Política de Segurança de Rede

1. Política de Controle de Acesso

1.1 Requisitos de Segurança do Navegador

- Aplicar requisitos mínimos de versão do navegador:
  - Chrome: Versão 88 ou superior
  - Firefox: Versão 85 ou superior
  - Safari: Versão 14 ou superior
  - Edge: Versão 88 ou superior
- Bloquear acesso de sistemas operacionais obsoletos (Windows XP, Windows 98)
- Implementar validação e sanitização de User-Agent

1.2 Validação de Requisições

- Implementar validação rigorosa de caminhos URI
- Lista branca de caminhos e métodos HTTP permitidos por serviço
- Limitação de taxa:
  - Geral: 1000 requisições por IP por hora
  - Endpoints de autenticação: 10 tentativas por IP por hora
  - Caminhos administrativos: 100 requisições por usuário autenticado por hora
- Limites de tamanho de requisição:
  - Requisição GET máxima: 8KB
  - Requisição POST máxima: 1MB
  - Upload de arquivo máximo: 10MB

1.3 Controle de Acesso Geográfico

- Implementar geo-cercamento para operações sensíveis
- Monitoramento aprimorado para regiões de alto volume
- Exigir acesso VPN para funções administrativas

2. Segurança da Infraestrutura

2.1 Segurança da API

- Implementar política CORS:

```
Access-Control-Allow-Origins: [dominios-permitidos]
Access-Control-Allow-Methods: GET, POST, PUT, PATCH
Access-Control-Max-Age: 7200
```

- Requisitos de versionamento de API
- Padrões de criptografia de requisição/resposta

2.2 Monitoramento e Alertas

- Alertas em tempo real para:
    - Tentativas de acesso a URIs suspeitos
    - Padrões anômalos de requisição
    - Anomalias geográficas
    - Falhas de autenticação
- Relatórios semanais de segurança
- Auditorias mensais de conformidade com a política

2.3 Autenticação e Autorização

- Autenticação multifator para acesso administrativo
- Controle de acesso baseado em função (RBAC)
- Gerenciamento de sessão:
    - Duração máxima da sessão: 8 horas
    - Tempo limite de inatividade: 30 minutos
    - Requisitos de armazenamento seguro de sessão

3. Resposta a Incidentes

3.1 Detecção e Análise

- Detecção automatizada de:
    - Tentativas de força bruta
    - Travessia de diretório
    - Injeção SQL
    - Tentativas de XSS
- Retenção de logs: mínimo de 90 dias

3.2 Contenção e Recuperação

- Bloqueio automático de IP para ataques detectados
- Procedimentos de escalonamento de incidentes
- Procedimentos de restauração do sistema
- Requisitos de análise pós-incidente

4. Conformidade e Atualizações

4.1 Revisão da Política

- Revisões trimestrais da política
- Teste de penetração anual
- Auditorias regulares de conformidade
- Treinamento de segurança para funcionários

4.2 Documentação

- Manter registros de incidentes
- Atualizar procedimentos de segurança
- Documentar todas as exceções à política
- Acompanhar métricas de segurança