relação aos demais.

Tabela 1: Comparação par a par dos critérios

Critério	Confidencialidade	Integridade	Disponibilidade
Confidencialidade	1	3	5
Integridade	1/3	1	3
Disponibilidade	1/5	1/3	1

Fonte: Autores, 2024

Observa-se que:

- A Confidencialidade é considerada 3 vezes mais importante que a Integridade e 5 vezes mais importante que a Disponibilidade.
- A Integridade é 3 vezes mais importante que a Disponibilidade.

Esses valores, como apontado anteriormente, são obtidos por meio de julgamentos de especialistas decisores no qual refletem a prioridade relativa entre os critérios de cada um. A escala de Saaty permite a quantificação da importância relativa de cada fator, auxiliando na tomada de decisão.

Próximas etapas, a partir do preenchimento da Tabela 1 pelos especialistas decisores, é calcular os pesos para cada critério, conforme se observa nas Tabelas 2, 3 e 4.

Tabela 2: Soma das colunas da tabela 1

Critério	Confidencialidade	Integridade	Disponibilidade
Soma	1.533	4.333	9

Fonte: Autores, 2024

Tabela 3: Normalização

Critério	Confidencialidade	Integridade	Disponibilidade
Confidencialidade	0,6521739	0,6923077	0,555556
Integridade	0,2173913	0,2307692	0,333333
Disponibilidade	0,1304348	0,0769231	0,111111

Fonte: criada pelos autores

Tabela 4: Cálculo dos pesos dos critérios

Critério	Peso
Confidencialidade	0,633346
Integridade	0,260498
Disponibilidade	0,106156

Fonte: Autores, 2024

Tabela 5: Análise de Consistência

ƛmáx	3,039
R.I.	0,58
C.I.	0,019
C.R.	0,033

Fonte: Autores, 2024

Para calcular os pesos o processo se inicia com a construção de uma matriz de comparação par a par, na qual cada critério é comparado com os demais em termos de sua importância relativa - Tabela 1.

A Tabela 2 apresenta a soma das colunas da matriz de comparação par a par na Tabela 1; essa etapa é importante para a normalização da matriz, que é realizada na Tabela 3.

Na Tabela 3, cada valor da matriz da Tabela 1 é dividido pela soma da coluna correspondente da Tabela 2. Essa normalização garante que a soma dos valores em cada coluna seja igual a 1.

A Tabela 4 exibe o cálculo dos pesos de cada critério. Os pesos são calculados pela média aritmética dos valores de cada linha da matriz da Tabela 3.

Finalmente, a Tabela 5 aponta para uma Análise de Consistência adequada, ao passo que a Cálculo de Consistência aponta para a Razão de Consistência de 0,033, mantendo-se, portanto, abaixo de 10%, o que é favorável, conforme preconizado pelo autor do método.

Os pesos finais obtidos foram: *i)* Confidencialidade = 0,633346; *ii)* Integridade = 0,260498; e *iii)* Disponibilidade = 0,106156.

Esses pesos representam a importância relativa de cada critério na tomada de decisão. O critério de Confidencialidade, com peso 0,633346, é o mais importante, seguido pela

Integridade (0,260498) e pela Disponibilidade (0,106156).

d) Comparação Par a Par das Alternativas

A comparação par a par das alternativas para cada critério é mais uma etapa fundamental no método AHP, utilizada para determinar a importância relativa de cada alternativa em relação a um critério específico. Esse processo facilita a tomada de decisão ao permitir uma avaliação detalhada e estruturada das alternativas.

Por meio da comparação par a par, capturamos as preferências dos tomadores de decisão de forma mais intuitiva, comparando as alternativas duas a duas e expressando a importância relativa de uma sobre a outra.

Essa etapa possibilita o cálculo das prioridades de cada alternativa em relação a cada critério. Ao normalizar as comparações e calcular os pesos médios, obtemos uma visão clara de qual alternativa é mais adequada para cada critério.

As tabelas de comparação par a par contribuem para a transparência do processo de tomada de decisão, documentando os julgamentos e permitindo a justificativa das escolhas. Além disso, ajudam a garantir a consistência das decisões, assegurando que sejam baseadas em critérios claros e objetivos.

No contexto do estudo de caso, a comparação par a par será importante para determinar qual alternativa (*firewall*, controle de acesso, treinamento ou antivírus) é mais eficaz em relação a cada critério (confidencialidade, integridade e disponibilidade), começando por confiabilidade. A seguir, os processos para determinar os pesos e as análises destas alternativas frente aos critérios, serão análogos feito no subitem *4.3, item c*.

Tabela 6: alternativas em relação ao critério confiabilidade

Alternativa	*Firewall*	Controle de acesso	Treinamento	Antivírus
Firewall	1	5	2	3
Controle de acesso	1/5	1	5	3
Treinamento	1/2	1/5	1	4
Antivírus	1/3	1/3	1/4	1

Fonte: Autores, 2024

Tabela 7: Soma das Colunas

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Soma	2,033	6,533	8,250	11

Fonte: Autores, 2024

Tabela 8: Normalização

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Firewall	0,4918033	0,765306	0,242424	0,272727
Controle de Acesso	0,0983607	0,153061	0,606061	0,272727
Treinamento	0,2459016	0,030612	0,121212	0,363636
Antivírus	0,1639344	0,051020	0,030303	0,090909

Fonte: Autores, 2024

Tabela 9: Cálculo dos Pesos das alternativas frente a confiabilidade

Alternativa	pesos
Firewall	0,443065
Controle de acesso	0,282552
Treinamento	0,190341
Antivírus	0,084042

Fonte: Autores, 2024

Tabela 10: Análise de Consistência

λmáx	3,821
R.I.	0,9
C.I.	0,060
C.R.	0,066

Fonte: Autores, 2024

As tabelas apresentadas demonstram a aplicação do método AHP para calcular a prioridade (pesos) de cada alternativa (*Firewall*, Controle de Acesso, Treinamento e Antivírus) em relação ao critério de Confiabilidade.

A Tabela 6: A matriz de comparação par a par indica a importância relativa de cada alternativa em relação às demais. Por exemplo, o valor "2" na célula Controle de Acesso x *Firewall* indica que o Controle de Acesso é considerado duas vezes mais importante que o *Firewall* em termos de Confiabilidade.

A Tabela 7: A soma das colunas da matriz de comparação é parte importante para a normalização dos dados.

A Tabela 8: Cada elemento da matriz original foi dividido pela soma da sua coluna, resultando na matriz normalizada. Essa normalização garante que a soma dos elementos em cada coluna seja igual a 1.

A Tabela 9: O cálculo dos pesos, de cada alternativa é feito pela média aritmética dos valores de cada linha da matriz normalizada.

A Tabela 10 aponta para uma Análise de Consistência adequada, ao passo que a Cálculo de Consistência aponta para a Razão de Consistência de 0,066, mantendo-se, portanto, abaixo de 10%, o que é favorável, conforme preconizado pelo autor do método.

Os Resultados obtidos das tabelas apontam para os pesos revelados: *Firewall* (0,443065) é a alternativa mais importante para garantir a Confiabilidade, seguidas pelos outras, *Controle de acesso* (0,282552), Treinamento (0,190341) e Antivírus (0,084042).

Essa análise demonstra como o método AHP permite a quantificação da importância relativa de cada alternativa em relação a um critério específico, auxiliando na tomada de decisão de forma estruturada e transparente. Vamos realizar o mesmo processo para Integridade

Tabela 11: alternativas em relação ao critério Integridade

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Firewall	1	2	7	8
Controle de Acesso	1/2	1	5	1/2
Treinamento	1/7	1/5	1	7
Antivírus	1/8	2	1/7	1

Fonte: Autores, 2024

Tabela 12: Soma das Colunas

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Soma	1,768	5,200	13,143	16,500

Fonte: Autores, 2024

Tabela 13: Normalização

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Firewall	0,5656566	0,384615	0,532609	0,484848
Controle de Acesso	0,2828283	0,192308	0,380435	0,030303
Treinamento	0,0808081	0,038462	0,076087	0,424242
Antivírus	0,0707071	0,384615	0,010870	0,060606

Fonte: Autores, 2024

Tabela 14: Cálculo dos pesos das alternativas frente a integridade

Alternativa	Prioridade
Firewall	0,491932
Controle de Acesso	0,221468
Treinamento	0,154900
Antivírus	0,131700

Fonte: Autores, 2024

Tabela 15: Análise de Consistência

ƛmáx	3,941
R.I.	0,9
C.I.	0,020
C.R.	0,022

Fonte: Autores, 2024

As Tabelas 11 a 14 ilustram o processo de cálculo dos pesos das alternativas (*Firewall*, Controle de Acesso, Treinamento e Antivírus) em relação ao critério de Integridade, utilizando o método AHP.

Tabela 11: A matriz de comparação par a par, construída com base em julgamentos de especialistas, quantifica a importância relativa de cada alternativa em relação às demais no que diz respeito à Integridade.

Tabela 12: Apresenta a soma dos valores de cada coluna da matriz de comparação, etapa necessária para a normalização.

Tabela 13: Exibe a matriz normalizada, obtida pela divisão de cada elemento da matriz original pela soma da sua coluna.

Tabela 14: Por fim, os pesos de cada alternativa são calculados pela média aritmética dos valores de cada linha da matriz normalizada.

A Tabela 15 aponta para uma Análise de Consistência adequada, ao passo que a Cálculo de Consistência aponta para a Razão de Consistência de 0,022, mantendo-se, portanto, abaixo de 10%, o que é favorável, conforme preconizado pelo autor do método.

O *Firewall* destaca-se como a alternativa mais importante para garantir a Integridade (0,491932), seguido pelo Controle de Acesso (0,221468), Treinamento (0,154900) e Antivírus (0,131700).

O método permitiu a análise estruturada da importância relativa de cada alternativa, facilitando a tomada de decisão em relação à Integridade. Partiremos para o último critério, Disponibilidade, conforme projetado nas Tabelas 16 a 20.

Tabela 16: alternativas em relação ao critério disponibilidade

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Firewall	1	2	7	8
Controle de Acesso	1/2	1	5	1/2
Treinamento	1/7	1/5	1	8
Antivírus	1/8	2	1/8	1

Fonte: Autores, 2024

Tabela 17: Soma das Colunas

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Soma	1,768	5,200	13,125	17,500

Fonte: Autores, 2024

Tabela 18: Normalização

Alternativa	*Firewall*	Controle de Acesso	Treinamento	Antivírus
Firewall	0,5656566	0,384615	0,533333	0,457143
Controle de Acesso	0,2828283	0,192308	0,380952	0,028571
Treinamento	0,0808081	0,038462	0,076190	0,457143
Antivírus	0,0707071	0,384615	0,009524	0,057143

Fonte: Autores, 2024

Tabela 19: Cálculo das Prioridades

Alternativa	Prioridade
Firewall	0,485187
Controle de Acesso	0,221165
Treinamento	0,163151
Antivírus	0,130497

Fonte: Autores, 2024

Tabela 20: Análise de Consistência

ƛmáx	3,989
R.I.	0,9
C.I.	0,004
C.R.	0,004

Fonte: Autores, 2024

As Tabelas 16 a 20 apresentam o processo de cálculo dos pesos das alternativas (*Firewall*, Controle de Acesso, Treinamento e Antivírus) em relação ao critério de Disponibilidade, utilizando o método AHP.

A Tabela 16: A matriz de comparação par a par, elaborada com base em julgamentos de especialistas, expressa a importância relativa de cada alternativa em relação às demais no que tange à Disponibilidade.

A Tabela 17: Contém a soma dos valores de cada coluna da matriz de comparação, etapa necessária para a normalização.

A Tabela 18: Exibe a matriz normalizada, obtida pela divisão de cada elemento da matriz original pela soma da sua coluna.

A Tabela 19: Finalmente, os pesos de cada alternativa são calculados pela média aritmética dos valores de cada linha da matriz normalizada.

A Tabela 20 aponta para uma Análise de Consistência adequada, ao passo que a Cálculo de Consistência aponta para a Razão de Consistência de 0,004, mantendo-se, portanto, abaixo de 10%, o que é favorável, conforme preconizado pelo autor do método.

O *Firewall* é a alternativa mais importante para garantir a Disponibilidade (0,485187), seguido pelo Controle de Acesso (0,221165), Treinamento (0,163151) e Antivírus (0,130497).

O método AHP permite a análise estruturada da importância relativa de cada alternativa, facilitando a tomada de decisão em relação à Disponibilidade.

e) Integração dos Pesos dos Critérios com as Prioridades das Alternativas

Integramos os pesos dos critérios com as prioridades das alternativas para obter uma pontuação global para cada alternativa, conforme Tabelas 21 e 22.

Tabela 21: Pesos dos critérios

Critério	Peso
Confidencialidade	0,633346
Integridade	0,260498
Disponibilidade	0,106156

Fonte: Autores, 2024

Tabela 22: Prioridades das Alternativas para Cada Critério

Critério	Alternativa	Prioridade
Confidencialidade	*Firewall*	0,443065229
	Controle de Acesso	0,28255244
	Treinamento	0,190340592
	Antivírus	0,084041739
Integridade	*Firewall*	0,491932283
	Controle de Acesso	0,221468447
	Treinamento	0,15489975
	Antivírus	0,13169952
Disponibilidade	*Firewall*	0,485187035
	Controle de Acesso	0,221164946
	Treinamento	0,163150738
	Antivírus	0,13049728

Fonte: Autores, 2024

f) Cálculo da Pontuação Global

Para calcular a pontuação global de cada alternativa, multiplicamos a prioridade de cada alternativa pelo peso do critério correspondente e somamos os resultados.

Tabela 23: Cálculo da Pontuação Global/*Ranking*

Alternativa	Confidencialidade	Integridade	Disponibilidade	*Ranking*
Firewall	0,443065229	0,491932283	0,485187035	0,4602665
Controle de Acesso	0,28255244	0,221468447	0,221164946	0,2601235
Treinamento	0,190340592	0,15489975	0,163150738	0,178222
Antivírus	0,084041739	0,13169952	0,13049728	0,101388

Fonte: Autores, 2024

Após calcular os pesos dos critérios (Confidencialidade, Integridade e Disponibilidade) e os de cada alternativa (*Firewall*, Controle de Acesso, Treinamento e Antivírus) em relação a cada critério, integramos esses resultados para obter a pontuação global de cada alternativa. Essa pontuação representa a ponderação da importância de cada critério e a prioridade da

alternativa em relação a ele.

A Tabela 21: Apresenta os pesos dos critérios, calculados na Tabela 4.

A Tabela 22: Reúne as prioridades (pesos) de cada alternativa em relação a cada critério, também calculadas nas tabelas 8, 13 e 18.

A Tabela 23: Demonstra o cálculo da pontuação global de cada alternativa, estabelecendo o *Ranking* final. Para isso, multiplicamos a prioridade de cada alternativa em relação a um critério pelo peso desse critério, somando-se os resultados para todos os critérios:

- *Firewall* (0,4602665): Apresenta a maior pontuação global, sendo a alternativa mais importante para atender aos critérios de segurança da informação.
- Controle de acesso (0,2601235): É a segunda alternativa mais importante.
- Treinamento (0,178222) e Antivírus (0,101388): Apresentaram pontuações mais baixas, indicando menor importância em relação às demais alternativas.

Com base nesses resultados, o método AHP permitiu a tomada de decisão de forma estruturada e transparente, priorizando as alternativas mais relevantes para atender aos critérios de segurança da informação da Empresa citada.

5. Resultados

Os resultados da aplicação do modelo AHP indicaram que a alternativa "Implantação de *Firewall*" obteve a maior pontuação global (0,4602665), seguida por "Implantação de um Controle de Acesso" (0,2601235), "Treinamento de conscientização em segurança" (0,178222) e "Aquisição de um *software* antivírus" (0,101388). Vamos analisar esses resultados em detalhes, fundamentando a análise com referências reais.

5.1. Importância da Confidencialidade

A confidencialidade foi o critério mais importante, com um peso de 0,633346. Isso reflete a necessidade crítica de proteger informações sensíveis contra acessos não autorizados. Segundo Madzík e Falát (2022), a perda de confidencialidade pode resultar em danos

significativos à reputação e à confiança dos clientes. A alta prioridade dada ao "*Firewall*" (0,443065229) e ao "Controle de acesso" (0,28255244) é consistente com práticas recomendadas de segurança da informação, que enfatizam a importância de controlar quem pode acessar dados e proteger a rede contra invasões.

5.2. Integridade das Informações

A integridade, com um peso de 0,260498, destaca a necessidade de garantir que as informações sejam precisas e não adulteradas. A integridade é fundamental para a tomada de decisões baseada em dados confiáveis. A prioridade relativamente alta das alternativas do "*Firewall*" (0,491932283) e do "Controle de Acesso" (0,221468447) para este critério é justificada, pois ambos ajudam a prevenir alterações não autorizadas nos dados. Segundo Canco et al. (2021), a integridade é frequentemente comprometida por ataques cibernéticos que visam modificar dados, e medidas robustas de controle de acesso e *firewall* são essenciais para mitigar esses riscos.

5.3. Disponibilidade das Informações

A disponibilidade, com um peso de 0,106156, surge para garantir que as informações estejam acessíveis quando necessário. As prioridades (pesos) "*Firewall*" (0,485187035) e do "Controle de Acesso" (0,221164946), para este critério, refletem a necessidade de manter os sistemas operacionais e minimizar o tempo de inatividade. A disponibilidade é frequentemente ameaçada por ataques de negação de serviço (DoS), e a implementação de *firewalls* e sistemas de controle de acesso podem ajudar a proteger contra esses ataques.

5.4. Análise das Alternativas

a) Implementação de um *Firewall*

- **Pontuação Global**: 0,4602665
- **Justificativa**: *Firewalls* são fundamentais para proteger a rede contra acessos não autorizados e ataques cibernéticos. Eles ajudam manter a integridade e a disponibilidade dos sistemas, bloqueando tráfego malicioso e prevenindo

ataques. Estudos indicam que a implementação de *firewalls* é uma das primeiras linhas de defesa contra ameaças externas.

b) Implantação de um Controle de Acesso

- **Pontuação Global**: 0,2601235
- **Justificativa**: Maior pontuação. Sistemas de controle de acesso são essenciais para garantir que apenas usuários autorizados possam acessar informações sensíveis, mantendo a confidencialidade e a integridade dos dados. Segundo Opoku et al. (2021), a implementação de sistemas de controle de acesso é uma prática recomendada para melhorar a segurança da informação em ambientes corporativos.

c) Treinamento de Conscientização em Segurança

- **Pontuação Global**: 0,178222
- **Justificativa**: Embora tenha uma pontuação menor, o treinamento de conscientização é essencial para educar os funcionários sobre as melhores práticas de segurança. Funcionários bem treinados são a primeira linha de defesa contra-ataques de engenharia social e outras ameaças internas. Segundo pesquisas, a conscientização em segurança pode reduzir significativamente o risco de violações de dados causadas por erro humano.

d) Aquisição de um *Software* Antivírus

- **Pontuação Global**: 0,101388
- **Justificativa**: *Software* antivírus é importante para proteger os computadores contra *malware*. No entanto, sua prioridade é menor em comparação com outras medidas, pois ele atua mais como uma camada adicional de defesa. Estudos mostram que, embora o *software* antivírus seja essencial, ele deve ser complementado por outras medidas de segurança para ser eficaz.

6. Discussões e considerações finais

Os resultados do AHP fornecem uma base sólida para a tomada de decisões sobre quais medidas de segurança implementar primeiro. A empresa deve priorizar a implantação de um sistema de controle de acesso e a implementação de um *firewall*, pois essas medidas oferecem o maior impacto na proteção das informações confidenciais, integridade e disponibilidade. A análise corrobora a importância de uma abordagem multifacetada para a segurança da informação, combinando tecnologia, processos e educação dos funcionários para criar um ambiente seguro e resiliente.

A literatura existente apoia a abordagem adotada pela empresa. Por exemplo, Madzík e Falát (2022) destacam a importância de uma abordagem sistemática e baseada em critérios para a tomada de decisões em segurança da informação. Além disso, Canco et al. (2021) enfatizam a necessidade de integrar várias camadas de segurança para proteger contra diferentes tipos de ameaças. Opoku et al. (2021) também sugerem que a implementação de sistemas de controle de acesso e *firewalls* é essencial para manter a segurança da informação em ambientes corporativos.

A aplicação do método AHP permitiu à empresa identificar e priorizar as medidas de segurança mais eficazes, alinhando-se com as melhores práticas e recomendações da literatura. A análise detalhada dos critérios e alternativas garantiu que a decisão fosse bem fundamentada e baseada em uma avaliação objetiva das necessidades de segurança da empresa.

Referências

CANCO, I.; KRUJA, D.; IANCU, T. AHP, a Reliable Method for Quality Decision Making: A Case Study in Business. Sustainability, v. 13, n. 24, p. 13932, 2021. https://doi.org/10.3390/su132413932.

GORDON, LAWRENCE A.; LOEB, MARTIN P. The Economics of Information Security Investment. ACM Transactions on Information and System Security, v. 5, n. 4, p. 438-457, 2002.

MADZÍK, P.; FALÁT, L. State-of-the-art on analytic hierarchy process in the last 40 years: Literature review based on Latent Dirichlet Allocation topic modelling. PLoS ONE, v. 17, n. 5, e0268777, 2022. https://doi.org/10.1371/journal.pone.0268777.

SAATY, Thomas L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill, 1980.

SCHIAVON, G. H. B. Estudo de caso fictício no curso de Direito. Revista de Pedagogía del Derecho, v. 16, n. 1, p. 181-203, 2019.

STAKE, R. E. The Art of Case Study Research. Thousand Oaks, CA: Sage, 1995.

WHITMAN, MICHAEL E.; MATTORD, HERBERT J. Principles of Information Security. 4th ed. Boston: Cengage Learning, 2011.

YIN, R. K. Case Study Research: Design and Methods. 5th ed. Thousand Oaks, CA: Sage, 2014.