# Proposta de Arquitetura de Defesa e Plano de Monitoramento/IR – Loja Zeta

**Cliente:** LojaZeta
**Consultor:** Adriel Shimaski Alves da Cruz
Data: 22/09/2025
Versao: 1.0

# Sumário Executivo

A Loja Zeta, enquanto operação de e-commerce, enfrenta riscos relevantes como ataques de injeção SQL, tentativas de força bruta contra autenticação, indisponibilidade por sobrecarga e exploração de vulnerabilidades não corrigidas.

A arquitetura de defesa proposta adota o princípio de **defesa em profundidade**, criando múltiplas barreiras de proteção, visibilidade e resposta.

### Proteção perimetral e disponibilidade

uso de WAF/CRS integrado ao balanceador de carga para filtrar tráfego malicioso antes de chegar à aplicação.

### Aplicação resiliente e escalável

instâncias Node.js distribuídas e atualizadas com patching contínuo.

### Banco de dados protegido

PostgreSQL com criptografia em repouso, segregação de privilégios e monitoramento de consultas suspeitas.

### Identidade centralizada

camada de autenticação e autorização (IAM/Auth) com políticas fortes de senhas e MFA.

### Monitoramento e correlação

SIEM recebendo logs da aplicação, banco e identidade, com alertas em tempo real e métricas como MTTD e MTTR.

### Resposta estruturada a incidentes

plano baseado no ciclo NIST IR (Detecção → Contenção → Erradicação → Recuperação → Lições).

Com essa abordagem, a Loja Zeta alcançará:

- Redução do tempo de detecção e resposta a ataques.
- Maior disponibilidade da aplicação e experiência confiável para o cliente.
- Conformidade com boas práticas de segurança aplicáveis ao setor de e-commerce.
- Base sólida para futuras integrações em nuvem e expansão de mercado.

# Objetivo e Escopo

## Objetivo

O objetivo desta proposta é fornecer à Loja Zeta uma arquitetura de defesa em profundidade que seja prática, escalável e aderente às necessidades de um e-commerce em crescimento. O foco principal é **proteger a aplicação web e os dados dos clientes**, aumentar a visibilidade sobre incidentes de segurança e garantir que a equipe, mesmo reduzida, consiga responder rapidamente a ataques e falhas.

## Escopo

O trabalho cobre as seguintes áreas:

1. **Arquitetura de Defesa em Camadas**
   - Proteção perimetral (WAF/CRS, firewall e segmentação de rede).
   - Segurança da aplicação Node.js e banco de dados PostgreSQL.
   - Controles de identidade e autenticação centralizada.
2. **Monitoramento e SIEM**
   - Centralização de logs (Nginx, aplicação, banco e sistema operacional).
   - Criação de alertas acionáveis para ataques comuns (SQLi, XSS, brute-force).
   - Métricas de eficácia: MTTD (tempo de detecção), MTTR (tempo de resposta), cobertura de logs.
1. **Resposta a Incidentes (NIST IR)**
   - Procedimentos de detecção, contenção, erradicação, recuperação e lições aprendidas.
   - Runbooks específicos para ataques já observados: SQLi, XSS, brute-force em /login e indisponibilidade da aplicação.
2. **Plano de Ação 80/20**
   - Quick wins de até 30 dias (impacto imediato).
   - Ações de médio prazo (90 dias).
   - Estratégia de longo prazo (180 dias) para consolidação da segurança.

### Fora do escopo

- Implementação de SOC 24/7 dedicado.
- Conformidade regulatória específica (ex.: PCI-DSS), embora a arquitetura facilite adequações futuras.
- Desenvolvimento de novas funcionalidades de aplicação.

# Metodologia

A elaboração desta proposta seguiu uma abordagem consultiva baseada em boas práticas de segurança da informação e nas necessidades específicas da Loja Zeta.

## Etapas da análise

01

### Levantamento de contexto

- Análise do briefing fornecido (stack tecnológica: Nginx, Node.js e PostgreSQL).
- Consideração do histórico de incidentes recentes: tentativas de SQLi, XSS e brute-force em /login.
- Identificação das restrições: equipe reduzida (2 devs e 1 ops) e orçamento limitado.

02

### Definição de prioridades (princípio 80/20)

- Foco inicial em medidas de maior impacto e menor complexidade.
- Priorização da proteção da aplicação e identidade, pontos mais críticos do e-commerce.

03

### Construção da arquitetura de defesa em camadas

- Organização em perímetro, rede, aplicação, dados e identidade.
- Integração de mecanismos de monitoramento e resposta a incidentes.

04

### Adesão a frameworks reconhecidos

- NIST Cybersecurity Framework para ciclo de vida de resposta a incidentes.
- Boas práticas de hardening em sistemas Linux, Node.js e PostgreSQL.

## Premissas consideradas

- O ambiente de produção está hospedado em nuvem (IaaS).
- A equipe técnica tem conhecimentos básicos de administração de sistemas e bancos de dados.
- O orçamento inicial será direcionado para soluções de código aberto ou baixo custo (ex.: WAF CRS, ferramentas de SIEM open source).
- O crescimento do e-commerce exigirá escalabilidade horizontal, logo a arquitetura deve suportar múltiplas instâncias de aplicação.

# Arquitetura de Defesa (Camadas)

A Loja Zeta adotará uma estratégia de **defesa em profundidade**, aplicando controles em múltiplos níveis para dificultar ataques, reduzir a superfície de exposição e aumentar a resiliência da infraestrutura.

## 1. Camada de Perímetro

- **Firewall de Aplicação Web (WAF/CRS)**: protege contra ataques de injeção (SQLi, XSS) e requisições maliciosas.
- **Firewall de Rede**: restrição de portas e protocolos, permitindo apenas o tráfego necessário (HTTP/HTTPS para aplicação, portas seguras para administração).
- **Balanceador de Carga**: distribui tráfego entre múltiplas instâncias da aplicação, garantindo disponibilidade e resiliência.

## 2. Camada de Rede

- **Segmentação de Rede**: separação entre ambiente de produção, banco de dados e rede de administração.
- **Isolamento de Rede para Visitantes/Wi-Fi**: visitantes ou dispositivos não corporativos não devem ter acesso à rede de produção.
- **Monitoramento de tráfego**: integração com IDS/IPS (quando possível) para detectar acessos anômalos.

## 3. Camada de Aplicação

- **Hardening da aplicação Node.js**: atualização contínua (patching) e uso de boas práticas de codificação segura.
- **Proteção contra brute-force**: limitação de tentativas de login e uso de MFA (autenticação multifator).
- **Proteção contra injeção**: validação de entrada e parametrização de queries.

## 4. Camada de Dados

- **Banco de Dados PostgreSQL**: acesso restrito apenas à aplicação.
- **Criptografia em repouso**: dados sensíveis armazenados de forma segura.
- **Backups regulares**: já existentes, mas com plano de testes de restauração documentado.

## 5. Camada de Identidade

- **Gerenciamento Centralizado de Identidade (IAM/Auth)**: autenticação e autorização centralizada.
- **Políticas de privilégios mínimos (PoLP)**: cada usuário ou serviço só acessa o necessário.
- **Auditoria de acessos**: registros de login, falhas e tentativas suspeitas coletados pelo SIEM.

# Benefícios da Arquitetura

### Redução da superfície de ataque

Menos portas e serviços expostos, diminuindo as oportunidades para invasores.

### Maior resiliência contra ataques web

Proteção específica contra SQLi, XSS e brute-force através de múltiplas camadas.

### Controle granular de identidades

Gestão centralizada de acessos com políticas de privilégios mínimos.

### Visibilidade ampliada

Centralização de logs e monitoramento para detecção proativa de ameaças.

### Preparação para crescimento

Escalabilidade sem perda de segurança, suportando expansão do negócio.

## 5. Benefícios da Implementação

- Redução do risco de incidentes cibernéticos e perdas financeiras.
- Maior confiança dos clientes e parceiros comerciais.
- Cumprimento de legislações de proteção de dados (LGPD).
- Ambiente de TI moderno, resiliente e escalável.

# Resposta a Incidentes (NIST IR)

A Loja Zeta adotará o framework do **NIST (National Institute of Standards and Technology)** para resposta a incidentes, garantindo uma abordagem estruturada e eficiente.

## Ciclo de Vida do Incidente (NIST IR)

### 1. Preparação

- **Equipe de Resposta:** Designação de responsáveis (Ops + Devs)
- **Documentação:** Runbooks detalhados para cada tipo de incidente
- **Ferramentas:** SIEM configurado, ferramentas de análise forense básicas
- **Comunicação:** Lista de contatos de emergência e procedimentos de escalação

### 2. Detecção e Análise

**Fontes de Detecção:**

- Alertas automáticos do SIEM
- Relatos de usuários
- Monitoramento proativo

**Análise Inicial:**

- Classificação da severidade (Crítico, Alto, Médio, Baixo)
- Identificação do escopo e impacto potencial

### 3. Contenção, Erradicação e Recuperação

**Contenção Imediata:**

- Isolamento de sistemas afetados
- Bloqueio de IPs maliciosos
- Revogação de credenciais comprometidas

**Erradicação:**

- Remoção de malware/código malicioso
- Aplicação de patches e correções

**Recuperação:**

- Restauração de sistemas a partir de backups
- Validação da integridade dos sistemas

### 4. Lições Aprendidas

- **Post-Mortem:** Análise detalhada do incidente
- **Documentação:** Atualização de runbooks e procedimentos
- **Melhorias:** Implementação de controles preventivos adicionais

# Runbooks Específicos

1

## SQL Injection

- **Detecção:** Alertas do WAF + queries suspeitas no PostgreSQL
- **Contenção:** Bloqueio imediato do IP no WAF
- **Erradicação:** Correção da vulnerabilidade na aplicação
- **Recuperação:** Restauração de dados se necessário
- **Tempo Esperado:** Contenção < 30 min, Correção < 4h

2

## Cross-Site Scripting (XSS)

- **Detecção:** Logs da aplicação + relatos de usuários
- **Contenção:** Remoção do conteúdo malicioso
- **Erradicação:** Implementação de sanitização de inputs
- **Recuperação:** Limpeza de caches e sessões afetadas
- **Tempo Esperado:** Contenção < 1h, Correção < 8h

3

## Brute-Force em Login

- **Detecção:** Múltiplas falhas de login do mesmo IP
- **Contenção:** Bloqueio temporário do IP + throttle de tentativas
- **Erradicação:** Revisão de políticas de senha + implementação de MFA
- **Recuperação:** Reset de senhas de contas potencialmente comprometidas
- **Tempo Esperado:** Contenção < 15 min, Correção < 2h

4

## Indisponibilidade da Aplicação

- **Detecção:** Monitoramento de saúde dos serviços
- **Contenção:** Failover para instância secundária
- **Erradicação:** Identificação e correção da causa raiz
- **Recuperação:** Restauração completa dos serviços
- **Tempo Esperado:** Contenção < 5 min, Recuperação < 1h

# Matriz de Severidade e Resposta

| Severidade | Impacto | Tempo de Resposta | Ações |
|---|---|---|---|
| **Crítico** | Sistema indisponível ou dados comprometidos | < 30 min | Mobilização total da equipe |
| **Alto** | Funcionalidade crítica afetada | < 2 horas | Envolvimento de especialistas |
| **Médio** | Impacto limitado | < 4 horas | Resolução durante horário comercial |
| **Baixo** | Impacto mínimo | < 8 horas | Resolução conforme disponibilidade |

# Comunicação Durante Incidentes

### Interna

Notificação imediata da equipe técnica e gestores

### Clientes

Comunicação transparente sobre afetações (se aplicável)

### Regulatórias

Notificação conforme exigências legais (LGPD)

# Recomendações (80/20) e Roadmap

Seguindo o princípio **80/20**, priorizamos ações que oferecem maior impacto com menor esforço, organizadas em ordem de criticidade e facilidade de implementação.

1

## Quick Wins (30 dias)

- Implementação de WAF/CRS básico
- Configuração de alertas críticos no SIEM
- Hardening básico da aplicação Node.js
- Políticas de senha mais rigorosas

2

## Médio Prazo (90 dias)

- Implementação completa do SIEM
- Segmentação de rede
- MFA para todos os acessos administrativos
- Runbooks detalhados e treinamento da equipe

3

## Longo Prazo (180 dias)

- Automação de resposta a incidentes
- Testes de penetração regulares
- Conformidade com frameworks de segurança
- Expansão para SOC dedicado

**Próximos Passos:** Após aprovação desta proposta, iniciaremos com a fase de Quick Wins, priorizando a proteção imediata da aplicação e a implementação dos controles de maior impacto.

# Conclusão e Próximos Passos

A arquitetura de defesa proposta para a Loja Zeta é um investimento estratégico crucial para o futuro da empresa. Ela não apenas fortalecerá sua postura de segurança contra ameaças cibernéticas em constante evolução, mas também garantirá a continuidade dos negócios, protegerá dados valiosos e solidificará a confiança de seus clientes e parceiros. Estamos confiantes de que esta abordagem proativa e em camadas proporcionará um ambiente digital resiliente e seguro.

## Próximos Passos

### Revisão e Aprovação

Análise final e aprovação da proposta pela liderança da Loja Zeta. (1 semana)

### Planejamento Detalhado

Elaboração de um plano de implementação detalhado e alocação de recursos específicos. (2 semanas)

### Início dos Quick Wins

Lançamento imediato da fase de Quick Wins para proteção prioritária. (Após planejamento)

### Monitoramento Contínuo

Estabelecimento de processos para monitoramento e otimização contínuos da segurança. (Em curso)

## Critérios de Sucesso e Resultados Mensuráveis

### Redução de Incidentes

Diminuição de **25%** no volume de incidentes de segurança detectados nos primeiros 6 meses após a implementação das fases iniciais.

### Tempo de Resposta

Melhoria de **50%** no Tempo Médio para Resposta (MTTR) a incidentes críticos, garantindo uma recuperação mais rápida.

### Conformidade Aprimorada

Alcance de **100%** de aderência às políticas de segurança internas e requisitos regulatórios relevantes.

### Conscientização da Equipe

Aumento de **70%** na participação e engajamento da equipe em treinamentos de segurança cibernética.

# Recomendações Finais

Para garantir o sucesso e a sustentabilidade desta iniciativa de segurança, recomendamos fortemente:

- Manter o **apoio e comprometimento contínuos da liderança**, essencial para o sucesso de qualquer programa de segurança.
- Investir na **capacitação e conscientização** de toda a equipe sobre as melhores práticas de segurança cibernética.
- Fomentar uma **cultura de segurança proativa**, onde todos os colaboradores se sintam responsáveis pela proteção dos ativos da empresa.

# Recomendações (80/20) e Roadmap

Seguindo o princípio **80/20**, priorizamos ações que oferecem maior impacto com menor esforço, organizadas em ordem de criticidade e facilidade de implementação. Este roadmap detalha a jornada da Loja Zeta em direção a um ambiente digital mais seguro.

## Plano de Ação Prioritário (80/20)

O plano a seguir lista as ações essenciais com base no princípio 80/20, focando em iniciativas de alto impacto com menor dificuldade de implementação.

| | | | | | |
|---|---|---|---|---|---|
| 1 | Configurar regras básicas no firewall | Alto | Baixa | 7 dias | Ops |
| 2 | Isolar rede de visitantes da produção | Alto | Média | 15 dias | Ops |
| 3 | Implementar backups automáticos criptografados | Alto | Média | 15 dias | Ops |
| 4 | Ativar MFA para acessos administrativos | Alto | Média | 15 dias | Ops/Devs |
| 5 | Implementar WAF/CRS no Nginx | Alto | Alta | 30 dias | Ops/Devs |
| 6 | Criar políticas de acesso Wi-Fi seguras | Médio | Alta | 30 dias | Ops |
| 7 | Revisar acessos administrativos (RBAC) | Médio | Alta | 45 dias | Ops |
| 8 | Implementar campanhas de awareness | Médio | Baixa | 60 dias | Todos |

# Roadmap Detalhado

O roadmap a seguir descreve a evolução da segurança da Loja Zeta em três fases distintas, com objetivos e entregáveis claros para cada período.

01

### Fase 1: Fundamentos (0-30 dias) - Quick Wins

**Objetivo:** Estabelecer proteções básicas e visibilidade mínima.

- **Semana 1-2:** Configuração de regras de firewall e isolamento da rede de visitantes.
- **Semana 3-4:** Ativação de MFA para contas administrativas e configuração inicial do WAF.
- **Entregáveis:** Firewall configurado, rede segmentada, backup automático funcionando, MFA ativo para admins.

02

### Fase 2: Fortalecimento (30-90 dias)

**Objetivo:** Expandir monitoramento e controles de segurança.

- **Mês 2:** Implementação de SIEM básico e configuração de alertas.
- **Mês 3:** Revisão de acessos administrativos (menor privilégio) e testes de restauração de backup.
- **Entregáveis:** SIEM operacional com alertas básicos, políticas de acesso revisadas, primeiro teste de restauração.

03

### Fase 3: Maturação (90-180 dias)

**Objetivo:** Consolidar programa de segurança e preparar para escala.

- **Mês 4-5:** Campanhas de conscientização em segurança e implementação de IDS/IPS básico.
- **Mês 6:** Simulação de incidente e auditoria de segurança interna.
- **Entregáveis:** Programa de awareness iniciado, IDS/IPS implementado, primeira simulação de incidente.

# Métricas de Sucesso por Fase

O sucesso da implementação será mensurado através de marcos e indicadores chave de performance para cada fase do roadmap.

### Fase 1 (30 dias)

- 100% dos sistemas com firewall configurado.
- Rede de visitantes isolada da produção.
- MFA implementado para contas críticas.
- Backups automáticos em execução.

### Fase 2 (90 dias)

- 80% dos logs centralizados no SIEM.
- Alertas configurados para ameaças críticas.
- Primeiro teste de restauração bem-sucedido.
- Políticas de acesso revisadas e documentadas.

### Fase 3 (180 dias)

- Redução de 50% em tentativas de acesso não autorizado.
- MTTD < 15 minutos para incidentes críticos.
- MTTR < 2 horas para incidentes comuns.
- Equipe treinada em procedimentos de IR.

# Dependências e Pré-requisitos

## Críticas

- Acesso administrativo total à infraestrutura existente.
- Aprovação de orçamento para aquisição de ferramentas essenciais.
- Comprometimento da equipe com os prazos estabelecidos para as tarefas.

## Importantes

- Documentação atualizada da infraestrutura de rede e sistemas.
- Backup atualizado e testado antes de qualquer mudança crítica no ambiente.
- Janela de manutenção acordada para implementações que possam afetar a operação.
  Riscos, Custos e Assunções

# Riscos Identificados

A implementação de qualquer projeto de segurança cibernética envolve riscos inerentes. A seguir, detalhamos os riscos mais relevantes, suas mitigações e a probabilidade de ocorrência, classificando-os em categorias técnicas e operacionais.

1

## Riscos Técnicos: Configuração Incorreta do WAF

- **Impacto:** Bloqueio de tráfego legítimo ou falha na proteção essencial, afetando a disponibilidade e segurança.
- **Mitigação:** Realizar testes exaustivos em ambiente de homologação antes de qualquer implantação em produção.
- **Probabilidade:** Média

2

## Riscos Técnicos: Falha na Restauração de Backup

- **Impacto:** Indisponibilidade prolongada e perda de dados em caso de incidente crítico, comprometendo a continuidade do negócio.
- **Mitigação:** Implementar e testar regularmente os procedimentos de restauração de backup para garantir sua eficácia.
- **Probabilidade:** Baixa

3

## Riscos Técnicos: Resistência à Adoção de MFA

- **Impacto:** Segurança comprometida em acessos administrativos críticos, aumentando a superfície de ataque.
- **Mitigação:** Promover treinamento contínuo e comunicação clara dos benefícios da Autenticação Multifator para todos os usuários.
- **Probabilidade:** Média

4

## Riscos Operacionais: Falta de Recursos Humanos Especializados

- **Impacto:** Atraso na implementação de medidas de segurança ou configuração inadequada das ferramentas.
- **Mitigação:** Avaliar a necessidade de consultoria externa pontual ou investir em treinamento intensivo da equipe interna.
- **Probabilidade:** Alta

5

## Riscos Operacionais: Indisponibilidade Não Planejada

- **Impacto:** Interrupção das vendas online e potencial dano à reputação da Loja Zeta.
- **Mitigação:** Planejar janelas de manutenção com antecedência, comunicar proativamente e ter um plano de rollback eficiente.
- **Probabilidade:** Baixa

Para garantir a transparência e a sustentabilidade do projeto, é fundamental compreender os riscos potenciais, as estimativas de custos envolvidas e as premissas sobre as quais esta proposta se baseia. Esta seção detalha esses aspectos, fornecendo uma visão completa para o planejamento e a tomada de decisão.

# Estimativa de Custos

A alocação de recursos financeiros é vital para a implementação bem-sucedida das recomendações. Apresentamos uma estimativa de custos dividida entre despesas iniciais e recorrentes, além de uma comparação entre custos de prevenção e correção de incidentes.

## Custos Iniciais (Primeiros 90 dias)

| Item | Tipo | Custo Estimado | Periodicidade |
|---|---|---|---|
| Ferramentas Open Source | Licença | R$ 0 | - |
| Consultoria Especializada | Serviço | R$ 5.000 - R$ 10.000 | Pontual |
| Treinamento da Equipe | Capacitação | R$ 2.000 - R$ 4.000 | Inicial |
| Hardware/Cloud Adicional | Infraestrutura | R$ 500 - R$ 1.000/mês | Mensal |
| **Total Estimado Fase 1** | | **R$ 7.500 - R$ 15.000** | - |

## Custos Recorrentes (Após 90 dias)

| Item | Custo Mensal | Custo Anual |
|---|---|---|
| Manutenção SIEM | R$ 300 - R$ 600 | R$ 3.600 - R$ 7.200 |
| Monitoramento Cloud | R$ 200 - R$ 400 | R$ 2.400 - R$ 4.800 |
| Backup e Storage | R$ 150 - R$ 300 | R$ 1.800 - R$ 3.600 |
| **Total Recorrente** | **R$ 650 - R$ 1.300/mês** | **R$ 7.800 - R$ 15.600/ano** |

## Custos de Incidente (Prevenção vs. Correção)

Investir em prevenção é sempre mais econômico do que remediar as consequências de um incidente de segurança. A tabela a seguir ilustra essa diferença de custos.

| Cenário | Custo de Prevenção | Custo de Correção |
|---|---|---|
| Vazamento de Dados | R$ 10.000 (implementação) | R$ 50.000 - R$ 200.000 (multas, perda de reputação) |
| Ransomware | R$ 5.000 (backup, proteção endpoint) | R$ 100.000+ (resgate, tempo de inatividade) |
| Indisponibilidade | R$ 3.000 (alta disponibilidade) | R$ 10.000 - R$ 50.000/dia (vendas perdidas) |

# Assunções do Projeto

Esta proposta foi desenvolvida com base em certas premissas. A validação contínua dessas assunções é crucial para o sucesso do projeto e para evitar desvios no planejamento.

## Assunções Técnicas

- **Infraestrutura Existente:** A infraestrutura atual da Loja Zeta possui a capacidade e configuração necessárias para suportar a implementação das soluções de segurança propostas sem grandes reformas.
- **Compatibilidade:** As ferramentas open source e as novas configurações serão compatíveis com o stack tecnológico atual da empresa, não gerando conflitos significativos com sistemas existentes.

## Assunções Operacionais

- **Recursos Humanos:** A equipe de TI atual da Loja Zeta terá disponibilidade e capacidade para absorver novas responsabilidades relacionadas à segurança e participar ativamente dos treinamentos e da implementação.
- **Acesso e Permissões:** Será concedido o acesso administrativo e as permissões necessárias para a equipe responsável pela implementação e configuração das soluções de segurança, sem restrições burocráticas significativas.

## Assunções de Negócio

- **Orçamento:** O budget estimado para o projeto será aprovado e disponibilizado conforme o cronograma, e não haverá cortes significativos durante as fases de implementação.
- **Priorização:** A segurança cibernética será tratada como uma prioridade estratégica pela alta direção da Loja Zeta, garantindo o apoio necessário e a concessão de janelas de manutenção.

# Planos de Contingência

Para cada risco identificado, existem planos de contingência para minimizar seu impacto e garantir a continuidade das operações. Estar preparado para o inesperado é um pilar fundamental da segurança cibernética.

## Para Riscos Técnicos

- **Backup de Configurações:** Todas as alterações críticas serão precedidas por backups de configurações e documentação detalhada do plano de rollback.
- **Ambiente de Testes:** A implementação de novas ferramentas ou configurações será sempre realizada primeiro em ambiente de homologação, replicando o cenário de produção.
- **Monitoramento Intensivo:** Após cada mudança crítica, haverá um período de monitoramento intensivo para detectar anomalias rapidamente.

## Para Riscos Operacionais

- **Plano de Transição:** Treinamento gradual e documentação detalhada para a equipe interna, facilitando a absorção de novas responsabilidades.
- **Suporte Externo:** Manter contato com consultorias especializadas para suporte pontual em implementações complexas ou em momentos de pico de demanda.
- **Comunicação Clara:** Alinhamento constante com todos os stakeholders sobre o progresso do projeto e quaisquer desafios que possam surgir.

## Para Riscos de Budget

- **Faseamento:** O projeto foi concebido em fases, permitindo distribuir os custos ao longo do tempo e reavaliar o orçamento em cada etapa.
- **Alternativas Open Source:** Sempre que viável, serão priorizadas soluções de código aberto para reduzir custos de licenciamento sem comprometer a segurança.
- **ROI Claro:** Demonstração contínua do valor e retorno sobre o investimento (ROI) das iniciativas de segurança através de métricas de redução de risco e conformidade.

# Conclusão e Próximos Passos

A proposta apresentada oferece à Loja Zeta uma base sólida para a construção de um programa de segurança cibernética eficaz e sustentável. Com a abordagem de **defesa em profundidade**, **monitoramento centralizado** e **resposta estruturada a incidentes**, a empresa estará significativamente mais preparada para enfrentar os desafios de segurança no ambiente de e-commerce.

## Principais Benefícios Esperados

**70-80%**

### Ataques Reduzidos

Redução nas tentativas de ataques bem-sucedidos nos primeiros 90 dias.

**< 15min**

### MTTD

Tempo Médio para Detecção de incidentes críticos.

**< 2h**

### MTTR

Tempo Médio para Resposta em cenários críticos.

- Conformidade com boas práticas de segurança e requisitos regulatórios básicos.
- Preservação da reputação e confiança dos clientes.

A estratégia **80/20**roadmap

---

## Próximos Passos Imediatos (Semana 1)

01

### Reunião de Alinhamento Final

Data Sugerida: Próximos 2 dias úteis. Participantes: Diretoria, TI, Segurança. Objetivo: Aprovação formal da proposta e liberação de recursos.

02

### Kick-off do Projeto

Data: Imediatamente após aprovação. Entregável: Cronograma detalhado com marcos e responsáveis. Ações: Designação formal da equipe de projeto.

03

### Implementação das Ações Críticas

Prioridade 1: Configuração de firewall (Dias 1-7). Prioridade 2: Isolamento de rede (Dias 8-15). Prioridade 3: Backups automatizados (Dias 8-15).

---

# Critérios de Sucesso Mensuráveis

## 30 Dias (Fase 1)

- Firewall configurado e testado.
- Rede de visitantes isolada.
- MFA ativo para contas administrativas.
- Backups automáticos em execução.

## 90 Dias (Fase 2)

- SIEM operacional com >80% de cobertura de logs.
- Alertas configurados para ameaças críticas.
- Primeiro teste de restauração bem-sucedido.
- Políticas de acesso revisadas e documentadas.

## 180 Dias (Fase 3)

- MTTD < 15min para incidentes críticos.
- MTTR < 2h para incidentes comuns.
- Equipe treinada em procedimentos de IR.
- Primeira simulação de incidente realizada.

---

# Recomendações Finais

### Comprometimento da Alta Direção

A segurança deve ser tratada como prioridade estratégica, com alocação adequada de recursos humanos e financeiros.

### Cultura de Segurança

Envolvimento de todas as áreas da empresa através de treinamentos regulares e conscientização contínua.

### Melhoria Contínua

Revisão periódica do programa de segurança e ajustes baseados em métricas e lições aprendidas.

### Preparação para Crescimento

Arquitetura escalável para suportar expansão e planejamento para futuras integrações em nuvem.

---

# Contato e Acompanhamento

- **Próxima Revisão Formal:** 30 dias após implementação inicial.
- **Métricas de Acompanhamento:** Relatório quinzenal de progresso.
- **Canal de Comunicação:** Reuniões semanais de alinhamento.

Ponto Focal: **Adriel Shimaski**

---

# Checklist de Início Rápido

## Antes de Começar

- Obter aprovação formal da diretoria.
- Designar equipe do projeto.
- Estabelecer canal de comunicação.
- Definir reuniões de acompanhamento.

## Primeira Semana

- Configurar acesso às ferramentas.
- Iniciar configuração do firewall.
- Agendar treinamentos da equipe.
- Documentar procedimentos básicos.

## Primeiro Mês

- Completar implementação da Fase 1.
- Realizar primeiro teste de backup.
- Configurar alertas básicos.
- Documentar lições aprendidas.

# Plano de Implementação Faseado

A implementação da arquitetura de defesa e do plano de monitoramento/IR será realizada em fases bem definidas, garantindo uma abordagem estruturada e progressiva. Este roteiro de três fases permite à Loja Zeta construir uma base de segurança robusta e evoluir para um estado de otimização contínua, minimizando interrupções e maximizando a eficácia das medidas de segurança.

## Fase 1: Fundamentos (Dias 1-30)

Nesta fase inicial, o foco está em estabelecer os pilares essenciais da segurança, configurando a infraestrutura de rede e aplicando proteções básicas imediatas para mitigar os riscos mais críticos.

Configuração de Rede

- Segmentação de VLANs para isolamento lógico de sistemas críticos e dados sensíveis.
- Configuração de firewall com regras de segurança rígidas e controle de acesso baseado em políticas.
- Isolamento de redes para ambientes específicos (e.g., administrativa, PCI-DSS, visitantes) para reduzir a superfície de ataque.

Proteção Básica

- Implementação de WAF (Web Application Firewall) com regras OWASP CRS para proteger contra vulnerabilidades web comuns.
- Configuração de rate limiting em endpoints críticos (e.g., login, API) para prevenir ataques de força bruta e DDoS.
- Estabelecimento de rotinas de backup e recovery básico para dados essenciais, garantindo a resiliência operacional.

## Fase 2: Monitoramento (Dias 31-90)

Com a fundação estabelecida, esta fase concentra-se na visibilidade e na capacidade de detecção de ameaças, preparando a organização para uma resposta proativa a incidentes.

Implementação do SIEM

- Coleta de logs centralizada de todos os sistemas e aplicações relevantes para análise unificada.
- Configuração de alertas e correlações para identificar padrões de atividades suspeitas e violações de políticas.
- Criação de dashboards de monitoramento para uma visão em tempo real da postura de segurança.

Automação

- Desenvolvimento de scripts de resposta a incidentes para automatizar ações em caso de detecção.
- Automação de backups regulares e testes de restauração para garantir a integridade dos dados.
- Implementação de monitoramento contínuo para garantir a conformidade e identificar desvios na configuração.

## Fase 3: Otimização (Dias 91-180)

A fase final visa refinar a arquitetura, otimizar o desempenho e fortalecer as defesas com medidas avançadas, garantindo uma segurança escalável e duradoura.

Melhorias de Performance

- Otimização de queries de banco de dados para melhorar a velocidade e eficiência das aplicações.
- Estratégias de cache para reduzir a latência e a carga sobre os servidores.
- Implementação de balanceamento de carga avançado para distribuir o tráfego e garantir alta disponibilidade.

Segurança Avançada

- Realização de pentesting interno para identificar vulnerabilidades antes de serem exploradas por atacantes.
- Análise de vulnerabilidades contínua para manter a infraestrutura protegida contra novas ameaças.
- Desenvolvimento de um Plano de Continuidade de Negócios (PCN) e Recuperação de Desastres (DR) para cenários de grande impacto.

# Critérios de Aceitação

A validação do sucesso da implementação será medida por critérios objetivos, focando tanto na eficácia da segurança quanto na manutenção do desempenho das operações.

## Testes de Segurança

A robustez das defesas será verificada através de testes rigorosos e cenários de ataque simulados.

- WAF bloqueia com sucesso payloads de SQL Injection e Cross-Site Scripting (XSS) em testes.
- Rate limiting é efetivo em endpoints críticos, prevenindo tentativas de login fraudulentas.
- Backups são restaurados com sucesso em ambiente de teste, validando a integridade dos dados.
- Alertas são gerados para atividades suspeitas, demonstrando a eficácia do SIEM.

## Métricas de Performance

O desempenho da Loja Zeta não será comprometido, com metas claras para disponibilidade e tempo de resposta.

- **Disponibilidade (Uptime):** Garantia de 99.9% de disponibilidade da plataforma.
- **Tempo de Resposta:** Menos de 200ms para 95% das requisições, assegurando uma experiência fluida ao usuário.
- **MTTD (Mean Time To Detect):** Tempo médio para detecção de incidentes críticos inferior a 15 minutos.
- **MTTR (Mean Time To Respond):** Tempo médio para resposta a incidentes críticos inferior a 2 horas.

# Manutenção e Suporte Contínuo

Para garantir a eficácia a longo prazo da arquitetura de defesa, um plano robusto de manutenção e suporte será implementado, assegurando a vigilância constante e a atualização das defesas.

## Atividades Regulares

A segurança é um processo contínuo que exige atenção diária, semanal e mensal para se adaptar às novas ameaças.

Diárias

- Verificação de logs de segurança e alertas gerados pelo SIEM.
- Monitoramento de performance dos sistemas e aplicações.
- Verificação da execução bem-sucedida dos backups.

Semanais

- Análise de vulnerabilidades nos sistemas e aplicações.
- Realização de testes de restauração de backups em ambiente controlado.
- Revisão de políticas de segurança e regras do firewall/WAF.

Mensais

- Atualização de regras do WAF e assinaturas de segurança.
- Análise detalhada de métricas de segurança e relatórios de incidentes.
- Treinamento da equipe em novos procedimentos e ameaças emergentes.

## Estrutura de Suporte

Um sistema de suporte e escalonamento claro garantirá que quaisquer problemas sejam resolvidos de forma eficiente e rápida, minimizando o impacto nas operações.

- **Horário Comercial (08:00-18:00):** Suporte prioritário para todas as questões, com canais de comunicação dedicados.
- **Fora do Horário (After Hours):** Suporte para emergências críticas apenas, com equipe de plantão designada.
- **Processo de Escalação:** Uma hierarquia clara de escalonamento (Nível 1 → Nível 2 → Especialista) para garantir que os incidentes sejam direcionados à equipe apropriada com a ur

# Plano de Ação

Este plano detalha as etapas e recursos necessários para a implementação da arquitetura de defesa e do monitoramento de segurança na Loja Zeta, dividido em fases incrementais para garantir uma transição suave e eficaz.

### Visão Geral do Projeto

O projeto será executado em um período de seis meses, dividido em três fases distintas, com uma equipe dedicada e um orçamento inicial focado na construção da base de segurança.

- **Duração Total:** 180 dias (6 meses)
- **Fases:** 3 (Fundamentos, Monitoramento, Otimização)
- **Equipe:** 2 Devs + 1 Ops + Consultor externo
- **Orçamento Inicial:** R$ 15.000
- **Orçamento Recorrente:** R$ 1.300/mês

---

# Fase 1: Fundamentos (Dias 1-30)

Esta fase inicial estabelece a base de segurança, configurando os elementos essenciais de rede e proteção perimetral para criar um ambiente mais robusto.

## Semana 1: Preparação e Planejamento

**Objetivo:** Estabelecer a base do projeto, garantir acessos e definir as métricas de sucesso para o monitoramento.

| Data | Atividade | Responsável | Status | Entregável |
|---|---|---|---|---|
| Dia 1-2 | Kick-off do projeto | Gerente | [ ] | Ata de kick-off |
| Dia 3-4 | Análise ambiente atual | Ops | [ ] | Relatório de baseline |
| Dia 5 | Definição de métricas | Todos | [ ] | KPIs documentados |

**Checklist Semana 1:**

- Ambiente de desenvolvimento configurado
- Acesso a todos os sistemas concedido
- Documentação atualizada
- Cronograma detalhado aprovado

## Semana 2-3: Configuração de Rede

**Objetivo:** Implementar a segmentação da rede e os controles básicos de firewall para isolar os ambientes.

| Atividade | Complexidade | Prazo | Dependências |
|---|---|---|---|
| Configurar VLANs | Média | 5 dias | Diagrama de rede |
| Implementar firewall | Alta | 7 dias | Regras de negócio |
| Isolar rede visitantes | Baixa | 3 dias | - |

**Riscos Identificados:**

- Impacto na conectividade durante a implementação
- Necessidade de rollback planejado e documentado

## Semana 4: WAF e Proteção Básica

**Objetivo:** Ativar proteções perimetrais cruciais como o WAF para defender contra ataques comuns da web.

```
# Comandos de implementação WAF
sudo apt install nginx-module-security
sudo cp owasp-crs.conf /etc/nginx/conf.d/
sudo nginx -t && sudo systemctl reload nginx
```

**Testes a Realizar:**

- WAF bloqueia payloads SQLi
- Rate limiting funciona conforme esperado
- Logs são gerados corretamente e visíveis

---

# Fase 2: Monitoramento (Dias 31-90)

Esta fase visa estabelecer um monitoramento contínuo e eficaz da segurança, garantindo a visibilidade sobre as atividades da rede e sistemas.

## Mês 2: SIEM e Centralização de Logs

**Objetivo:** Implementar uma solução SIEM para coletar, correlacionar e analisar eventos de segurança em tempo real.

### Instalação Wazuh (Dias 31-45)

O Wazuh será a ferramenta central para a coleta e análise de logs, proporcionando detecção de intrusão e gerenciamento de vulnerabilidades.

```
# Instalação servidor Wazuh
curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

### Configuração Agentes (Dias 46-60)

A implantação de agentes nos principais ativos garantirá que todos os eventos relevantes sejam capturados e enviados para o SIEM.

- Agente no servidor web
- Agente no banco de dados
- Configuração de regras personalizadas para monitoramento específico

## Alertas e Dashboards (Dias 61-90)

Serão criados alertas proativos e dashboards intuitivos para facilitar a visualização e a resposta a incidentes de segurança.

- Configuração de alertas por email para eventos críticos
- Dashboards Grafana para visualização da postura de segurança
- Treinamento da equipe de operações para uso e interpretação das ferramentas

# Métricas de Sucesso para a Fase 2

Para garantir que a Fase 2 de Monitoramento seja considerada um sucesso, definimos métricas claras e alcançáveis que guiarão nossos esforços e permitirão a avaliação contínua do progresso.

- **80% dos Logs Centralizados**

  Atingir a integração e centralização de pelo menos 80% dos logs de segurança dos sistemas e aplicações críticas no SIEM, garantindo visibilidade abrangente.

- **Alertas para Ameaças Críticas Ativos**

  Configurar e testar alertas para todas as ameaças consideradas críticas, assegurando que a equipe seja notificada prontamente sobre incidentes de alta prioridade.

- **Equipe Treinada no Uso do SIEM**

  Garantir que a equipe de operações esteja plenamente capacitada no uso das funcionalidades do SIEM, incluindo a investigação de alertas e a geração de relatórios básicos.

---

# Fase 3: Otimização (Dias 91-180)

A última fase do plano de implementação foca na otimização da arquitetura de defesa e do monitoramento, introduzindo automação e refinando processos para aumentar a eficiência e a resiliência.

## Mês 4-5: Automação e Melhorias Contínuas

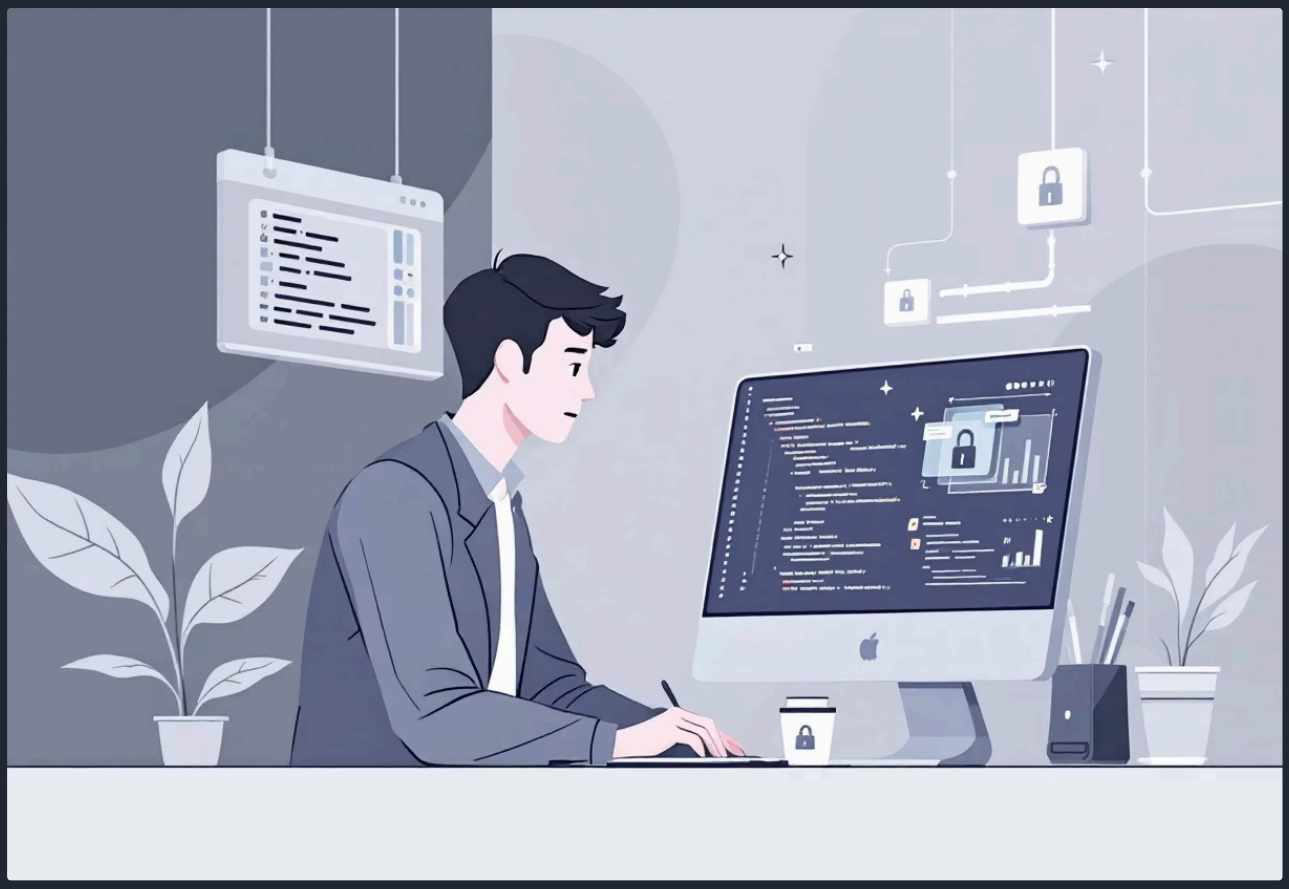
Neste período, o foco será em reduzir a carga manual e aprimorar a resposta a incidentes através da automação e da análise de performance.

### Objetivos

- Automação de respostas a incidentes de segurança comuns.
- Otimização da performance dos sistemas de segurança e monitoramento.
- Revisão e atualização periódica das políticas de segurança.
- Exploração de novas funcionalidades e integrações do SIEM.

### Atividades

- Desenvolvimento e implantação de scripts de automação para tarefas repetitivas.
- Análise de performance dos firewalls, WAF e SIEM, realizando ajustes finos conforme necessário.
- Revisão e atualização da documentação de segurança e runbooks existentes.
- Avaliação de ferramentas complementares para enriquecer a postura de segurança.



## Mês 6: Validação e Entrega Final

O último mês será dedicado à validação completa da solução implementada, garantindo que todos os componentes estejam operacionais, seguros e que a equipe esteja preparada para o handover.

- **Testes de Penetração Internos:** Realização de simulações de ataque controladas para identificar e corrigir vulnerabilidades remanescentes.
- **Simulação de Incidente:** Execução de um exercício de resposta a incidentes completo para testar a eficácia dos runbooks e a prontidão da equipe.
- **Documentação Final do Projeto:** Consolidação de toda a documentação, incluindo arquitetura, configurações, runbooks e políticas atualizadas.
- **Treinamento e Handover:** Treinamento final para a equipe de operações e formalização da transição do projeto para a operação contínua.

---

# Matriz de Riscos e Mitigações

A seguir, apresentamos uma matriz detalhada dos riscos técnicos e operacionais identificados para este projeto, juntamente com as estratégias de mitigação planejadas para cada um. Esta abordagem proativa visa minimizar interrupções e garantir o sucesso da implementação.

## Riscos Técnicos

| | | | |
|---|---|---|---|
| Configuração incorreta do WAF ou Firewall | Alta | Alto | Testes em ambiente de homologação, validação com equipe técnica. |
| Indisponibilidade de serviços durante a implementação | Média | Alto | Implementação em janela de manutenção programada, plano de rollback documentado. |
| Performance dos sistemas impactada pelas ferramentas de segurança | Baixa | Médio | Monitoramento contínuo da performance, ajustes de otimização, testes de carga. |
| Incompatibilidade de integrações do SIEM com sistemas legados | Média | Médio | Testes de integração prévios, desenvolvimento de conectores customizados se necessário. |

## Riscos Operacionais

| | | | |
|---|---|---|---|
| Resistência da equipe interna à adoção de novas ferramentas/processos | Média | Médio | Treinamento intensivo, comunicação clara dos benefícios, envolvimento no processo de decisão. |
| Falta de recursos humanos especializados para manutenção pós-projeto | Baixa | Alto | Planejamento de contratação ou capacitação interna, contrato de suporte com consultoria externa. |
| Mudanças de escopo inesperadas durante o projeto | Baixa | Médio | Processo formal de controle de mudanças, revisão periódica do escopo com stakeholders. |
| Orçamento estourado devido a custos não previstos | Baixa | Alto | Controle financeiro rigoroso, reserva para contingências, aprovação de despesas adicionais. |

# Cronograma Detalhado do Projeto

O cronograma abaixo ilustra as três fases principais e suas respectivas atividades, fornecendo uma visão clara da duração e sequência de cada etapa. Este diagrama de Gantt é uma representação visual do planejamento para a implementação completa.

---

# Checklist de Entregáveis - Loja Zeta

Para cada fase do projeto, uma série de entregáveis chave foi definida para garantir o progresso e a conclusão bem-sucedida das atividades planejadas. Este checklist serve como um guia para a validação das etapas e o encerramento de cada período.

### Entrega Fase 1 (Dia 30)

- Firewall configurado e testado.
- VLANs implementadas e documentadas.
- WAF ativo com regras OWASP.
- Backup automatizado funcionando.
- MFA implementado para administradores.

### Entrega Fase 2 (Dia 90)

- SIEM operacional com >80% cobertura de logs.
- Alertas configurados e testados para ameaças críticas.
- Dashboards de segurança ativos no Grafana.
- Equipe treinada no uso das ferramentas SIEM.

### Entrega Final (Dia 180)

- Automação de respostas a incidentes implementada.
- Testes de penetração realizados e relatórios gerados.
- Documentação completa do projeto entregue.
- Plano de manutenção e suporte contínuo estabelecido.

---

# Comunicação e Reporting do Projeto

Uma comunicação eficaz é fundamental para o sucesso do projeto. Serão estabelecidas reuniões regulares e métricas claras para manter todas as partes interessadas informadas sobre o progresso, desafios e decisões importantes.

## Reuniões Regulares

| | | | |
|---|---|---|---|
| Reunião de Status do Projeto | Semanal | Equipe Completa do Projeto | Acompanhamento do progresso, revisão de tarefas, alinhamento de próximos passos. |
| Reunião Técnica | Quinzenal | Equipe Técnica (Devs, Ops, Consultor) | Discussão aprofundada de desafios técnicos, soluções e planejamento de implementações. |
| Reunião de Steering Committee | Mensal | Diretoria da Loja Zeta, Gerente de Projeto | Revisão de alto nível, decisões estratégicas, aprovação de mudanças de escopo/orçamento. |

## Métricas de Reporting

Os relatórios periódicos incluirão as seguintes métricas para fornecer uma visão abrangente do status do projeto:

- **Progresso:** Percentual de conclusão das fases e atividades em relação ao planejado.
- **Riscos:** Identificação de novos riscos, status dos riscos existentes e eficácia das mitigações.
- **Qualidade:** Resultados dos testes de segurança (WAF, SIEM, pentest) e da simulação de incidentes.
- **Orçamento:** Comparativo entre gastos reais e o orçamento planejado, com justificativas para desvios.
- **Desafios:** Pontos de bloqueio e necessidade de suporte da diretoria.

# Tecnologias e Ferramentas - Loja Zeta

Esta seção detalha a arquitetura tecnológica e as ferramentas que serão implementadas para garantir a defesa e o monitoramento da Loja Zeta. A seleção foi baseada em critérios de robustez, segurança, escalabilidade e custo-benefício, priorizando soluções de código aberto quando possível para maximizar a flexibilidade e minimizar dependências.

## Stack Tecnológico Principal

A base da nossa arquitetura de defesa é um stack tecnológico moderno e eficiente, desenhado para suportar as operações da Loja Zeta com alta performance e segurança.

### Camada de Aplicação

| Componente | Versão | Finalidade | Observações |
|---|---|---|---|
| Node.js | 18.x LTS | Runtime da aplicação | Versão LTS com suporte até 2025 |
| Express.js | 4.x | Framework web | Configuração de segurança reforçada |
| Nginx | 1.22+ | Reverse proxy + Load balancer | Com módulo WAF integrado |

## Banco de Dados

| Componente | Versão | Configuração |
|---|---|---|
| PostgreSQL | 15.x | Cluster ativo-standby para alta disponibilidade |
| pgBouncer | 1.18+ | Connection pooler para otimizar o uso de recursos |
| Wal-G | 2.0+ | Ferramenta para backup e recovery contínuo de PostgreSQL |

## Segurança e Monitoramento

| Categoria | Ferramenta | Licença | Uso |
|---|---|---|---|
| WAF | ModSecurity + OWASP CRS | Open Source | Proteção contra ataques web conhecidos |
| SIEM | Wazuh | Open Source | Correlação de logs, detecção de intrusão e alertas |
| Monitoring | Prometheus + Grafana | Open Source | Coleta e visualização de métricas de performance e segurança |
| Vulnerability | Trivy | Open Source | Scan de vulnerabilidades em containers e código-fonte |

---

# Especificações de Configuração

Detalhes das configurações de segurança essenciais para a proteção da infraestrutura da Loja Zeta.

## 1. Componentes de Segurança

- **WAF/CRS:** ModSecurity configurado com as regras do OWASP Core Rule Set para filtragem de tráfego malicioso.
- **Rate Limiting:** Implementação de limitação de requisições por IP e/ou endpoint para mitigar ataques de força bruta e DoS.
- **Geo-blocking:** Bloqueio de tráfego originado de regiões geográficas de alto risco para o negócio.

## Banco de Dados

| Componente | Versão | Configuração |
|---|---|---|
| PostgreSQL | 15.x | Cluster ativo-standby para alta disponibilidade |
| pgBouncer | 1.18+ | Connection pooler para otimizar o uso de recursos |
| Wal-G | 2.0+ | Ferramenta para backup e recovery contínuo de PostgreSQL |

## Segurança e Monitoramento

| Categoria | Ferramenta | Licença | Uso |
|---|---|---|---|
| WAF | ModSecurity + OWASP CRS | Open Source | Proteção contra ataques web conhecidos |
| SIEM | Wazuh | Open Source | Correlação de logs, detecção de intrusão e alertas |
| Monitoring | Prometheus + Grafana | Open Source | Coleta e visualização de métricas de performance e segurança |
| Vulnerability | Trivy | Open Source | Scan de vulnerabilidades em containers e código-fonte |

---

# Especificações de Configuração

Detalhes das configurações de segurança essenciais para a proteção da infraestrutura da Loja Zeta.

## 1. Componentes de Segurança

- **WAF/CRS:** ModSecurity configurado com as regras do OWASP Core Rule Set para filtragem de tráfego malicioso.
- **Rate Limiting:** Implementação de limitação de requisições por IP e/ou endpoint para mitigar ataques de força bruta e DoS.
- **Geo-blocking:** Bloqueio de tráfego originado de regiões geográficas de alto risco para o negócio.

# 2. Camada de Rede

## 2.1 Segmentação

A rede será segmentada em VLANs distintas para isolar diferentes tipos de tráfego e serviços, reduzindo a superfície de ataque.

- **VLAN 10:** Rede pública (DMZ) para serviços expostos à internet.
- **VLAN 20:** Rede de aplicação para os servidores de aplicação.
- **VLAN 30:** Rede de banco de dados para os servidores de dados.
- **VLAN 40:** Rede administrativa para acesso seguro de equipes internas.

## 2.2 Controles de Acesso

- **ACLs (Access Control Lists):** Regras de firewall rigorosas aplicadas entre VLANs para controlar o fluxo de comunicação.
- **NAC (Network Access Control):** Controle de acesso à rede para garantir que apenas dispositivos autorizados se conectem.
- **VPN site-to-site:** Conexão VPN segura para acesso remoto, garantindo confidencialidade e integridade.

# 3. Camada de Dados

## 3.1 Estratégia de Backup

Uma estratégia robusta de backup e recuperação será implementada para proteger os dados críticos da Loja Zeta.

- **Backup completo:** Diário (23:00), cobrindo todos os dados.
- **Backup incremental:** Horário, para minimizar a perda de dados entre backups completos.
- **Retenção:** 30 dias local para recuperação rápida + 90 dias na nuvem para recuperação de desastres.
- **Testes de restauração:** Semanal, para validar a integridade e funcionalidade dos backups.

## 3.2 Criptografia

Todos os dados serão criptografados para garantir a confidencialidade, tanto em repouso quanto em trânsito.

- **Dados em repouso:** Utilização de LUKS para criptografia de disco e PostgreSQL TDE (Transparent Data Encryption).
- **Dados em trânsito:** Uso de TLS 1.3 para todas as comunicações, assegurando canais seguros.

---

# 2. Camada de Rede

## 2.1 Segmentação

A rede será segmentada em VLANs distintas para isolar diferentes tipos de tráfego e serviços, reduzindo a superfície de ataque.

- **VLAN 10:** Rede pública (DMZ) para serviços expostos à internet.
- **VLAN 20:** Rede de aplicação para os servidores de aplicação.
- **VLAN 30:** Rede de banco de dados para os servidores de dados.
- **VLAN 40:** Rede administrativa para acesso seguro de equipes internas.

## 2.2 Controles de Acesso

- **ACLs (Access Control Lists):** Regras de firewall rigorosas aplicadas entre VLANs para controlar o fluxo de comunicação.
- **NAC (Network Access Control):** Controle de acesso à rede para garantir que apenas dispositivos autorizados se conectem.
- **VPN site-to-site:** Conexão VPN segura para acesso remoto, garantindo confidencialidade e integridade.

# 3. Camada de Dados

## 3.1 Estratégia de Backup

Uma estratégia robusta de backup e recuperação será implementada para proteger os dados críticos da Loja Zeta.

- **Backup completo:** Diário (23:00), cobrindo todos os dados.
- **Backup incremental:** Horário, para minimizar a perda de dados entre backups completos.
- **Retenção:** 30 dias local para recuperação rápida + 90 dias na nuvem para recuperação de desastres.
- **Testes de restauração:** Semanal, para validar a integridade e funcionalidade dos backups.

## 3.2 Criptografia

Todos os dados serão criptografados para garantir a confidencialidade, tanto em repouso quanto em trânsito.

- **Dados em repouso:** Utilização de LUKS para criptografia de disco e PostgreSQL TDE (Transparent Data Encryption).
- **Dados em trânsito:** Uso de TLS 1.3 para todas as comunicações, assegurando canais seguros.

---

# Especificações Técnicas

## 4.1 Requisitos de Hardware/Software

Os requisitos mínimos de hardware e software para os principais componentes da infraestrutura são os seguintes:

| Componente | Especificação | Quantidade | Observações |
|---|---|---|---|
| Servidor Web | 4vCPU, 8GB RAM, 100GB SSD | 2 | Ativo/standby para redundância e balanceamento de carga |
| Banco de Dados | 8vCPU, 16GB RAM, 200GB SSD | 1 | Com replicação para alta disponibilidade |
| SIEM | 4vCPU, 8GB RAM, 500GB HDD | 1 | Servidor dedicado para coleta e análise de logs |

---

## Configuração de Segurança NGINX (Exemplo)

A seguir, um exemplo de configuração de segurança para o NGINX, ilustrando a implementação de cabeçalhos de segurança, rate limiting e integração com o WAF.

```
http {
    # Security headers
    add_header X-Frame-Options DENY;
    add_header X-Content-Type-Options nosniff;
    add_header X-XSS-Protection "1; mode=block";

    # Rate limiting
    limit_req_zone $binary_remote_addr zone=login:10m rate=10r/m;

    # WAF configuration
    modsecurity on;
    modsecurity_rules_file /etc/nginx/modsecurity.conf;
}
```

### Explicação:

- **Security headers:**
  - **X-Frame-Options DENY:** Bloqueia o carregamento do site em frames/iframes, prevenindo ataques de clickjacking.
  - **X-Content-Type-Options nosniff:** Evita que navegadores interpretem arquivos como um tipo diferente do que foi declarado pelo servidor.
  - **X-XSS-Protection "1; mode=block":** Habilita proteção contra Cross-Site Scripting (XSS), detectando e bloqueando ataques.
- **Rate limiting:**
  - **limit_req_zone $binary_remote_addr zone=login:10m rate=10r/m;:** Define uma zona de limite de requisições por IP chamada "login". Limita cada IP a 10 requisições por minuto, protegendo contra abusos e ataques DoS.
- **WAF configuration (Web Application Firewall):**
  - **modsecurity on;:** Ativa o ModSecurity, firewall de aplicações web para inspeção profunda do tráfego.
  - **modsecurity_rules_file /etc/nginx/modsecurity.conf;:** Define o arquivo de regras do ModSecurity, que conterá as regras OWASP CRS e outras personalizações.

Para garantir a segurança, eficiência e escalabilidade da Loja Zeta, implementamos um conjunto robusto de tecnologias e ferramentas. Esta seção detalha as configurações de segurança para aplicações Node.js e as ferramentas essenciais para o ciclo de desenvolvimento e operação.

---

# Configurações de Segurança Node.js

A segurança da aplicação Node.js é primordial. As seguintes dependências e configurações foram escolhidas para proteger contra vulnerabilidades comuns, garantir a integridade dos dados e otimizar o desempenho.

## Dependências Essenciais (package.json)

```
{
  "dependencies": {
    "helmet": "^7.0.0",
    "express-rate-limit": "^6.7.0",
    "bcryptjs": "^2.4.3",
    "express-validator": "^7.0.1"
  }
}
```

- **Helmet:** Adiciona automaticamente cabeçalhos HTTP de segurança para proteger a aplicação contra ataques como Cross-Site Scripting (XSS), Clickjacking e outros. É uma camada de proteção fundamental.
- **express-rate-limit:** Impõe limites de taxa às requisições, protegendo a aplicação contra ataques de Força Bruta e Negação de Serviço (DoS) ao restringir o número de requisições que um usuário ou IP pode fazer em um determinado período.
- **bcryptjs:** Uma biblioteca poderosa e amplamente utilizada para hash seguro de senhas. Garante que as senhas dos usuários sejam armazenadas de forma criptografada, impedindo o acesso não autorizado mesmo em caso de violação de dados.
- **express-validator:** Facilita a validação e sanitização de dados de entrada do usuário. Isso é crucial para prevenir ataques de injeção e garantir que apenas dados válidos e seguros sejam processados pela aplicação.

## Configuração da Aplicação (app.js)

```
const helmet = require('helmet');
const rateLimit = require('express-rate-limit');

app.use(helmet());
app.use(rateLimit({
  windowMs: 15 * 60 * 1000, // 15 minutos
  max: 100, // Máximo de 100 requisições por IP
  message: 'Too many requests from this IP'
}));
```

- **app.use(helmet()):** Integra o Helmet à aplicação Express, ativando automaticamente um conjunto de cabeçalhos de segurança que fortalecem as defesas HTTP da aplicação.
- **app.use(rateLimit(...)):** Aplica a política de limitação de taxa globalmente. Cada endereço IP é limitado a 100 requisições a cada 15 minutos (900.000 ms). Se o limite for excedido, o servidor responderá com um erro "429 Too Many Requests" e a mensagem personalizada "Too many requests from this IP", protegendo os recursos da aplicação.

---

## 2. Monitoramento e Alertas

O monitoramento contínuo é essencial para identificar e responder rapidamente a problemas de desempenho, disponibilidade e segurança.

| | | |
|---|---|---|
| Uptime | Pingdom | 99.9% de SLA (Service Level Agreement) de disponibilidade garantido. |
| Performance | New Relic | Tempo de resposta da aplicação inferior a 200ms para a maioria das requisições. |
| Security | Wazuh | Alertas em tempo real para eventos de segurança críticos, com notificação imediata à equipe de IR. |
| Logs | ELK Stack | Retenção de logs por 90 dias para análise forense e auditoria de segurança. |

## 3. Licenças e Custos

Uma combinação estratégica de ferramentas open-source e comerciais é utilizada para equilibrar custos e recursos.

### 3.1 Open Source (Gratuito)

- **Wazuh:** SIEM (Security Information and Event Management) e monitoramento de integridade de arquivos.
- **ModSecurity:** Web Application Firewall (WAF) para proteção de aplicações web.
- **Prometheus:** Sistema de monitoramento e alerta de métricas.
- **Grafana:** Ferramenta de visualização e painéis para monitoramento.
- **Trivy:** Scanner de vulnerabilidades para contêineres e sistemas de arquivos.

### 3.2 Commercial (Custos Estimados)

| | | |
|---|---|---|
| Cloudflare | 200 | Cloudflare |
| GitHub Team | 100 | GitHub |
| New Relic | 300 | New Relic |
| **Total Estimado** | 600 | |

## 4. Requisitos de Sistema

Os requisitos mínimos para a infraestrutura da Loja Zeta foram definidos para garantir desempenho e estabilidade.

### 4.1 Servidores de Produção

| | | | | |
|---|---|---|---|---|
| Web | 4 | 8GB | 100GB SSD | 2 |
| Database | 8 | 16GB | 200GB SSD | 2 |
| Monitoring | 2 | 4GB | 500GB HDD | 1 |

### 4.2 Requisitos de Rede

- **Largura de banda:** 100 Mbps dedicados para garantir fluxo de dados sem gargalos.
- **Latência:** Inferior a 50ms para usuários principais, otimizando a experiência do cliente.
- **Firewall:** Regras específicas e rigorosas por serviço para minimizar a superfície de ataque e controlar o tráfego.

## 5. Matriz de Compatibilidade

O controle de versão e o planejamento de upgrades são cruciais para manter a segurança e a funcionalidade.

| | | | |
|---|---|---|---|
| Node.js | 18.17.0 | Abr/2025 | Nov/2024 |
| PostgreSQL | 15.3 | Nov/2027 | Jan/2025 |
| Nginx | 1.22.1 | Abr/2026 | Mar/2025 |

## 6. Dependências de Segurança

Uma análise das dependências de segurança garante que os pacotes utilizados não introduzam vulnerabilidades conhecidas.

| | | |
|---|---|---|
| Express.js | 4.18.2 | Nenhuma crítica |
| Helmet | 7.0.0 | Nenhuma crítica |
| bcryptjs | 2.4.3 | Nenhuma crítica |

# Ferramentas de Desenvolvimento e Operação (DevOps)

Para otimizar o ciclo de vida do desenvolvimento de software e garantir operações seguras e contínuas, a Loja Zeta adota um conjunto integrado de ferramentas de DevOps. Essas ferramentas cobrem desde o controle de versão até o monitoramento em produção, assegurando qualidade e agilidade.

## 1. CI/CD Pipeline

Um pipeline de CI/CD bem definido é crucial para entregas rápidas e seguras. Ele automatiza as etapas de construção, teste e implantação.

| | | |
|---|---|---|
| Version Control | Git + GitHub | Regras de proteção de branches para garantir a integridade do código e revisões obrigatórias. |
| CI | GitHub Actions | Scans de segurança automatizados e testes de unidade/integração a cada push ou pull request. |
| Testing | Jest + Supertest | Testes de unidade, integração e segurança (como testes de API) são parte integrante do ciclo de desenvolvimento. |
| Container | Docker | Imagens de contêiner assinadas e verificadas para garantir sua autenticidade e integridade antes da implantação. |

## 2. Monitoramento e Alertas

O monitoramento contínuo é essencial para identificar e responder rapidamente a problemas de desempenho, disponibilidade e segurança.

| | | |
|---|---|---|
| Uptime | Pingdom | 99.9% de SLA (Service Level Agreement) de disponibilidade garantido. |
| Performance | New Relic | Tempo de resposta da aplicação inferior a 200ms para a maioria das requisições. |
| Security | Wazuh | Alertas em tempo real para eventos de segurança críticos, com notificação imediata à equipe de IR. |
| Logs | ELK Stack | Retenção de logs por 90 dias para análise forense e auditoria de segurança. |

## 3. Licenças e Custos

Uma combinação estratégica de ferramentas open-source e comerciais é utilizada para equilibrar custos e recursos.

### 3.1 Open Source (Gratuito)

- **Wazuh:** SIEM (Security Information and Event Management) e monitoramento de integridade de arquivos.
- **ModSecurity:** Web Application Firewall (WAF) para proteção de aplicações web.
- **Prometheus:** Sistema de monitoramento e alerta de métricas.
- **Grafana:** Ferramenta de visualização e painéis para monitoramento.
- **Trivy:** Scanner de vulnerabilidades para contêineres e sistemas de arquivos.

### 3.2 Commercial (Custos Estimados)

| | | |
|---|---|---|
| Cloudflare | 200 | Cloudflare |
| GitHub Team | 100 | GitHub |
| New Relic | 300 | New Relic |
| **Total Estimado** | 600 | |

## 4. Requisitos de Sistema

Os requisitos mínimos para a infraestrutura da Loja Zeta foram definidos para garantir desempenho e estabilidade.

### 4.1 Servidores de Produção

| | | | | |
|---|---|---|---|---|
| Web | 4 | 8GB | 100GB SSD | 2 |
| Database | 8 | 16GB | 200GB SSD | 2 |
| Monitoring | 2 | 4GB | 500GB HDD | 1 |

### 4.2 Requisitos de Rede

- **Largura de banda:** 100 Mbps dedicados para garantir fluxo de dados sem gargalos.
- **Latência:** Inferior a 50ms para usuários principais, otimizando a experiência do cliente.
- **Firewall:** Regras específicas e rigorosas por serviço para minimizar a superfície de ataque e controlar o tráfego.

## 5. Matriz de Compatibilidade

O controle de versão e o planejamento de upgrades são cruciais para manter a segurança e a funcionalidade.

| | | | |
|---|---|---|---|
| Node.js | 18.17.0 | Abr/2025 | Nov/2024 |
| PostgreSQL | 15.3 | Nov/2027 | Jan/2025 |
| Nginx | 1.22.1 | Abr/2026 | Mar/2025 |

## 6. Dependências de Segurança

Uma análise das dependências de segurança garante que os pacotes utilizados não introduzam vulnerabilidades conhecidas.
6. Dependências de Segurança

Uma análise das dependências de segurança garante que os pacotes utilizados não introduzam vulnerabilidades conhecidas.

| | | |
|---|---|---|
| Express.js | 4.18.2 | Nenhuma crítica |
| Helmet | 7.0.0 | Nenhuma crítica |
| bcryptjs | 2.4.3 | Nenhuma crítica |

### 3.2 Commercial (Custos Estimados)

| | | |
|---|---|---|
| Cloudflare | 200 | Cloudflare |
| GitHub Team | 100 | GitHub |
| New Relic | 300 | New Relic |
| **Total Estimado** | 600 | |

## 4. Requisitos de Sistema

Os requisitos mínimos para a infraestrutura da Loja Zeta foram definidos para garantir desempenho e estabilidade.

### 4.1 Servidores de Produção

| | | | | |
|---|---|---|---|---|
| Web | 4 | 8GB | 100GB SSD | 2 |
| Database | 8 | 16GB | 200GB SSD | 2 |
| Monitoring | 2 | 4GB | 500GB HDD | 1 |

### 4.2 Requisitos de Rede

- **Largura de banda:** 100 Mbps dedicados para garantir fluxo de dados sem gargalos.
- **Latência:** Inferior a 50ms para usuários principais, otimizando a experiência do cliente.
- **Firewall:** Regras específicas e rigorosas por serviço para minimizar a superfície de ataque e controlar o tráfego.

## 5. Matriz de Compatibilidade

O controle de versão e o planejamento de upgrades são cruciais para manter a segurança e a funcionalidade.

| | | | |
|---|---|---|---|
| Node.js | 18.17.0 | Abr/2025 | Nov/2024 |
| PostgreSQL | 15.3 | Nov/2027 | Jan/2025 |
| Nginx | 1.22.1 | Abr/2026 | Mar/2025 |

# 6. Dependências de Segurança

Uma análise das dependências de segurança garante que os pacotes utilizados não introduzam vulnerabilidades conhecidas.
6. Dependências de Segurança

Uma análise das dependências de segurança garante que os pacotes utilizados não introduzam vulnerabilidades conhecidas.

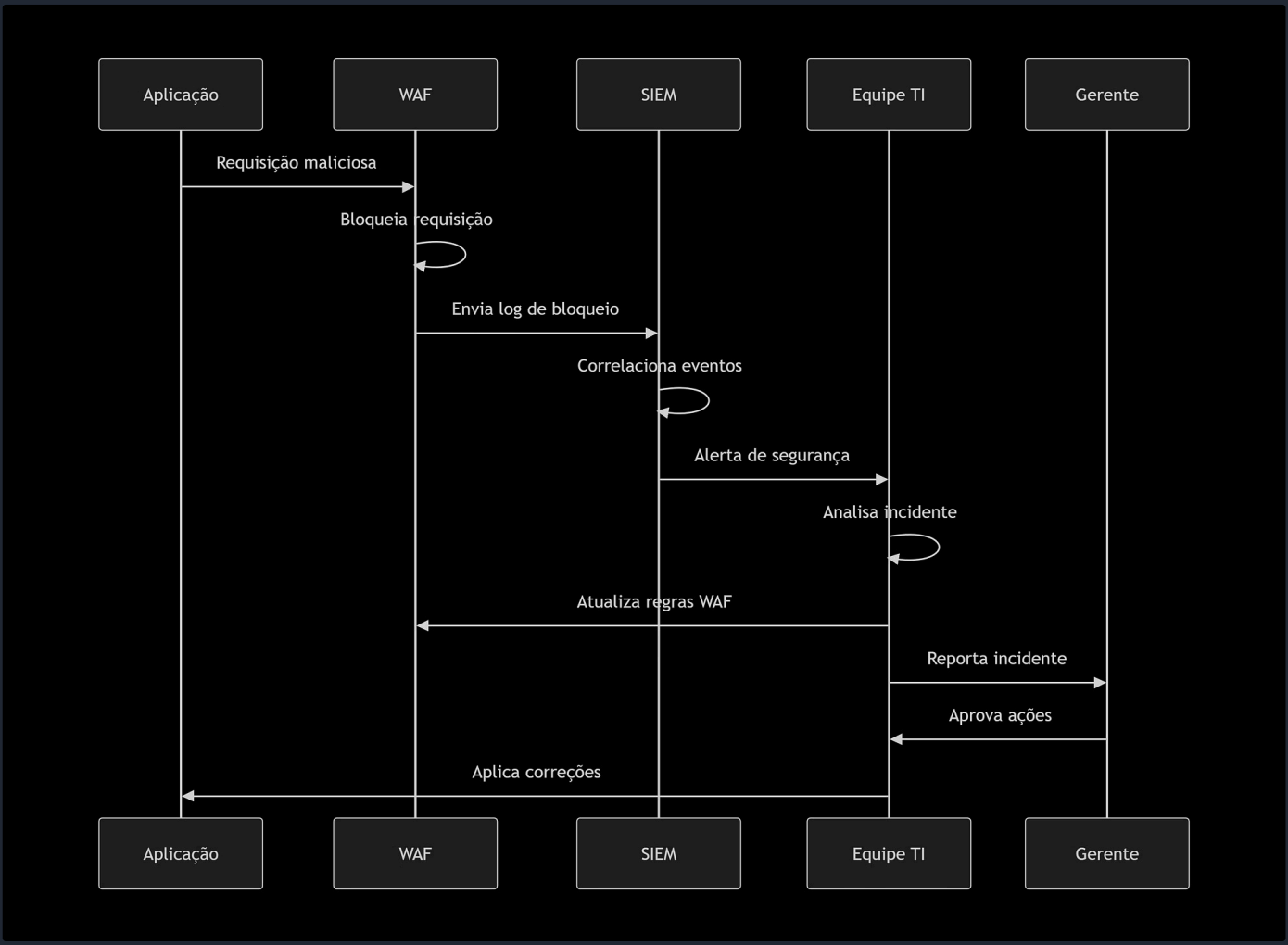
| | | |
|---|---|---|
| Express.js | 4.18.2 | Nenhuma crítica |
| Helmet | 7.0.0 | Nenhuma crítica |
| bcryptjs | 2.4.3 | Nenhuma crítica |

# Diagramas

Para consolidar a visão técnica da Loja Zeta, detalhamos a arquitetura proposta, focando no fluxo de dados, proteção de infraestrutura e segmentação de rede. Estes diagramas ilustram como os componentes se interligam e como as medidas de segurança são implementadas em cada camada.

## Fluxo de Dados e Proteção

Este diagrama apresenta o fluxo de dados dos usuários, desde a internet até os servidores de aplicação e banco de dados, destacando os pontos de controle e segurança implementados para proteger a infraestrutura da Loja Zeta.

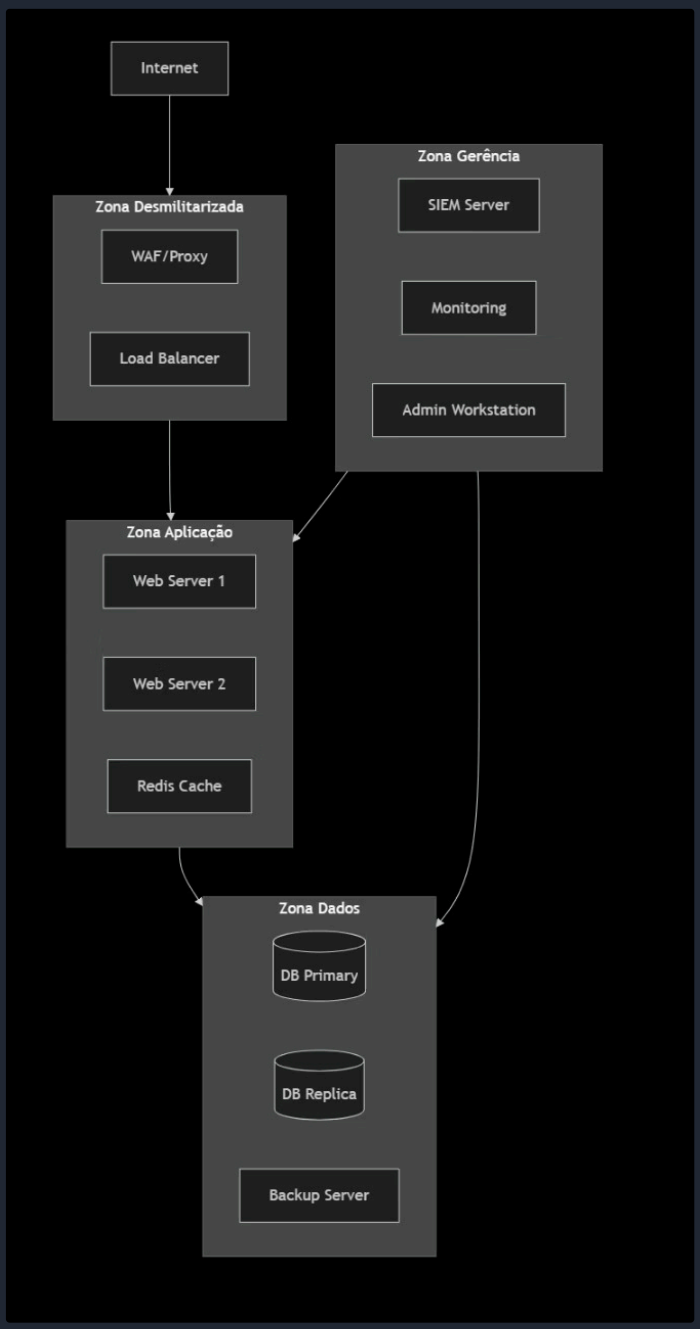



O fluxo inicia com a **Internet**, passando pelo **CDN Cloudflare** para otimização de performance e proteção DDoS. Em seguida, o tráfego é filtrado pelo **WAF/ModSecurity**, que atua como uma barreira de segurança contra ataques web. O **Load Balancer (Nginx)** distribui as requisições para os **Web Servers** (Node.js), que se conectam ao **PostgreSQL (Primary e Replica)**. Todo o sistema é monitorado por um **SIEM (Wazuh)** que alimenta os **Dashboards do Grafana** e aciona o **Sistema de Alertas**, enquanto a **Gestão de Identidade** (IAM, MFA, RBAC) garante acessos controlados.

---

# Arquitetura de Rede: Segmentação e Zonas de Segurança

Este diagrama ilustra a segmentação da rede da Loja Zeta em diferentes zonas de segurança, um pilar fundamental para isolar serviços e limitar o impacto de possíveis incidentes.

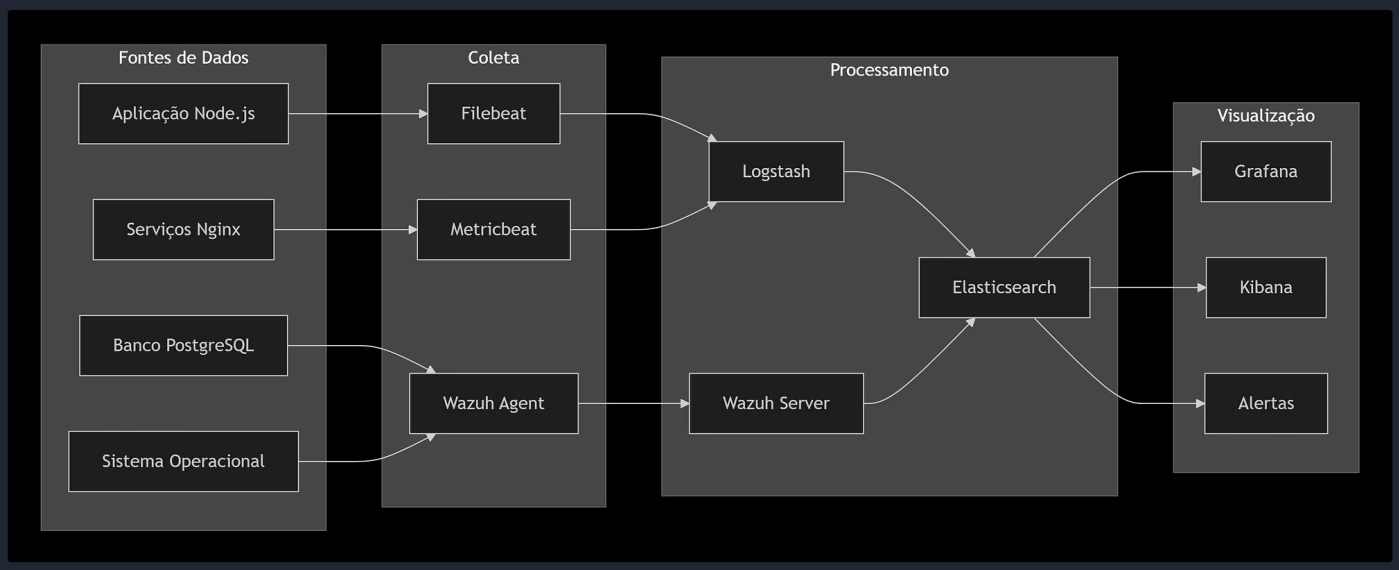



A arquitetura de rede é dividida em quatro zonas principais. A **DMZ (Zona Desmilitarizada)** expõe serviços públicos como WAF e Load Balancer. A **Zona de Aplicação (APP Zone)** hospeda os Web Servers e o Redis Cache. A **Zona de Dados (DATA Zone)** contém os bancos de dados primário, réplica e servidores de backup, sendo a zona mais restrita. Por fim, a **Zona de Gerência (MGMT Zone)** é dedicada a ferramentas de SIEM, Monitoramento e estações de trabalho administrativas, com acessos altamente controlados. Essa segmentação minimiza a superfície de ataque e o movimento lateral em caso de comprometimento.

Para complementar os diagramas de arquitetura e rede apresentados anteriormente, detalhamos aqui as especificações técnicas cruciais. Esta seção aborda o fluxo de coleta e análise de dados, a topologia física da infraestrutura, a configuração de portas e protocolos, as especificações de hardware dos componentes principais, o fluxo de tráfego detalhado e as considerações de segurança por camada. Estes detalhes são fundamentais para compreender a robustez e a segurança da Loja Zeta.

# Fluxo de Coleta e Análise

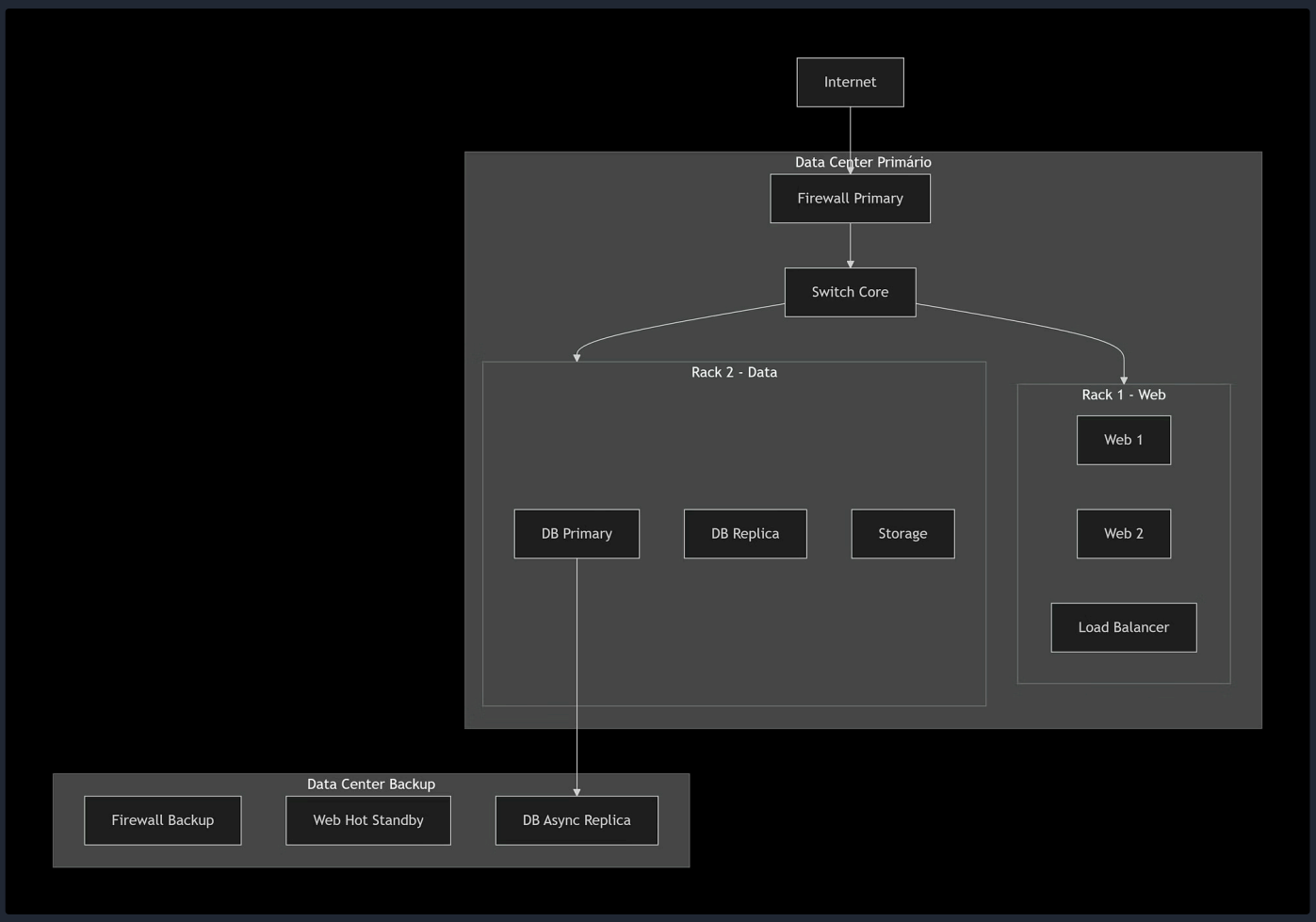
Este diagrama ilustra como os dados e logs são coletados de diversas fontes, processados e, finalmente, visualizados e utilizados para alertas. É um ciclo contínuo que garante a visibilidade sobre o desempenho e a segurança do sistema.

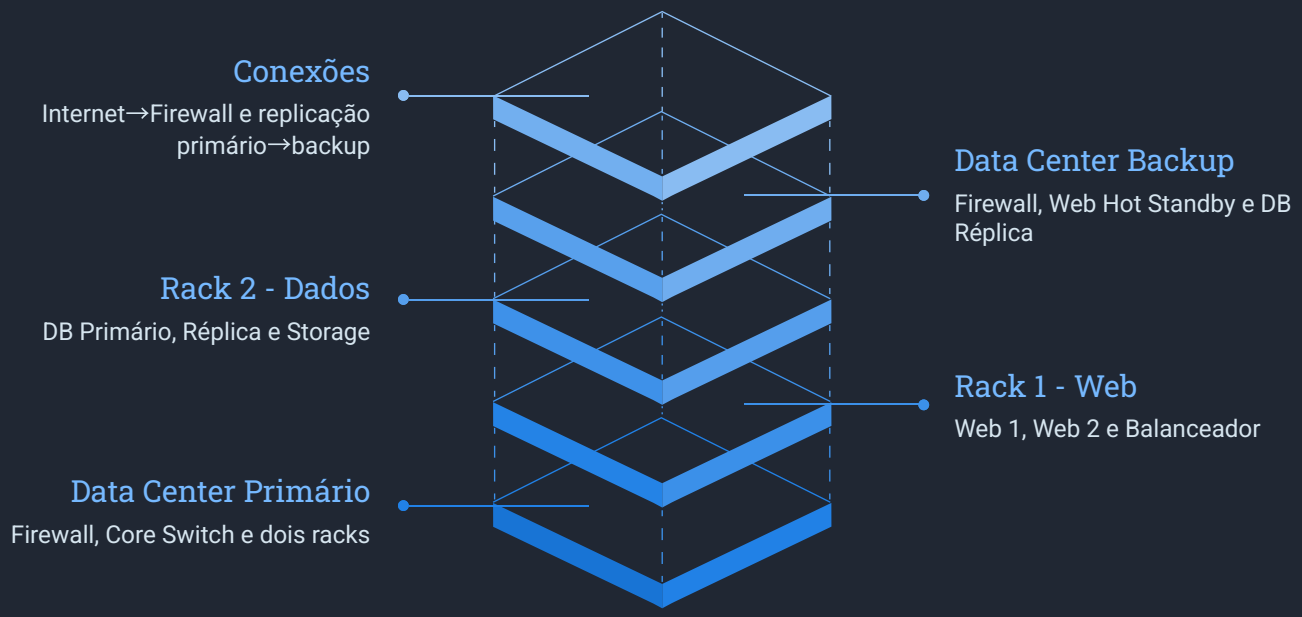


Conforme o fluxo, as aplicações, serviços e bancos de dados geram dados que são coletados por agentes específicos (Filebeat, Metricbeat, Wazuh Agent). Estes dados são então processados por ferramentas como Logstash, Elasticsearch e Wazuh Server, formando a base para visualizações em dashboards do Grafana e Kibana, além de acionar sistemas de alerta em tempo real.

# Topologia Física

A topologia física da Loja Zeta é projetada para resiliência e alta disponibilidade, distribuindo os componentes críticos entre um Data Center Primário e um Data Center de Backup, com replicação e contingência para garantir a continuidade dos negócios.




No Data Center Primário, temos a segmentação em racks dedicados para Web e Dados, com balanceamento de carga e alta disponibilidade. O Data Center de Backup serve como um ponto de recuperação de desastres, com réplicas assíncronas do banco de dados e servidores web em standby, prontos para assumir em caso de falha no primário.

# Configuração de Portas e Protocolos

A seguir, uma tabela detalhada das portas e protocolos utilizados, juntamente com suas direções e níveis de acesso, um componente chave para a definição das regras de firewall e segmentação de rede.

| | | | | |
|---|---|---|---|---|
| HTTP | 80 | TCP | Inbound | Público |
| HTTPS | 443 | TCP | Inbound | Público |
| SSH | 22 | TCP | Inbound | Admin only |
| PostgreSQL | 5432 | TCP | Internal | App only |
| Redis | 6379 | TCP | Internal | App only |

---

# Especificações de Hardware

Os requisitos de hardware são cuidadosamente definidos para cada componente, garantindo que a infraestrutura da Loja Zeta tenha o desempenho e a capacidade necessários para suportar a demanda e as operações críticas.

| Tipo | vCPU | RAM | Storage | Rede |
|---|---|---|---|---|
| Web Server | 4 vCPU | 8GB | 100GB SSD | 1Gbps |
| Database | 8 vCPU | 16GB | 200GB SSD | 1Gbps |
| SIEM | 4 vCPU | 8GB | 500GB HDD | 1Gbps |
| Load Balancer | 2 vCPU | 4GB | 50GB SSD | 1Gbps |

---

# Fluxo de Tráfego Detalhado

Compreender o caminho que uma requisição web percorre é essencial para otimização e diagnóstico de problemas, além de identificar pontos de segurança críticos.

1. Cliente → CDN (Cache e proteção DDoS)
2. CDN → WAF (Filtragem de ameaças)
3. WAF → Load Balancer (Distribuição de carga)
4. Load Balancer → Web Server (Processamento)
5. Web Server → Database (Consulta dados)
6. Web Server → Cliente (Resposta)

---

# Monitoramento e Logs

O processo de monitoramento e coleta de logs é a espinha dorsal para a segurança e a operação contínua, permitindo a detecção precoce de anomalias e incidentes.

1. Todos os componentes → Agentes (Coleta de logs)
2. Agentes → SIEM (Correlação e análise)
3. SIEM → Dashboards (Visualização)
4. SIEM → Alertas (Notificações)

---

# Considerações de Segurança por Camada

A segurança é abordada em múltiplas camadas, desde a rede até os dados, garantindo uma defesa profunda contra ameaças e vulnerabilidades.

## Camada de Rede

- **Segmentação:** VLANs separadas por função para isolamento de tráfego.
- **ACLs:** Controle granular de tráfego para permitir apenas comunicações autorizadas.
- **Monitoramento:** Detecção de anomalias e intrusões em tempo real.

## Camada de Aplicação

- **WAF:** Proteção contra as 10 principais ameaças do OWASP (OWASP Top 10).
- **Rate Limiting:** Prevenção de ataques de força bruta e abuso de recursos.
- **Headers Security:** Implementação de cabeçalhos de segurança HTTP para mitigar vulnerabilidades comuns.

## Camada de Dados

- **Encryption:** Criptografia de dados em trânsito e em repouso para proteger informações sensíveis.
- **Access Control:** Implementação do Princípio do Menor Privilégio para acessos ao banco de dados.
- **Backup:** Estratégia 3-2-1 para garantir a recuperação de dados em caso de desastre.