**UNIVERSIDADE NOVE DE JULHO**

**UNINOVE**

**Projeto Solutions Tec**

**Planejamento em Informática**

**Turma: 40**

**Semestre: 2**

**Github:** **https://github.com/Wngt/Solutions-Tec**

## Brenda Silva Carvalho- 2223201034

## Breno Mykael Nascimento Dias- 2223202829

## Graciani Alves da Silva- 2223202642

## Gustavo Alves dos Santos- 2216203718

## Phelipe Gabriel Alves de Sa- 2223202383

## Wellington Silva Sousa - 2223204596

**São Paulo**

**2024**

**Índice**

1Escorpo ........................................................................................................... 2

1.1 Introdução ...................................................................................................2

1.2 Sore nós ........................................................................................................2

1.3 Visão Futura:............................................................................................... 2

2. Serviços oferecidos ....................................................................................... 3

2.1Catálogos de Produtos ............................................................................... .3

2.2 Experiência de Compra Online.................................................................... 3

2.3 Suporte ao Cliente ........................................................................................3

2.4 Entrega Rápida e Confiável......................................................................... 3

3.Estruturação Interna da Empresa ...............................................................4 3.1 Aprendizado de Máquina: Implementação de Modelos de Aprendizadode Máquina..........................................................................................................4

3.2 Ciência de Dados..........................................................................................5

3.2.1 Utilização de técnicas estatísticas básicas para descrever osdados ..................................................................................................................5

3.3 Aprendizado de Máquina: Implementação de Modelos de Aprendizadode Máquina .........................................................................................................8

3.1.2 Código utilizado .........................................................................................8

3.4 Redes de Computadores............................................................................ 10

3.4.1 Departamentos ........................................................................................10

3.4.1 Departamentos:........................................................................................12

3.4.2 Definir a classe de Rede:.........................................................................12

3.5 Segurança da Informação ........................................................................ 13

3.5.1 Identificação e avaliação dos riscos de segurança para a

empresa.............................................................................................................14

3.5.2 Análise de vulnerabilidades e ameaças potenciais: ................................14

3.5.3 Implementação de Medidas de Segurança: ...........................................16

3.5.4 Configuração de sistemas de detecção de intrusão e prevençãode ataques....................................................................................................... 17

1. **Escorpo do Projeto** 
   1. **Introdução:**

Bem-vindo à Solutions Tec, sua loja online de confiança para todas as suas necessidades de peças de informática. Estamos comprometidos em fornecer as melhores soluções para construir, atualizar e manter seu computador com produtos de alta qualidade e um serviço excepcional.

* 1. **Sobre Nós:**

Solutions Tec foi fundada por um grupo de entusiastas de tecnologia apaixonados por computadores e inovação. Nossa equipe possui anos de experiência no setor de tecnologia e está dedicada a ajudar nossos clientes a encontrar as peças certas para suas necessidades específicas.

* 1. **Visão Futura:**

Na Solutions Tec, estamos constantemente buscando maneiras de expandir e aprimorar nossos serviços. Estamos comprometidos em continuar oferecendo as melhores peças de informática e a melhor experiência de compra online para nossos clientes.

1. **Serviços Oferecidos** 
   1. **Catálogos de Produtos:**

Explore nosso extenso catálogo de peças de informática, incluindo processadores, placas-mãe, placas de vídeo, memórias RAM, unidades de armazenamento, gabinetes, fontes de alimentação e muito mais. Trabalhamos com marcas líderes do setor para garantir que você tenha acesso às últimas tecnologias e aos produtos mais confiáveis.

**2.2 Experiência de Compra Online:**

Nossa plataforma de e-commerce foi projetada para oferecer uma experiência de compra fácil e conveniente. Navegue pelo nosso site intuitivo, encontre os produtos que você precisa e conclua sua compra com segurança usando métodos de pagamento confiáveis.

**2.3 Suporte ao Cliente:**

Nosso compromisso com o atendimento ao cliente é inigualável. Nossa equipe de suporte está disponível para ajudá-lo com qualquer dúvida ou problema que você possa ter. Entre em contato conosco por meio de chat ao vivo, e-mail ou telefone e teremos o maior prazer em ajudá-lo.

**2.4 Entrega Rápida e Confiável:**

Entendemos que você deseja receber seus produtos o mais rápido possível. Por isso, trabalhamos com parceiros logísticos confiáveis para garantir entregas rápidas e seguras em todo o país. Acompanhe o status do seu pedido em tempo real e receba suas peças de informática com rapidez e eficiência.

**3. Estruturação Interna da Empresa**

**3.1 Aprendizado de Máquina: Implementação de Modelos de Aprendizado de Máquina**

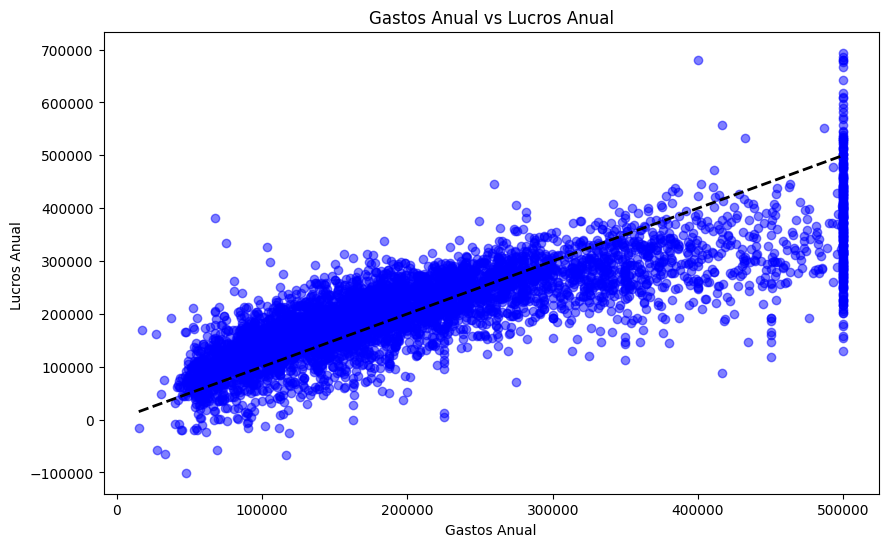
Algoritmo de Machine e Learn (ML) usado na empresa:

Regressão Linear (Modelo Supervisionado)

Regressão Linear:

Utilizando o modelo lógico de Regressão Linear formulado com margem de erro quase nulo, podemos afirmar que a empresa obteve uma margem de lucros significante maior que a margem de gastos no ano vigente. Considerando a compra de produtos para abastecimento do estoque, pagamento de funcionários,impostos e outros afins que são de total responsabilidade e confiabilidade cabíveis ao financeiro da empresa.

Valores abaixo na tabela a seguir:



Erro Médio Absoluto (MAE): 50966.660005188656

Erro Quadrático Médio (MSE): 4830762847.990561

Raiz do Erro Quadrático Médio (RMSE): 69503.68945596025

R-quadrado (R²): 0.6502334761951298

**3.2.1 Código utilizado abaixo:**

import pandas aspd

importmatplotlib.pyplotasplt

fromsklearn.model\_selectionimporttrain\_test\_split

fromsklearn.linear\_modelimportLinearRegression

fromsklearn.metricsimportmean\_absolute\_error, mean\_squared\_error, r2\_score

# Carregando o conjunto de dados

data = pd.read\_csv("sample\_data/california\_housing\_train.csv")

# Definindo as variáveis de entrada (features) e a variável de saída (target)

X = data.drop(columns=['median\_house\_value'])  # Features

y = data['median\_house\_value']  # Target

# Dividindo os dados em conjuntos de treinamento e validação (70% para treinamento, 30% para validação)

X\_train, X\_val, y\_train, y\_val = train\_test\_split(X, y, test\_size=0.3, random\_state=42)

# Criando uma instância do modelo de regressão linear

model = LinearRegression()

# Treinando o modelo com os dados de treinamento

model.fit(X\_train, y\_train)

# Fazendo previsões com os dados de validação

predictions = model.predict(X\_val)

# Calculando as métricas

mae = mean\_absolute\_error(y\_val, predictions)

mse = mean\_squared\_error(y\_val, predictions)

rmse = mean\_squared\_error(y\_val, predictions, squared=False)  # Calculando RMSE a partir do MSE

r2 = r2\_score(y\_val, predictions)

# Exibindo as métricas

print("Erro Médio Absoluto (MAE):", mae)

print("Erro Quadrático Médio (MSE):", mse)

print("Raiz do Erro Quadrático Médio (RMSE):", rmse)

print("R-quadrado (R²):", r2)

# Plotando as previsões em comparação com os valores reais

plt.figure(figsize=(10, 6))

plt.scatter(y\_val, predictions, color='blue', alpha=0.5)

plt.plot([y\_val.min(), y\_val.max()], [y\_val.min(), y\_val.max()], 'k--', lw=2)

plt.xlabel('Gastos Anual')

plt.ylabel('Lucros Anual ')

plt.title('Gastos Anual vs Lucros Anual')plt.show()

**3.2 Ciência de Dados**

**3.2.1 Utilização de técnicas estatísticas básicas para descrever os dados:**

import numpy as np

import pandas as pd

import statsmodels.api as sm

import matplotlib.pyplot as plt

#dados

idades\_novas = [20, 20, 24, 25, 30, 31, 33, 35]

salario\_novo = [1000, 1000, 1500, 2000, 3000, 3000, 2500, 4000]

#DataFrame

df\_novo = pd.DataFrame({'Idades': idades\_novas, 'Salario': salario\_novo})

#coluna de 1s para a constante do modelo

X\_novo = sm.add\_constant(df\_novo['Idades'])

modelo\_novo = sm.OLS(df\_novo['Salario'], X\_novo)

resultados\_novos = modelo\_novo.fit()

# Obtendo os coeficientes

coef\_constante\_novo, coef\_idades\_novo = resultados\_novos.params

# Plotando os novos dados e a nova linha de regressão

plt.scatter(df\_novo['Idades'], df\_novo['Salario'], label='Novos Dados')

plt.plot(df\_novo['Idades'], coef\_constante\_novo + coef\_idades\_novo \* df\_novo['Idades'], color='green', label='Nova Regressão Linear')

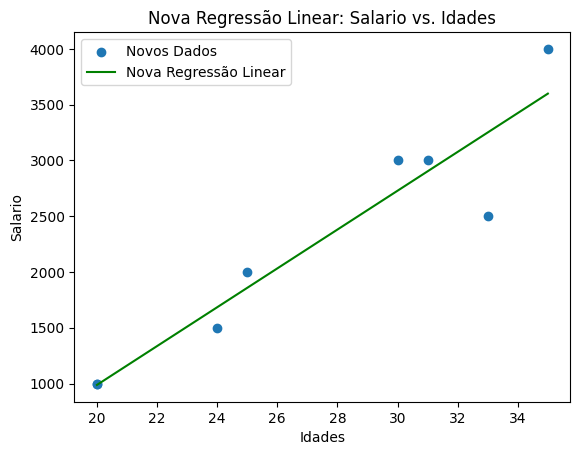
plt.xlabel('Idades')

plt.ylabel('Salario')

plt.title('Nova Regressão Linear: Salario vs. Idades')

plt.legend()

plt.show()

****

Previsão: [48.66666667]

from sklearn.linear\_model import LinearRegression

# Dados de exemplo

X = [[1.5], [2.0], [2.5]]  # Variável independente

y = [20,25,30]           # Variável dependente

# Criando o modelo de regressão linear

modelo = LinearRegression()

# Ajustando o modelo aos dados

modelo.fit(X, y)

# Fazendo previsões para novos dados

nova\_amostra = [[2.2]]

previsao = modelo.predict(nova\_amostra)

# Imprimindo a previsão

print("Previsão:", previsao)

Previsão: [48.66666667]

from sklearn.linear\_model import LinearRegression

from sklearn.metrics import mean\_squared\_error

# Dados de exemplo

X = [[1000], [2000], [3000]]

y = [20, 25, 30]

# Modelo de regressão linear

modelo = LinearRegression()

modelo.fit(X, y)

nova\_amostra = [[2.2]]

previsao = modelo.predict(nova\_amostra)

print("Previsão:", previsao)

R2 = modelo.score(X, y)

print(f'R-squared: {R2}')

y\_predito = modelo.predict(X)

erro\_medio\_quadratico = mean\_squared\_error(y, y\_predito)

print(f'Erro Médio Quadrático: {erro\_medio\_quadratico}')

resultado1 = 27

resultado2 = 29

if resultado1 > resultado2:

    print('Modelo 1 é melhor.')

else:

    print('Modelo 2 é melhor.')

Previsão: [15.011]

R-squared: 1.0

Erro Médio Quadrático: 0.0

Modelo 2 é melhor.

**3.3 Modelagem de Dados**

import pandas as pd

import seaborn as sns

import matplotlib.pyplot as plt

#idades e salários

idades = [20, 20, 24, 25, 30, 31, 33, 35]

salarios = [1000, 1000, 1500, 2000, 3000, 3000, 2500, 4000]

#DataFrame

dados = pd.DataFrame({

    'Idades': idades,

    'Salario': salarios

})

# Calcule as estatísticas descritivas

media = dados['Idades'].mean()

mediana = dados['Idades'].median()

desvio\_padrao = dados['Idades'].std()

# Imprima os resultados

print(f'Média: {media:.2f}, Mediana: {mediana:.2f}, Desvio Padrão: {desvio\_padrao:.2f}')

# Identificar padrões na coluna 'Idades'

print("Tendência nas Idades:")

print(dados['Idades'].value\_counts())

# padrões na coluna 'Salario'

print("\nTendência nos Salários:")

print(dados['Salario'].value\_counts())

# Gráfico de dispersão com Seaborn

sns.scatterplot(x='Idades', y='Salario', data=dados)

plt.xlabel('Idades')

plt.ylabel('Salário')

plt.title('Gráfico de Dispersão: Idades vs Salário')

plt.show()

Média: 27.25, Mediana: 27.50, Desvio Padrão: 5.80

Tendência nas Idades:

Idades

20 2

24 1

25 1

30 1

31 1

33 1

35 1

Name: count, dtype: int64

Tendência nos Salários:

Salario

1000 2

3000 2

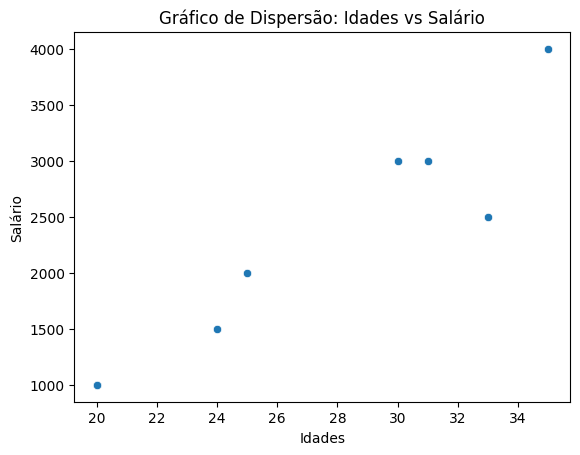
1500 1

2000 1

2500 1

4000 1

Name: count, dtype: int64



**3.4 Redes de Computadores**

**3.4.1 Departamentos:**

**Administração:**

Este departamento inclui a sala do CEO, salas de reunião executivas e outros espaços administrativos, para atividades relacionadas a administração da empresa.

**Rh:**

Este departamento lida com contratação, treinamento, folha de pagamento e outras questões relacionadas aos funcionários.

**Financeiro:**

Departamento financeiro cuida das finanças da empresa, incluindo contabilidade, planejamento financeiro e análise de custos.

**Departamento de Vendas e Marketing:**

Este departamento lida com as vendas e estratégias de marketing da empresa. Inclui salas de reunião para equipes de vendas, espaço para criação de campanhas de marketing.

**Departamento de Tecnologia da Informação (TI):**

Este departamento gerencia a infraestrutura de TI da empresa, incluindo redes, servidores, suporte técnico e segurança da informação.

**Equipamentos:**

**Administração e Recursos Humanos:**

* + Computadores desktop ou laptops;
  + Impressoras multifuncionais;
  + Telefones ou sistemas de telefonia;
  + Mobiliário de escritório;

**Finanças:**

* + Computadores desktop ou laptops com software financeiro;
  + Impressoras;
  + Calculadoras financeiras ou máquinas de calcular
  + Cofre para armazenamento;

**Vendas e Marketing:**

* + Computadores desktop ou laptops;
  + Telefones ou sistemas de telefonia;
  + Projetores ou telas;
  + Mobiliário para salas de reuniões;

**Tecnologia da Informação (TI):**

* + Servidores de rede para hospedar aplicativos e armazenar dados;
  + Computadores desktop ou laptops;
  + Equipamentos de rede, como roteadores, switches e firewalls;
  + Ferramentas de diagnóstico e manutenção de hardware e software;

**3.4.2 Definir a classe de Rede:**

* Classe de Rede: Classe C

**Definir o padrão de rede de cada departamento:**

**Administração e Recursos Humanos:**

* Faixa de endereços IP: 192.168.1.0 - 192.168.1.1

**Finanças:**

* Faixa de endereços IP: 192.168.2.0 - 192.168.2.1

**Vendas e Marketing:**

* Faixa de endereços IP: 192.168.3.0 - 192.168.3.1

**Tecnologia da Informação (TI):**

* Faixa de endereços IP: 192.168.4.0 - 192.168.4.1

**3.5 Segurança da Informação**

**3.5.1 Identificação e avaliação dos riscos de segurança para a empresa.**

20 possíveis ameaças e/ou vulnerabilidades:

1. Ataques de hackers: Invasores podem tentar acessar dados confidenciais dos clientes, como informações de pagamento e detalhes pessoais.

2. Phishing: E-mails fraudulentos podem ser enviados aos clientes, solicitando informações pessoais ou de pagamento, em nome da empresa.

3. Ataques de DDoS: Hackers podem lançar ataques de negação de serviço distribuído (DDoS) para derrubar o site da empresa, causando interrupções no serviço.

4. Vulnerabilidades de software: Falhas de segurança em plataformas de e-commerce, plugins ou sistemas operacionais podem ser exploradas por invasores.

5. Roubo de identidade: Dados pessoais dos clientes podem ser comprometidos, resultando em roubo de identidade e fraude.

6. Fraude de cartão de crédito: Transações fraudulentas podem ocorrer, causando prejuízos financeiros à empresa e aos clientes.

7. Vazamento de dados: Informações confidenciais dos clientes, como endereços de e-mail e números de telefone, podem ser expostas devido a brechas de segurança.

8. Falhas de autenticação: Senhas fracas ou métodos de autenticação inseguros podem facilitar o acesso não autorizado aos sistemas da empresa.

9. Ataques de engenharia social: Funcionários podem ser alvos de ataques de engenharia social, levando-os a revelar informações sensíveis ou conceder acesso indevido a sistemas.

10. Roubo de propriedade intelectual: Desenvolvedores de peças de computador podem ser alvo de roubo de propriedade intelectual, resultando na venda de produtos falsificados ou concorrência desleal.

11. Falhas de segurança de terceiros: Parceiros de negócios, como fornecedores de serviços de pagamento ou empresas de logística, podem enfrentar falhas de segurança que afetam indiretamente a empresa de e-commerce.

12. Ataques de injeção de SQL: Invasores podem explorar vulnerabilidades de segurança em bancos de dados para acessar ou manipular informações confidenciais.

13. Falta de atualizações de segurança: Não aplicar patches de segurança e atualizações de software pode deixar sistemas vulneráveis a ataques conhecidos.

14. Furto de mercadorias em trânsito: Produtos podem ser roubados durante o transporte, causando perdas financeiras para a empresa.

15. Violência física: Lojas físicas da empresa podem ser alvo de assaltos, representando um risco para funcionários e clientes.

16. Quebra de confiança do cliente: Incidentes de segurança podem minar a confiança dos clientes na empresa, levando a uma perda de vendas e reputação.

17. Riscos de conformidade: Não cumprir regulamentações de proteção de dados, como o GDPR (Regulamento Geral de Proteção de Dados) na União Europeia, pode resultar em multas e penalidades.

18. Ataques de ransomware: Sistemas da empresa podem ser infectados por ransomware, bloqueando o acesso aos dados até que um resgate seja pago.

19. Exposição de vulnerabilidades de infraestrutura: Configurações inadequadas de servidores e sistemas podem expor a empresa a ataques cibernéticos.

20. Falhas de backup e recuperação de dados: Se não forem implementadas estratégias eficazes de backup e recuperação de dados, a empresa pode enfrentar perda irreparável de informações importantes em caso de incidente de segurança.

**3.5.2 Análise de vulnerabilidades e ameaças potenciais:**

1. Ataques de hackers:
   * Impacto: Alto. Pode resultar em comprometimento de dados sensíveis dos clientes e danos à reputação da empresa.
   * Probabilidade: Moderada a alta. Com o aumento das ameaças cibernéticas, os ataques de hackers são uma preocupação constante para empresas de e-commerce.
2. Phishing:
   * Impacto: Moderado. Pode levar à divulgação de informações confidenciais dos clientes e danos à reputação da empresa.
   * Probabilidade: Moderada. Os ataques de phishing são comuns e podem ser direcionados a qualquer empresa com presença online.
3. Ataques de DDoS:
   * Impacto: Alto. Pode resultar na interrupção do serviço, causando perda de receita e danos à reputação.
   * Probabilidade: Moderada. Embora ataques DDoS sejam frequentes, sua probabilidade pode variar dependendo da visibilidade e importância percebida da empresa.
4. Vulnerabilidades de software:
   * Impacto: Variável. Depende da gravidade da vulnerabilidade e do potencial de exploração pelos invasores.
   * Probabilidade: Alta. Vulnerabilidades de software são descobertas regularmente, e os invasores estão constantemente procurando por elas.
5. Roubo de identidade:
   * Impacto: Alto. Pode resultar em danos financeiros e de reputação significativos para os clientes e para a empresa.
   * Probabilidade: Moderada a alta. O roubo de identidade é uma preocupação crescente devido à quantidade de informações pessoais disponíveis online.
6. Fraude de cartão de crédito:
   * Impacto: Alto. Pode causar prejuízos financeiros substanciais para a empresa e para os clientes afetados.
   * Probabilidade: Moderada. As transações fraudulentas são uma realidade comum no comércio eletrônico.
7. Vazamento de dados:
   * Impacto: Alto. Pode resultar em danos à reputação da empresa e em possíveis ações regulatórias e legais.
   * Probabilidade: Moderada a alta. Vazamentos de dados são cada vez mais comuns devido à sofisticação dos ataques cibernéticos.
8. Falhas de autenticação:
   * Impacto: Moderado a alto. Dependendo do nível de acesso comprometido, pode resultar em roubo de dados ou acesso não autorizado a sistemas críticos.
   * Probabilidade: Moderada. A segurança de autenticação é uma área comumente explorada por invasores.

**3.5.3 Implementação de Medidas de Segurança:**

Com base nos riscos identificados, é importante estabelecer políticas de controle de acesso sólidas para proteger os sistemas e dados da empresa de e-commerce. Aqui estão 10 políticas de controle de acesso que podem ajudar a mitigar os riscos:

1. Política de Senhas Fortes:

- Exigir senhas fortes com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

- Exigir a troca regular de senhas e proibir o uso de senhas antigas.

2. Política de Autenticação de Dois Fatores (2FA):

- Implementar a autenticação de dois fatores em todos os sistemas e aplicativos críticos.

- Exigir que os funcionários usem autenticação de dois fatores ao acessar sistemas remotos ou informações confidenciais.

3. Política de Controle de Acesso Baseado em Funções (RBAC):

- Atribuir privilégios de acesso com base nas funções e responsabilidades dos funcionários.

- Limitar o acesso apenas ao necessário para realizar as funções atribuídas.

4. Política de Monitoramento de Acesso:

- Implementar sistemas de monitoramento de acesso para rastrear e auditar atividades de usuários.

- Monitorar e revisar regularmente os registros de acesso para detectar atividades suspeitas.

5. Política de Gerenciamento de Identidades:

- Ter um processo formal para criar, modificar e encerrar contas de usuário.

- Revogar imediatamente o acesso de funcionários que deixam a empresa ou mudam de função.

6. Política de Acesso Baseada em Necessidade de Conhecimento (NOK):

- Limitar o acesso a informações confidenciais apenas aos funcionários que precisam delas para realizar suas funções.

- Implementar controles de acesso granulares para restringir o acesso a dados sensíveis.

7. Política de Criptografia de Dados:

- Criptografar dados confidenciais em repouso e em trânsito para protegê-los contra acesso não autorizado.

- Exigir que todos os dispositivos que acessam dados confidenciais usem comunicações criptografadas.

8. Política de Gerenciamento de Terceiros:

- Estabelecer requisitos de segurança para fornecedores e parceiros de negócios que acessam sistemas ou dados da empresa.

- Realizar avaliações regulares de segurança de terceiros e monitorar seu cumprimento com os padrões estabelecidos.

9. Política de Bloqueio de Conta Após Tentativas de Acesso Malsucedidas:

- Bloquear temporariamente contas de usuário após um número especificado de tentativas de login malsucedidas.

- Notificar os administradores de sistema sobre tentativas de login suspeitas.

10. Política de Treinamento de Conscientização em Segurança:

- Realizar treinamentos regulares de conscientização em segurança para funcionários, destacando práticas recomendadas de segurança cibernética.

- Educar os funcionários sobre os riscos de segurança, como phishing e engenharia social, e como identificar e relatar atividades suspeitas.

Essas políticas de controle de acesso ajudarão a fortalecer a postura de segurança da empresa de e-commerce e a reduzir os riscos de acesso não autorizado aos sistemas e dados.

**3.5.4 Configuração de sistemas de detecção de intrusão e prevenção de ataques:**

1. Firewalls de Próxima Geração:

- Instalar firewalls de próxima geração para filtrar o tráfego de rede e bloquear ameaças conhecidas e desconhecidas.

- Configurar regras de firewall para permitir apenas o tráfego necessário para os serviços autorizados.

2. Sistemas de Detecção de Intrusões (IDS):

- Implementar sistemas de detecção de intrusões para monitorar o tráfego de rede em busca de padrões e atividades suspeitas.

- Configurar alertas para notificar os administradores sobre possíveis intrusões ou tentativas de exploração.

3. Sistemas de Prevenção de Intrusões (IPS):

- Complementar os IDS com sistemas de prevenção de intrusões para bloquear automaticamente ameaças identificadas.

- Configurar as políticas de IPS para responder a ameaças específicas com ações apropriadas, como bloqueio de tráfego ou notificação de alerta.

4. Monitoramento de Log de Segurança:

- Implementar soluções de monitoramento de log de segurança para coletar e analisar registros de eventos de sistemas e aplicativos.

- Configurar alertas para detectar padrões incomuns de atividade que possam indicar tentativas de intrusão.

5. Análise de Comportamento de Usuário (UBA):

- Utilizar soluções de análise de comportamento de usuário para identificar atividades anômalas de usuários internos.

- Monitorar padrões de acesso e comportamento para detectar atividades suspeitas, como tentativas de acesso não autorizado ou roubo de credenciais.

6. Atualizações e Patches de Segurança:

- Manter todos os sistemas e aplicativos atualizados com as últimas correções de segurança e patches.

- Implementar um processo de gerenciamento de patches para garantir que as atualizações sejam aplicadas regularmente e de forma oportuna.

7. Filtragem de Conteúdo da Web:

- Implementar sistemas de filtragem de conteúdo da web para bloquear o acesso a sites maliciosos conhecidos e categorias de conteúdo perigoso.

- Configurar políticas de filtragem para impedir o download de arquivos executáveis suspeitos e conteúdo potencialmente malicioso.

8. Autenticação Multifatorial (MFA):

- Implementar a autenticação multifatorial em todos os sistemas e aplicativos para impedir o acesso não autorizado, mesmo em caso de roubo de credenciais.

- Exigir autenticação adicional, como códigos de verificação enviados por SMS ou aplicativos de autenticação, além de senhas.

9. Monitoramento de Endpoint:

- Utilizar soluções de monitoramento de endpoint para proteger dispositivos de usuários finais contra malware e atividades maliciosas.

- Configurar alertas para detectar atividades suspeitas nos endpoints, como alterações não autorizadas no sistema ou tentativas de execução de malware.

10. Treinamento de Conscientização em Segurança:

- Realizar treinamentos regulares de conscientização em segurança para todos os funcionários, destacando práticas recomendadas de segurança cibernética.

- Educar os funcionários sobre como reconhecer e relatar atividades suspeitas, como phishing e tentativas de engenharia social.

A implementação dessas medidas ajudará a fortalecer as defesas da empresa de e-commerce contra ameaças cibernéticas e a proteger os dados e sistemas críticos contra intrusões.