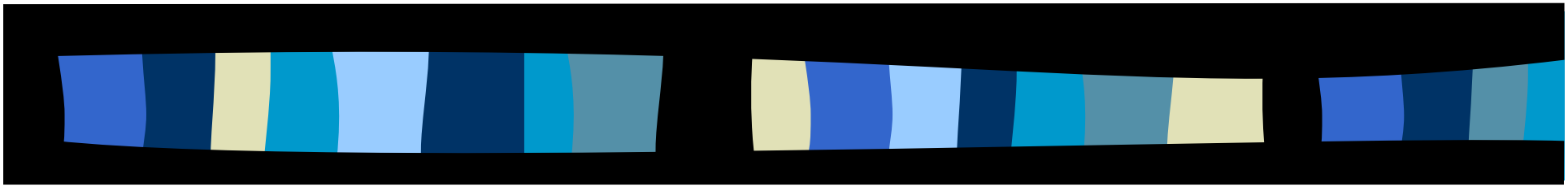
UFSC

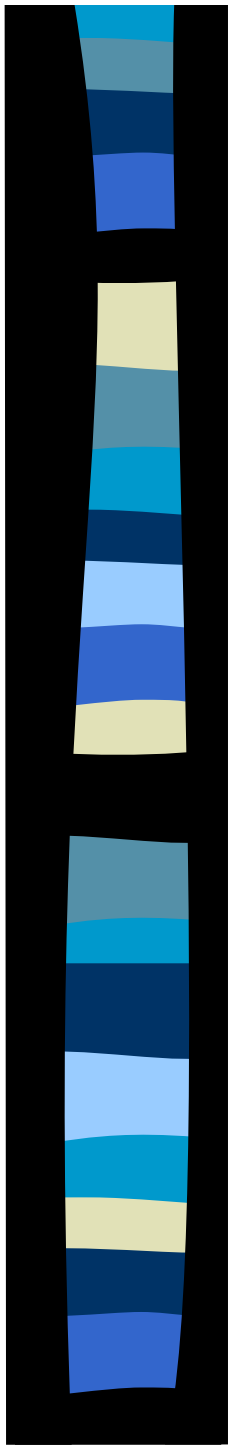
Linha de Pesquisa em Segurança de Redes



Igor Vinícius Mussoi de Lima
Renato Bobsin Machado

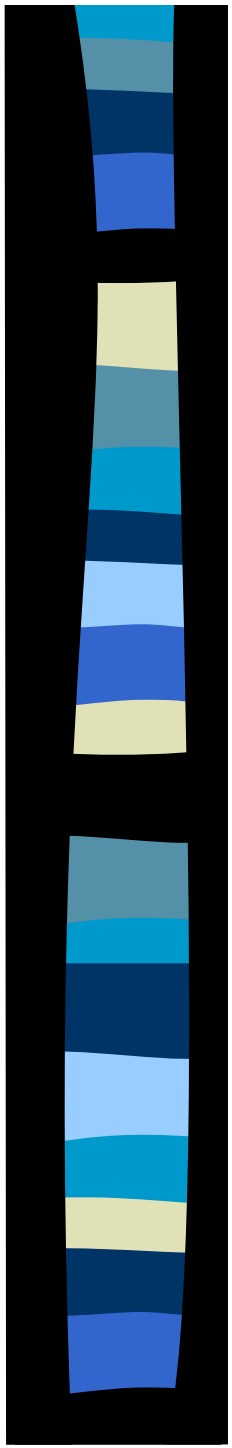
Orientadores:

João Bosco Mangueira Sobral
Kathia Lemos Jucá



Roteiro

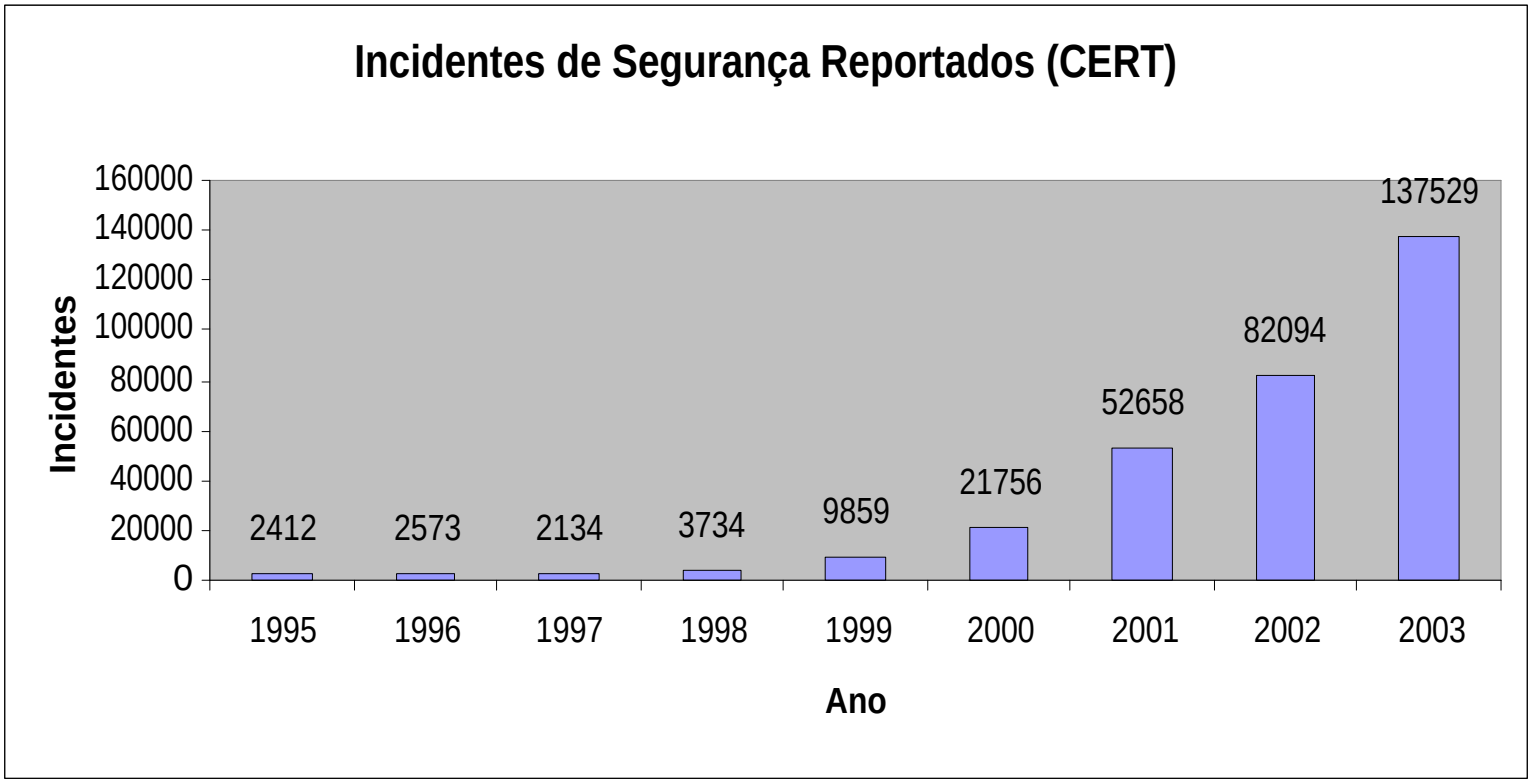
- Conceitos de Segurança
- Sistemas de Detecção de Intrusão
- Abordagem Baseada em Imunologia Computacional e Agentes Móveis
- Abordagem Baseada em Redes Neurais Artificiais



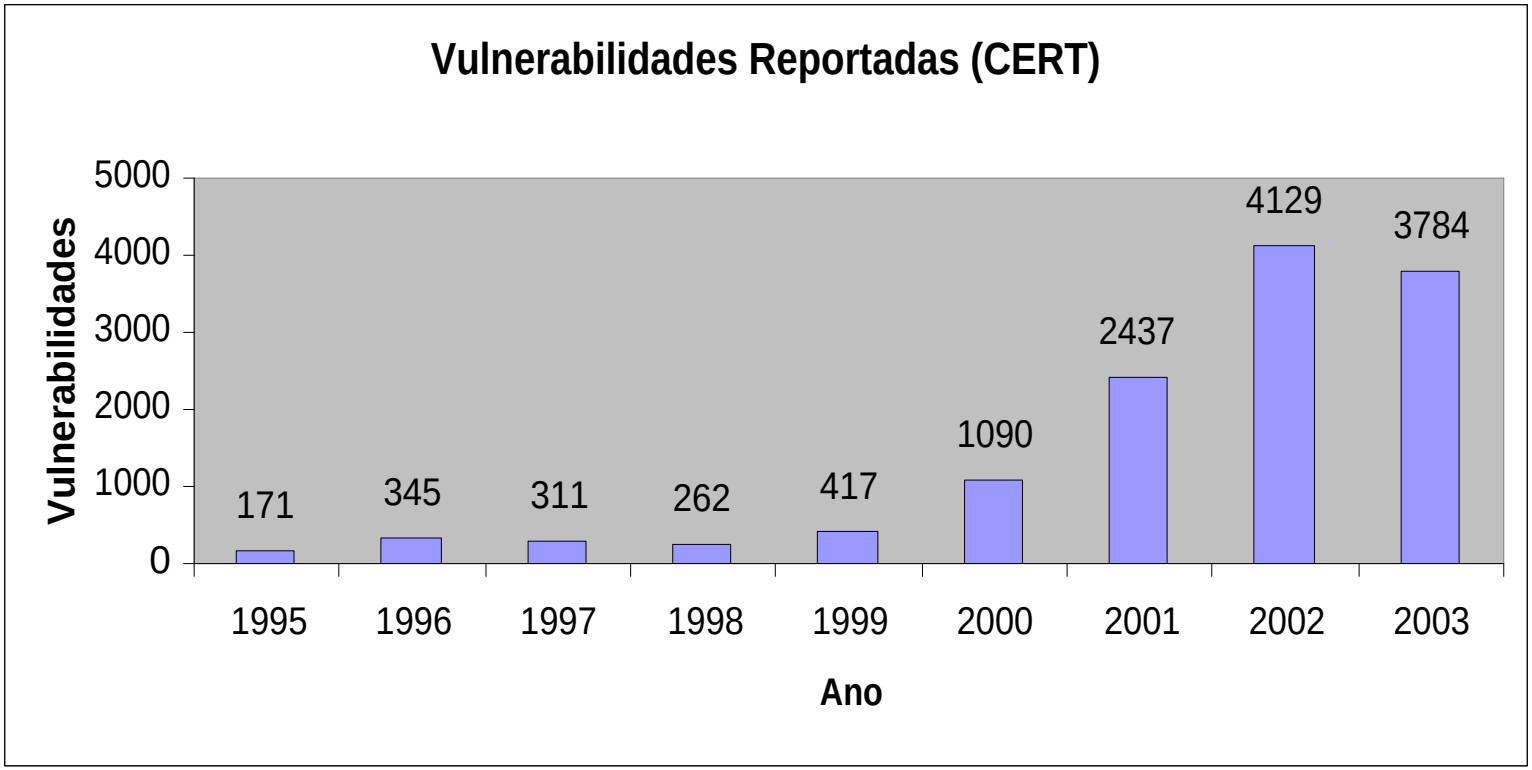
Segurança de Redes

- Evolução Tecnológica
- Importância das Redes
- Necessidade de Segurança

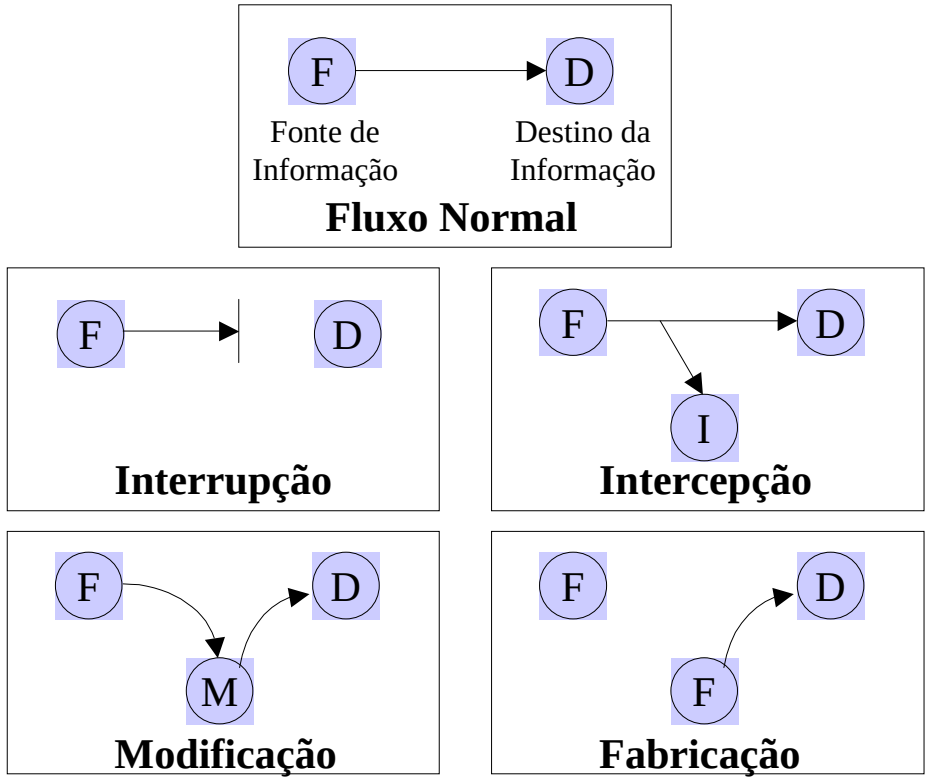
Segurança de Redes
Incidentes Reportados

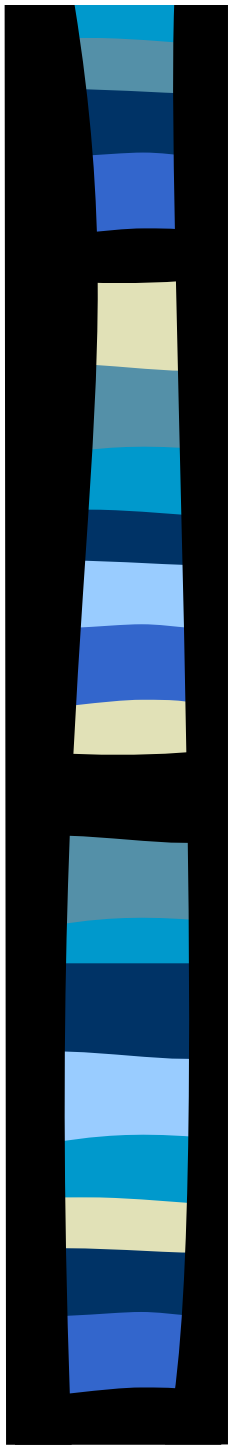


Segurança de Redes
Vulnerabilidades Reportadas



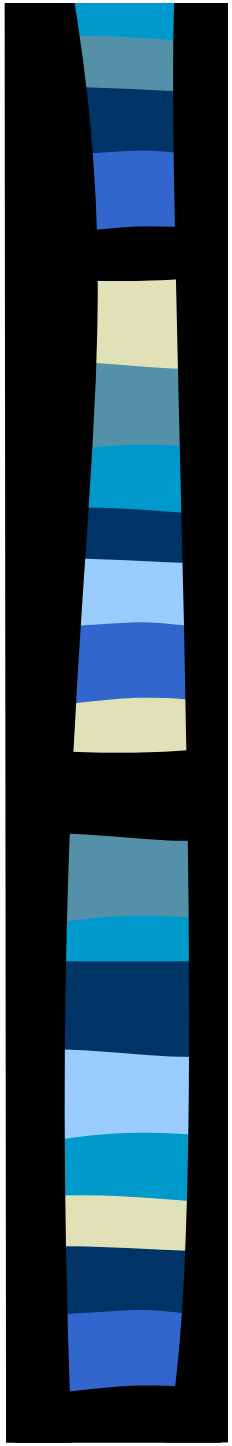
Ameaças a Segurança de Redes





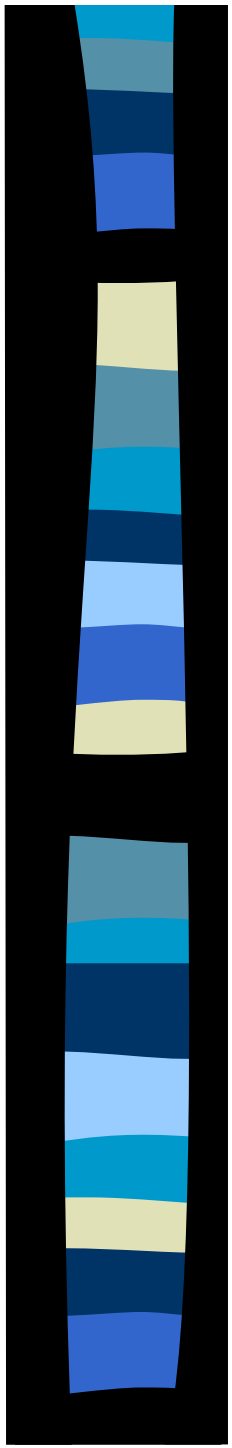
Classes de Ataques

- Sondagem
  - Descoberta de Vulnerabilidades
  - Ferramentas de *Scanners*
- Comprometimento de Serviços
  - *Deny of Services (DoS e DDoS)*
  - Exploração de Falhas
  - Inundação



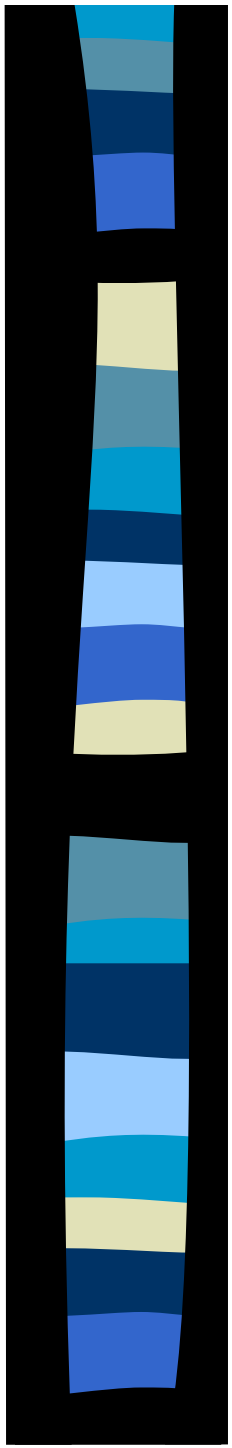
Classes de Ataques

- Intrusão
  - Aquisição de Privilégios, Recursos, Dados
  - Controle do Sistema
- Ataques ao Host
  - Falhas em Programas Executanto
- Ataques a Rede
  - Vulnerabilidades dos Protocolos e Serviços



Detecção de Intrusão

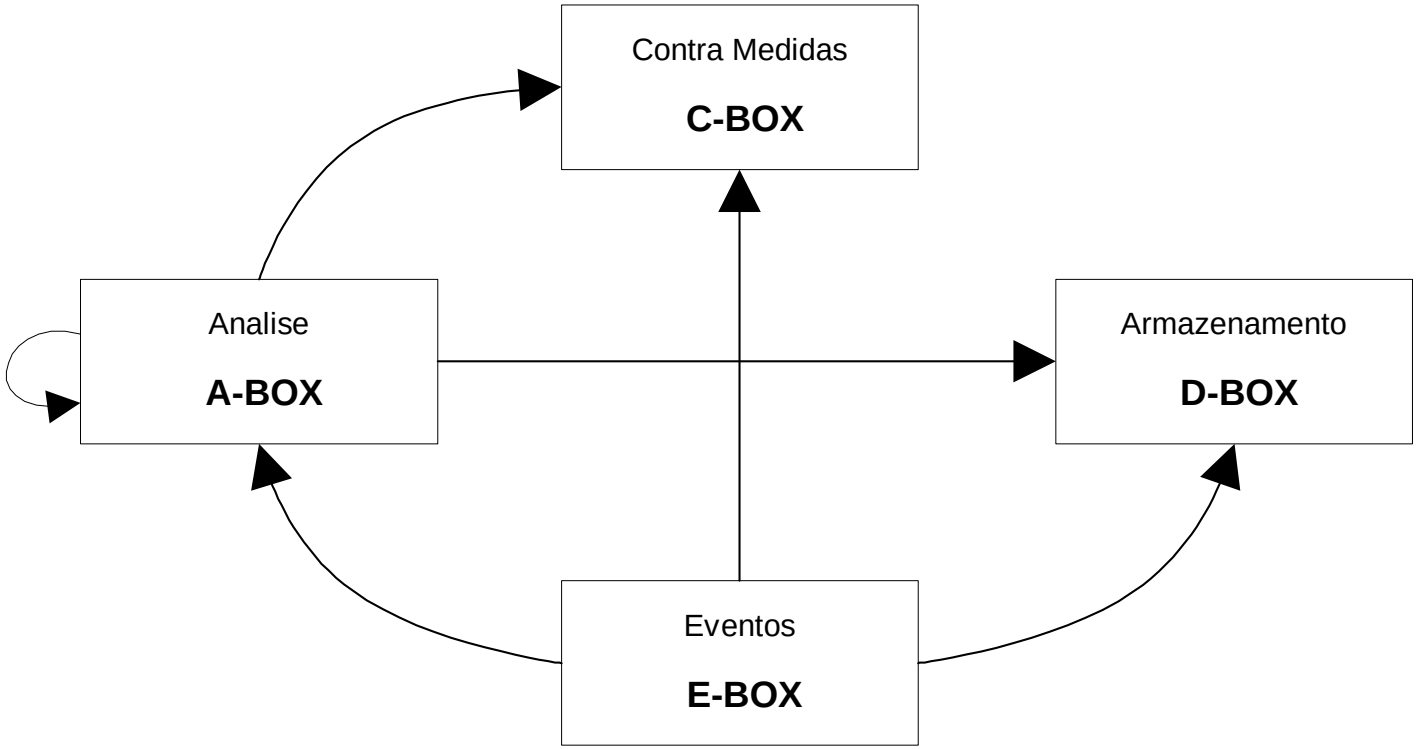
- Estabelecimento da Política de Segurança
- Identificação de Ações Ilícitas
- Sistemas de Detecção de Intrusão
  - Automatização
  - Necessidade de Métodos Eficazes
  - Pesquisas na Área



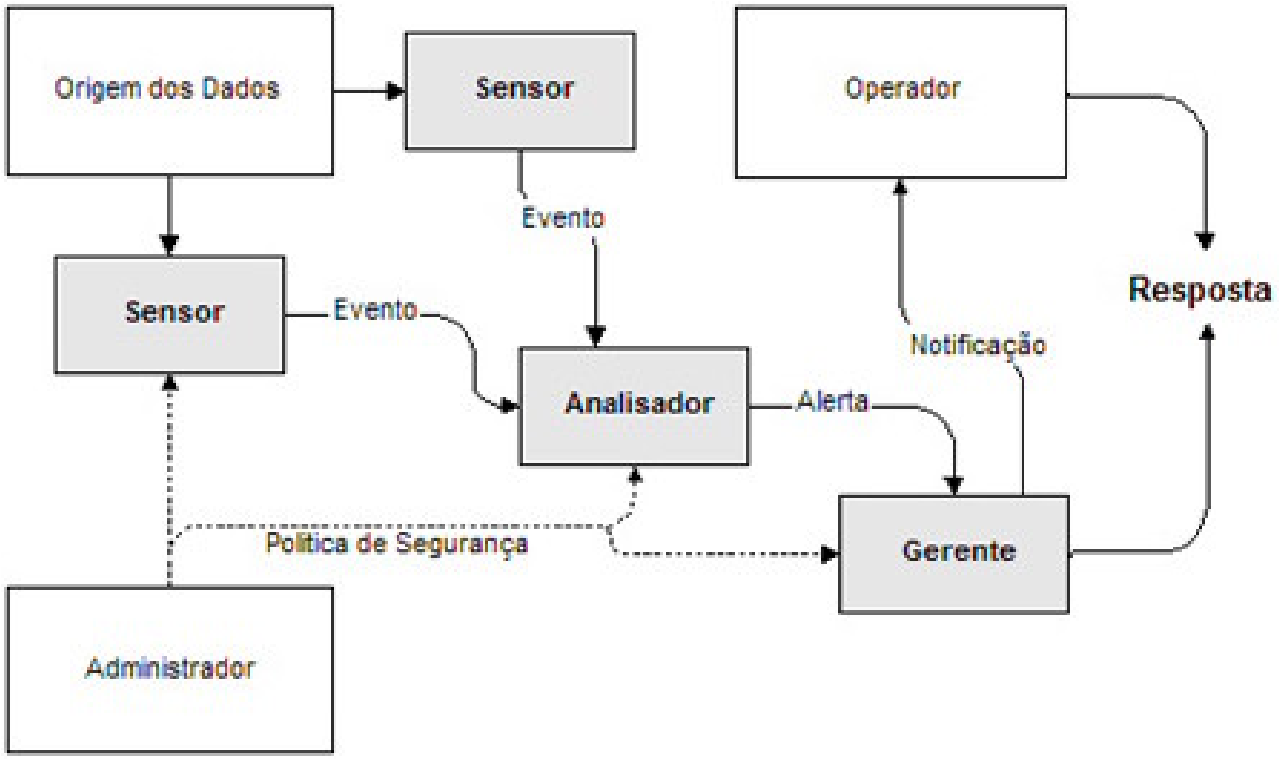
Padronização de IDS

- Geradores de Eventos
- Analisadores de Eventos
- Armazenamento
- Respostas

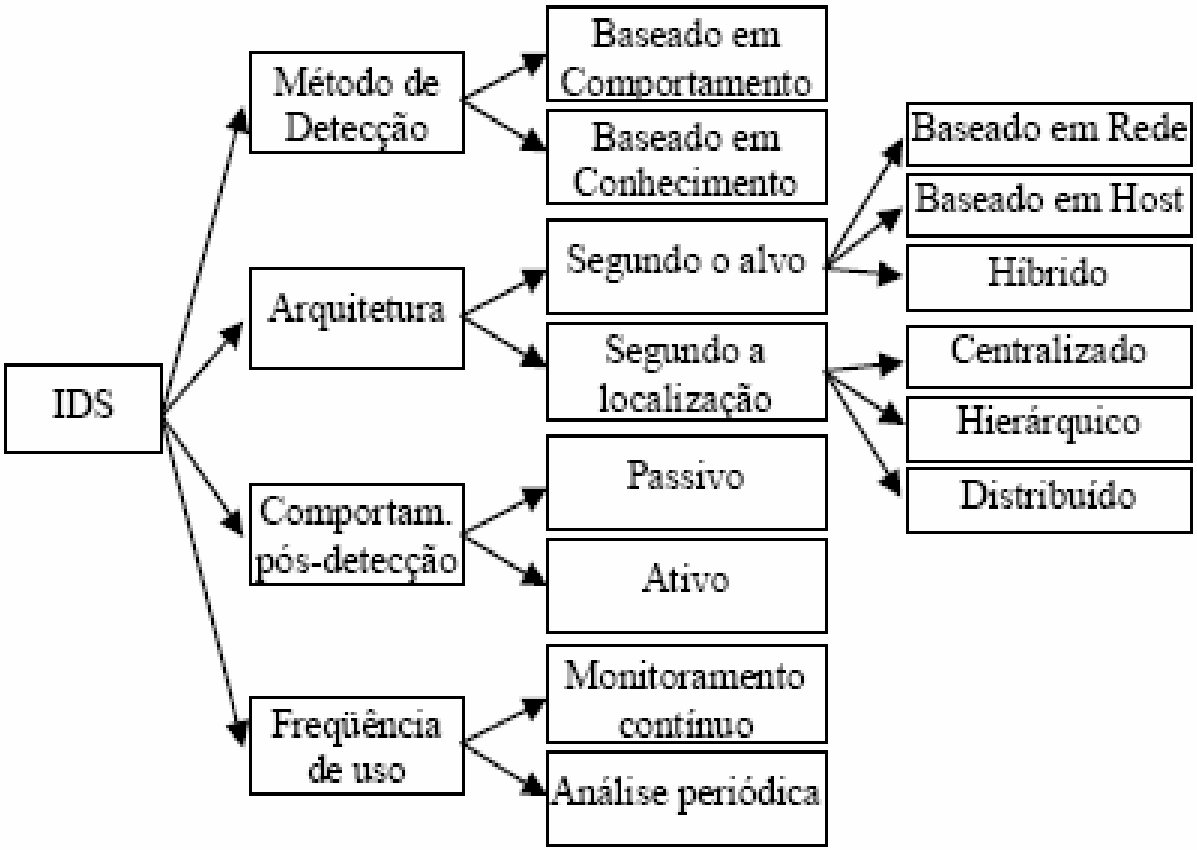
Padronização de IDS (CIDF)

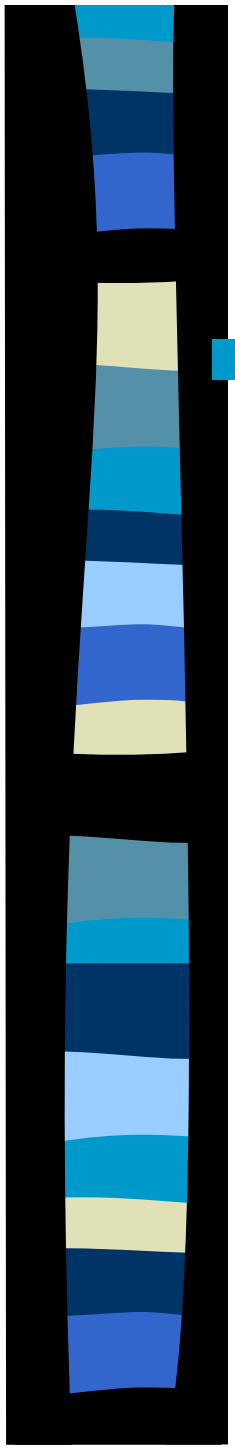


Padronização de IDS (IDWG)



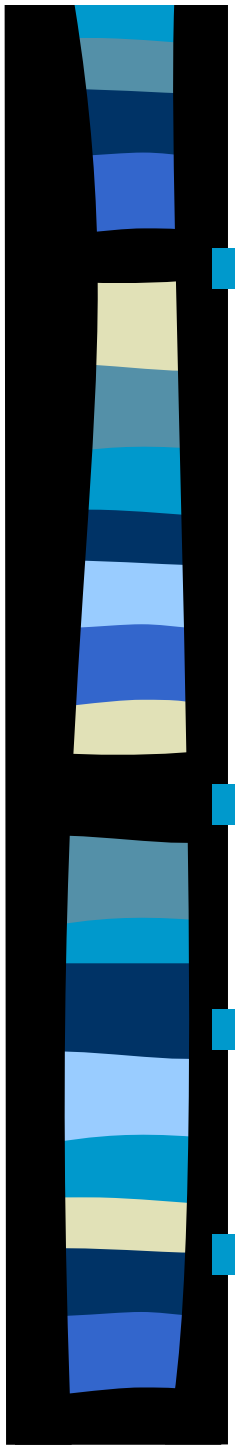
Classificação de IDS's





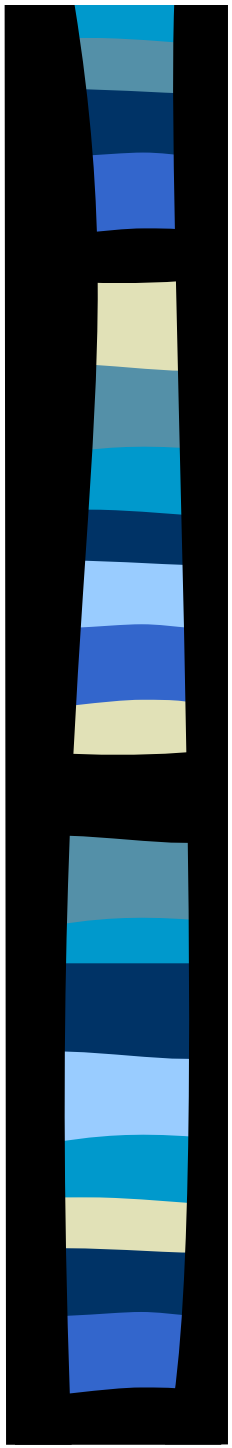
Classificação de IDSs

- Baseado em Comportamento (Anomalia)
  - Estabelecimento de Conjuntos de Atividades
  - Identifica Ataques Desconhecidos
  - Técnicas Computacionais Aplicadas
  - Classes de Eventos Gerados:
    - Falsos Positivos
    - Falsos Negativos
    - Verdadeiro Negativo
    - Verdadeiro Positivo

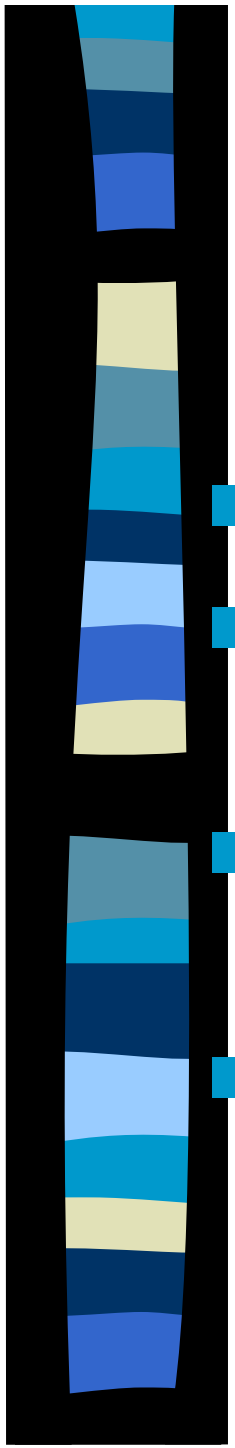


Classificação de IDSs

- Baseado em Conhecimento (Assinaturas)
  - Conjunto Conhecido e Pré-definido
  - Ineficaz para Novos Tipos de Ataque
  - Baixos Índices de Falsos Positivos e Falsos Negativos
- Arquitetura Baseada em *Host,* Rede e Híbrido
- Arquitetura Centralizada, Hierárquica e Distribuída
- Comportamento e Freqüência

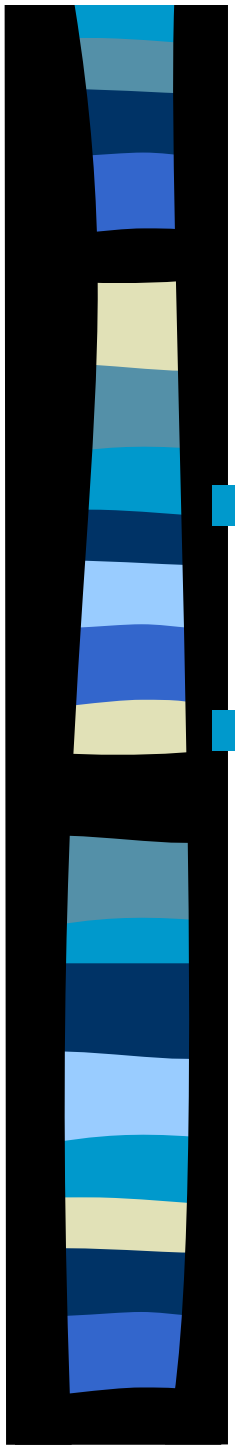


Abordagem Baseada em Imunologia Computacional e Agentes Móveis



Segurança de Redes/Sistemas Imunológicos Artificiais

- Sistemas Imunológicos Artificiais
- Paralelos com o Problema da Segurança em Rede
- Analogia estabelecida em 1987 (vírus de computador)
- Conexão entre Imunologia e Segurança a partir de 1994



Segurança de Redes e Sistemas Imunológicos

- Atualmente Aplica-se Princípios Sistema de Defesa do Corpo Humano
- Principais Características:
  - Detecção por Anomalia
  - Plano de Respostas Especializado
  - Contra-ataque
  - Memorização e Adaptação

Paradigma de Agentes Móveis

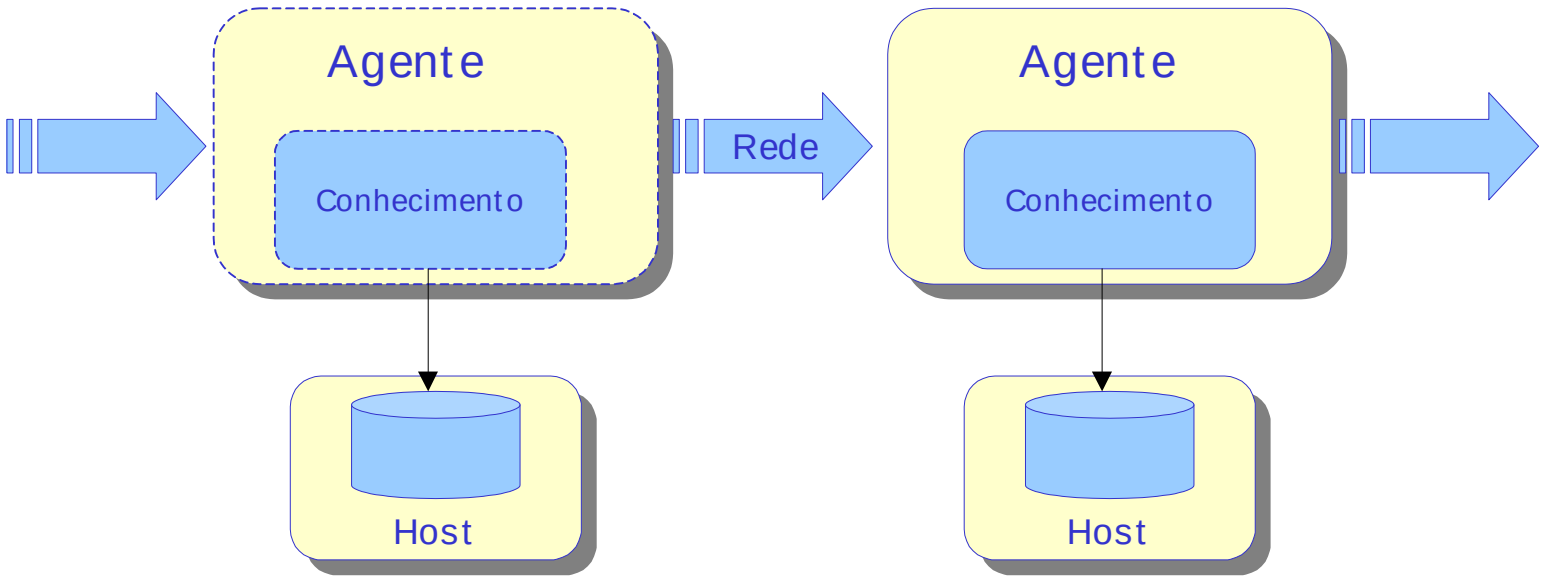
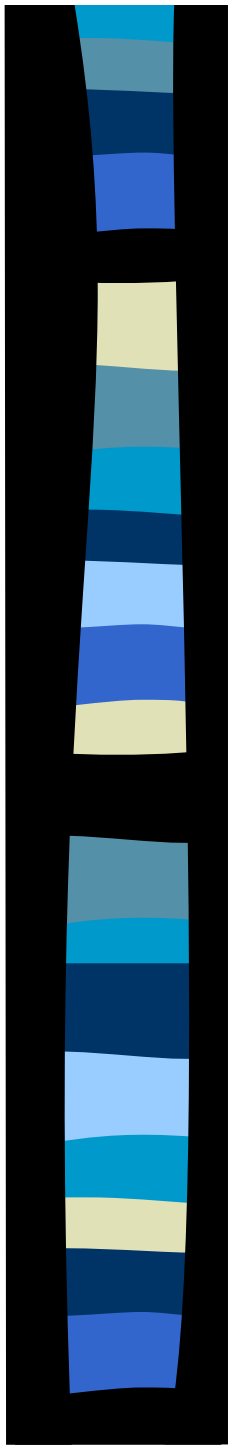
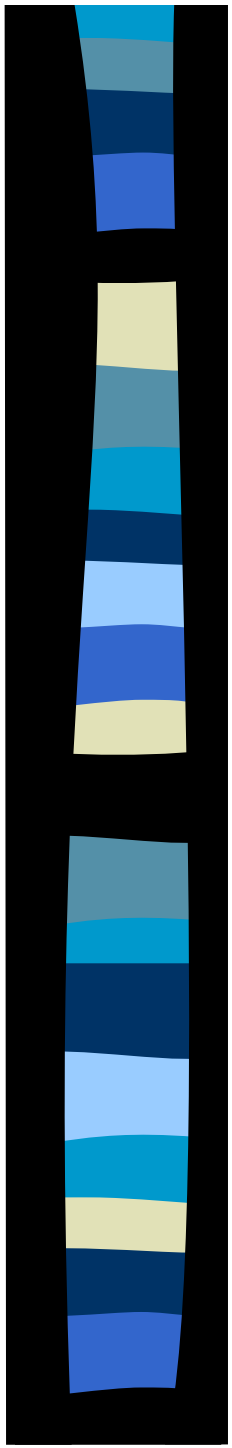


Figura 4.3 - Arquitetura de Agentes Móveis



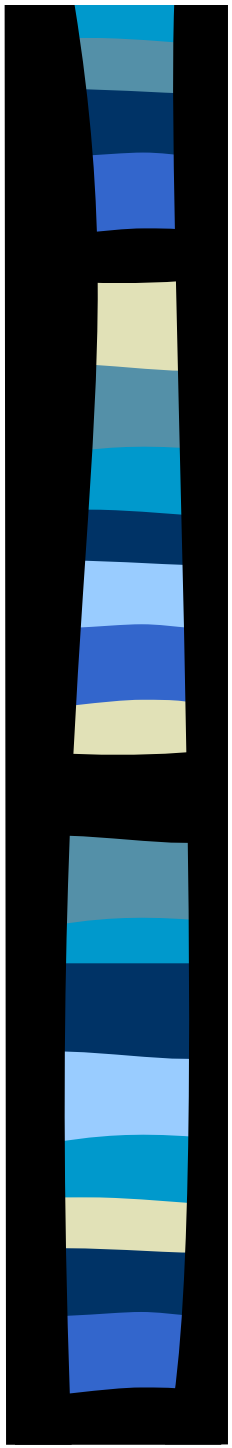
Agentes Móveis

"*Agentes itinerantes são programas que são despachados de um computador de origem, viajam entre servidores em uma rede até que se tornem hábeis para completar a sua tarefa; eles movem processos que progressivamente executam tarefas se movendo de um lugar para outro*" (CHESS, 1995).



Agentes Móveis

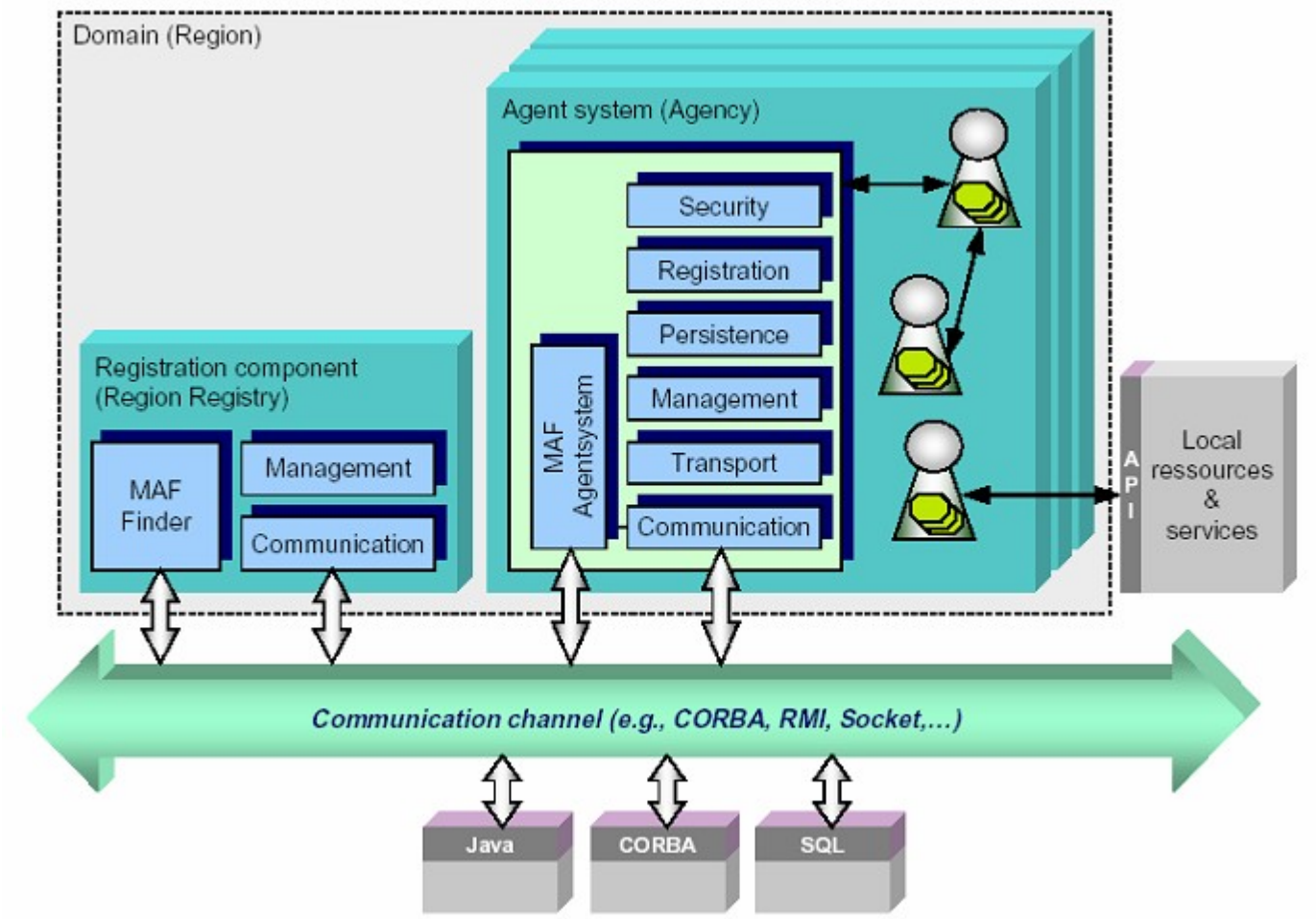
- Delegação
- Comunicação
- Mobilidade
- Ambientes de Execução
- Segurança
- Tolerância à Falhas
- Interoperabilidade.

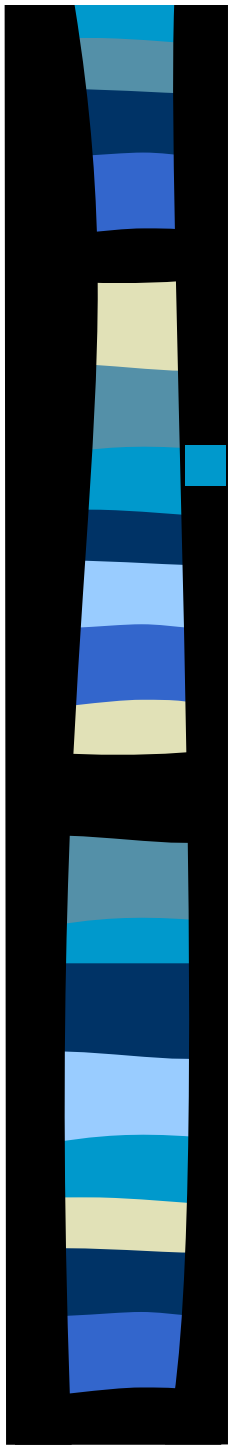


Agentes Móveis - MAF

- Região
- Sistema de Agentes (Agências)
- Place
- Agente
- Codebase

Agentes Móveis - MAF

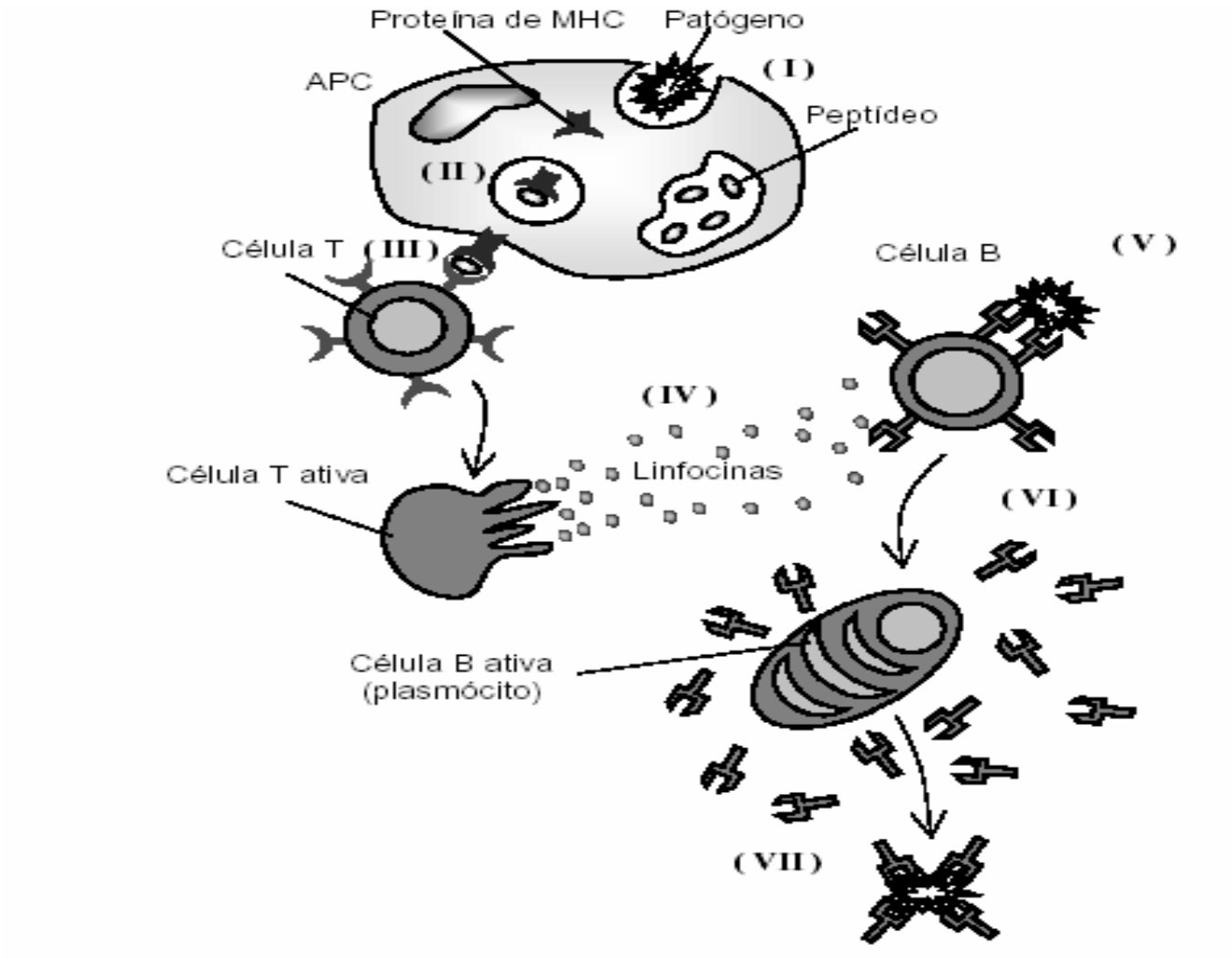


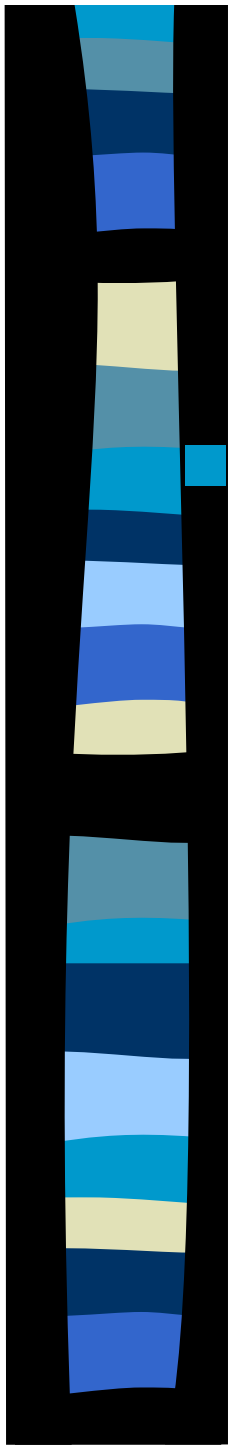


Um IDS Baseado em SIA e Agentes Móveis

- Requisitos Implementados
  - Funções do Modelo CIDF
  - Método de Detecção por Anomalia
  - Arquitetura Distribuída e Baseada em Host
  - Funcionamento em Tempo Real
  - Geração de Respostas Ativas e Passivas

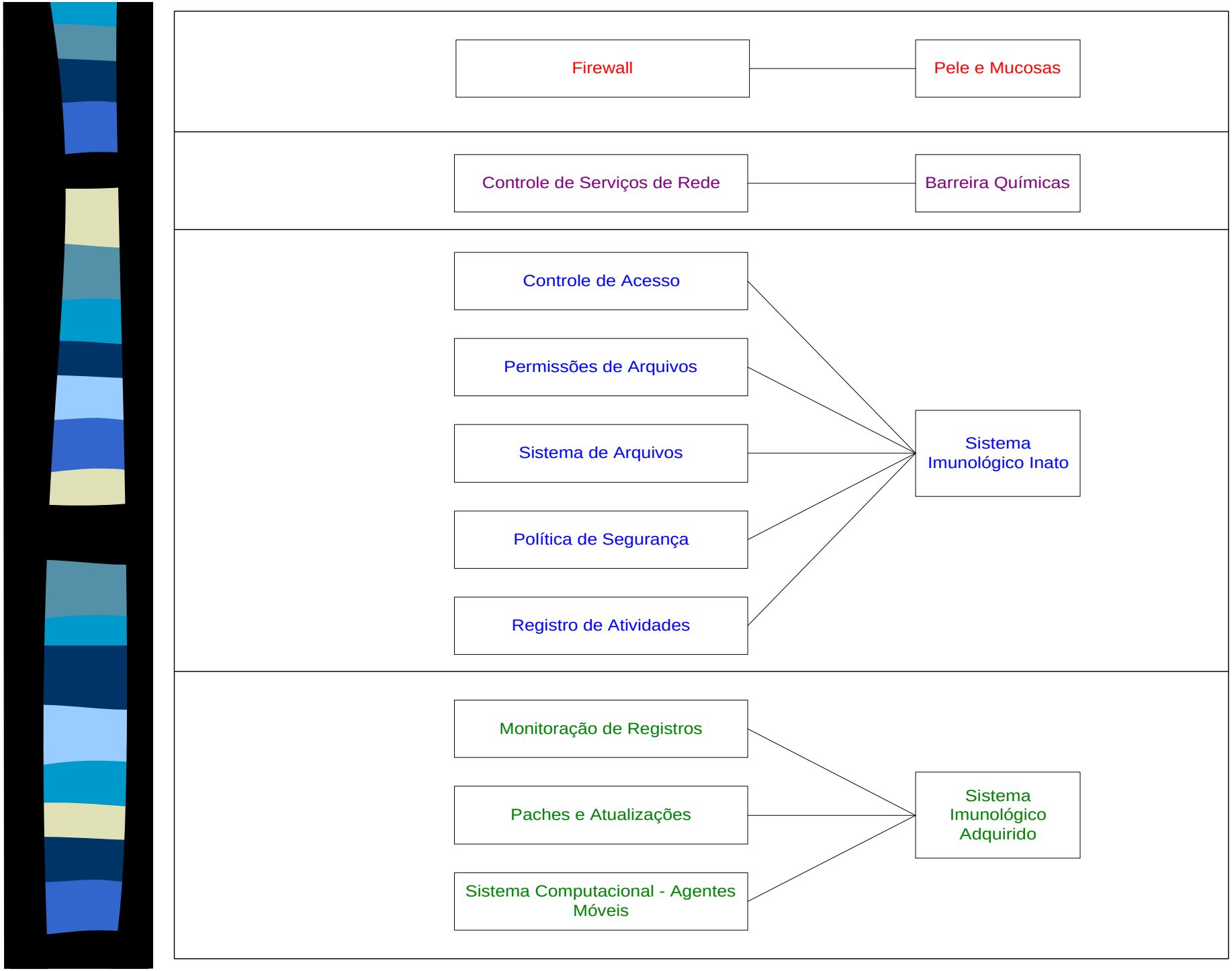
Inspiração no Sistema Imunológico Humano

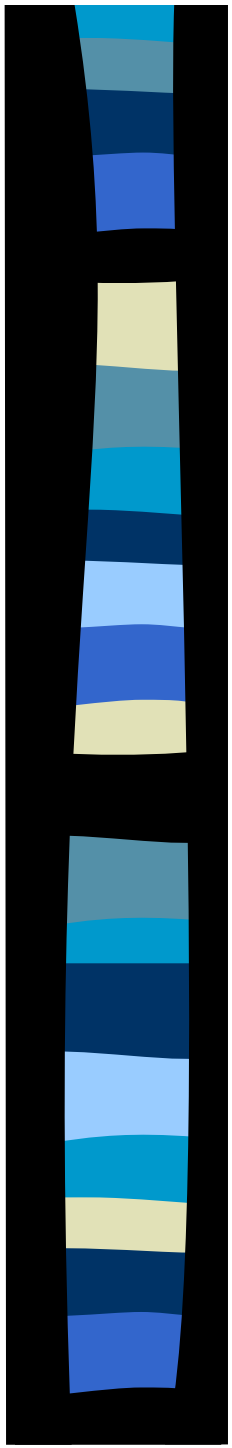




Sistema Imunológico Artificial

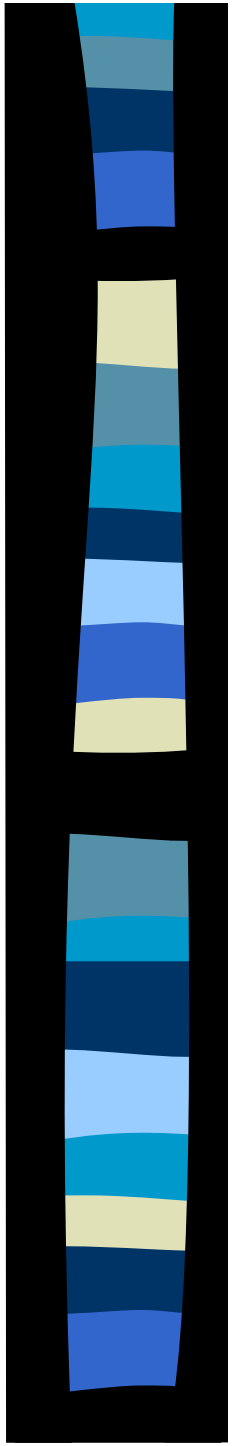
- Arquitetura Protegendo uma Rede Confiável de Computadores
  - Rede = Organismo
  - Servidor = Órgão
  - Processos Monitorados = Células

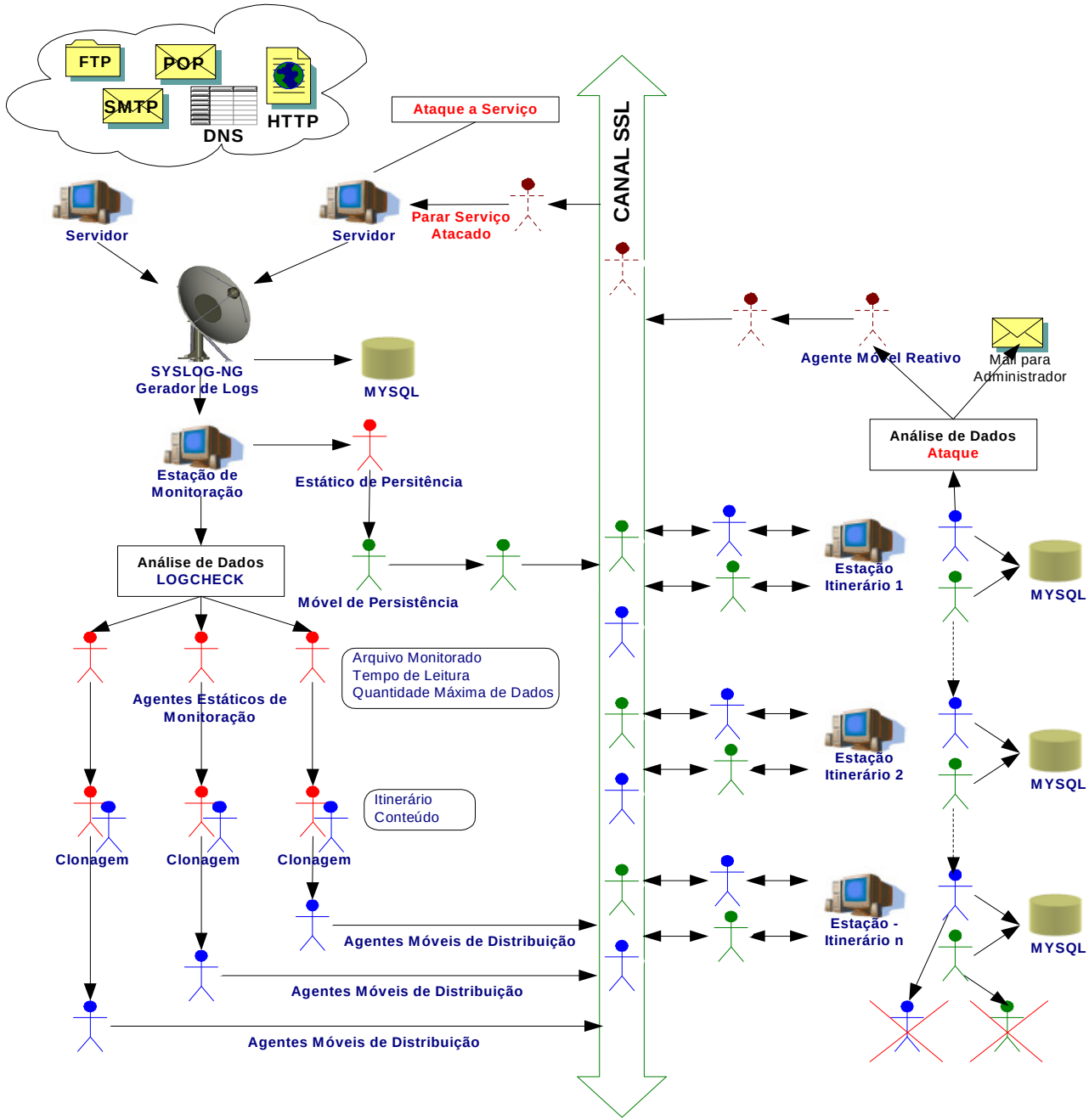

Firewall
Pele e Mucosas
Controle de Serviços de Rede
Barreira Químicas
Controle de Acesso
Permissões de Arquivos
Sistema de Arquivos
Política de Segurança
Registro de Atividades
Sistema Imunológico Inato
Monitoração de Registros
Paches e Atualizações
Sistema Computacional - Agentes Móveis
Sistema Imunológico Adquirido



Propriedades Imunológicas Adotados

- Detecção
- Diversidade
- Aprendizagem
- Tolerância

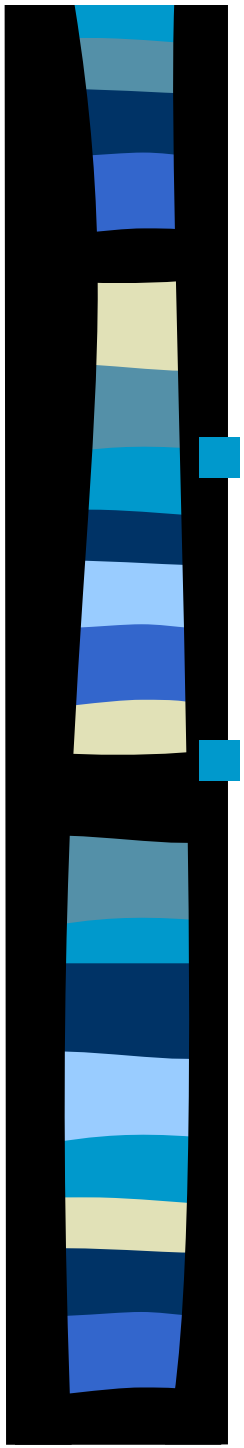



FTP
POP
SMTP
DNS
HTTP
Ataque a Serviço
Servidor
Servidor
Parar Serviço Atacado
CANAL SSL
SYSLOG-NG Gerador de Logs
MYSQL
Agente Móvel Reativo
Mail para Administrador
Análise de Dados Ataque
Estação de Monitoração
Estático de Persitência
Análise de Dados LOGCHECK
Móvel de Persistência
Estação Itinerário 1
MYSQL
Arquivo Monitorado
Tempo de Leitura
Quantidade Máxima de Dados
Agentes Estáticos de Monitoração
Estação Itinerário 2
MYSQL
Itinerário
Conteúdo
Clonagem
Clonagem
Clonagem
Estação - Itinerário n
MYSQL
Agentes Móveis de Distribuição
Agentes Móveis de Distribuição
Agentes Móveis de Distribuição

Serviços Monitorados

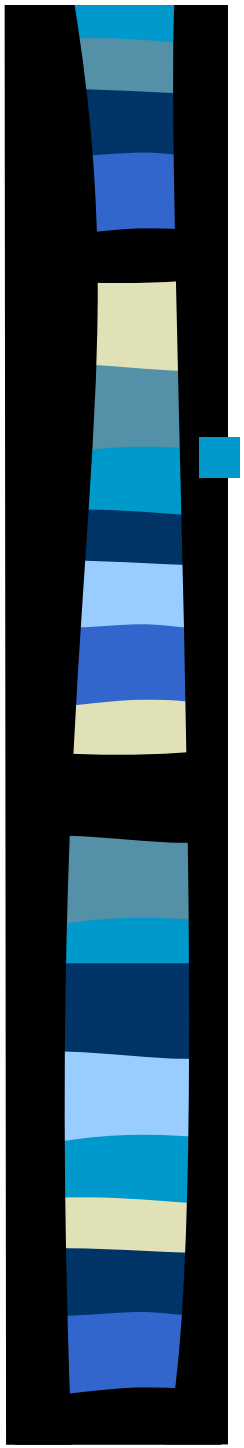
DNS, FTP, HTTP, POP3, SMTP
(Células Expostas aos Antígenos)

Sat Feb 28 09:54:50 2004 0 200.195.169.253 51478 /home/eder/arc_5.21e-5_i386.deb b _ i r eder ftp 0 * c
May 23 06:37:42 orgao named[10247]: unrelated additional info 'prioritytravel.com' type A from [64.74.96.242].53
[Thu Apr 22 10:41:15 2004] [error] [client 200.150.211.66] request failed: error reading the headers
Apr 10 00:23:13 email vpopmail[4660]: vchkpw: vpopmail user not found lidiest@foz.net:201.3.96.18



Detecção e Análise

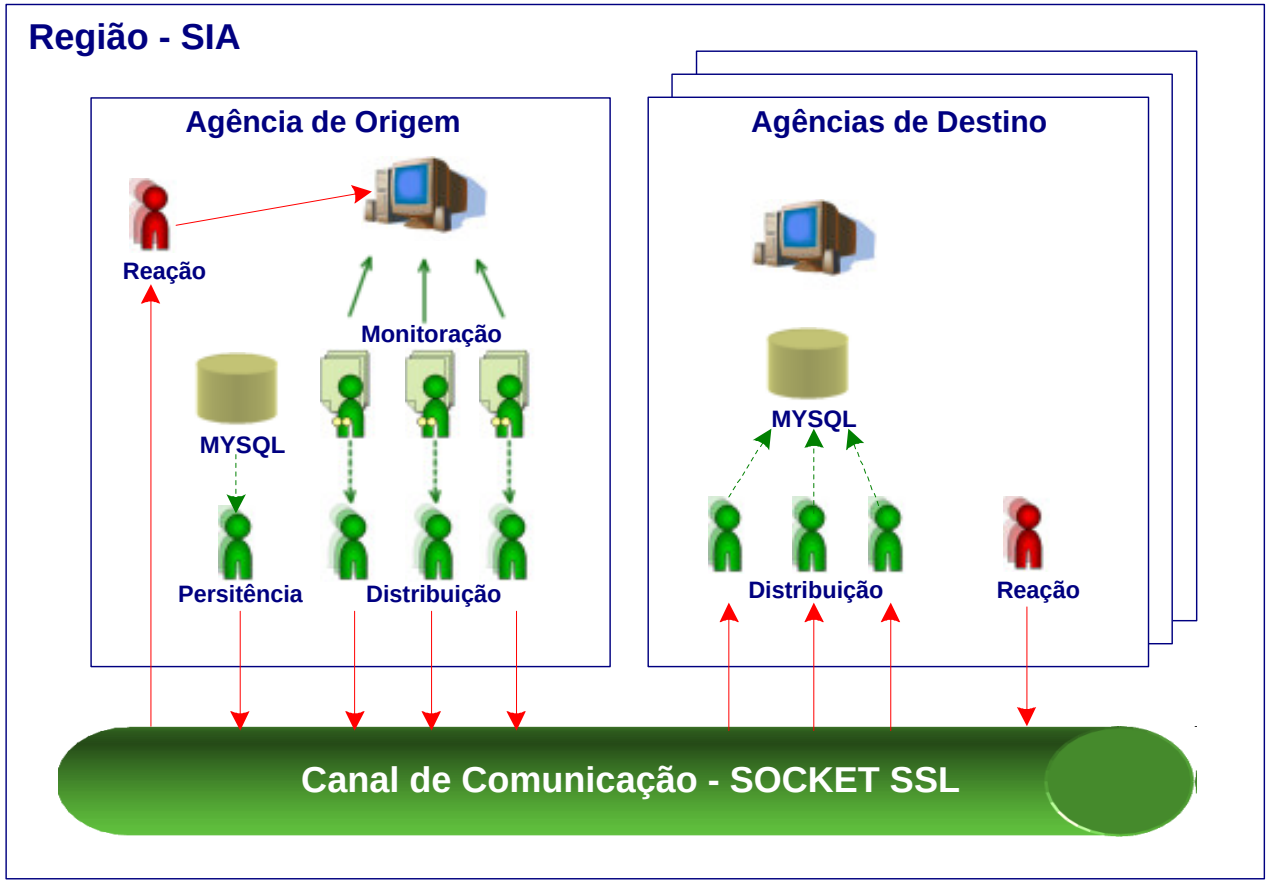
- **SYSLOG-NG - Detectores de Eventos (Macrófago)**
  - Ambiente Distribuído
- **LOGCHECK – Analisador de Eventos** (Célula T-Helper)
  - Logcheck.hacking
  - Logcheck.violations
  - Logcheck.violations.ignore
  - Logcheck.ignore

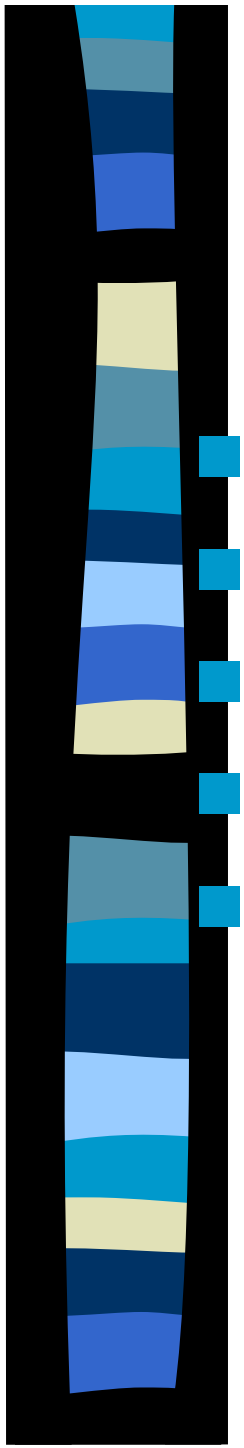


Detecção e Análise

- **LOGCHECK – Analisador de Eventos** (Célula T-Helper)
  - Atividades de Cracking
  - Violações de Segurança
  - Eventos de Segurança

Sistemas de Agentes(Linfócitos)

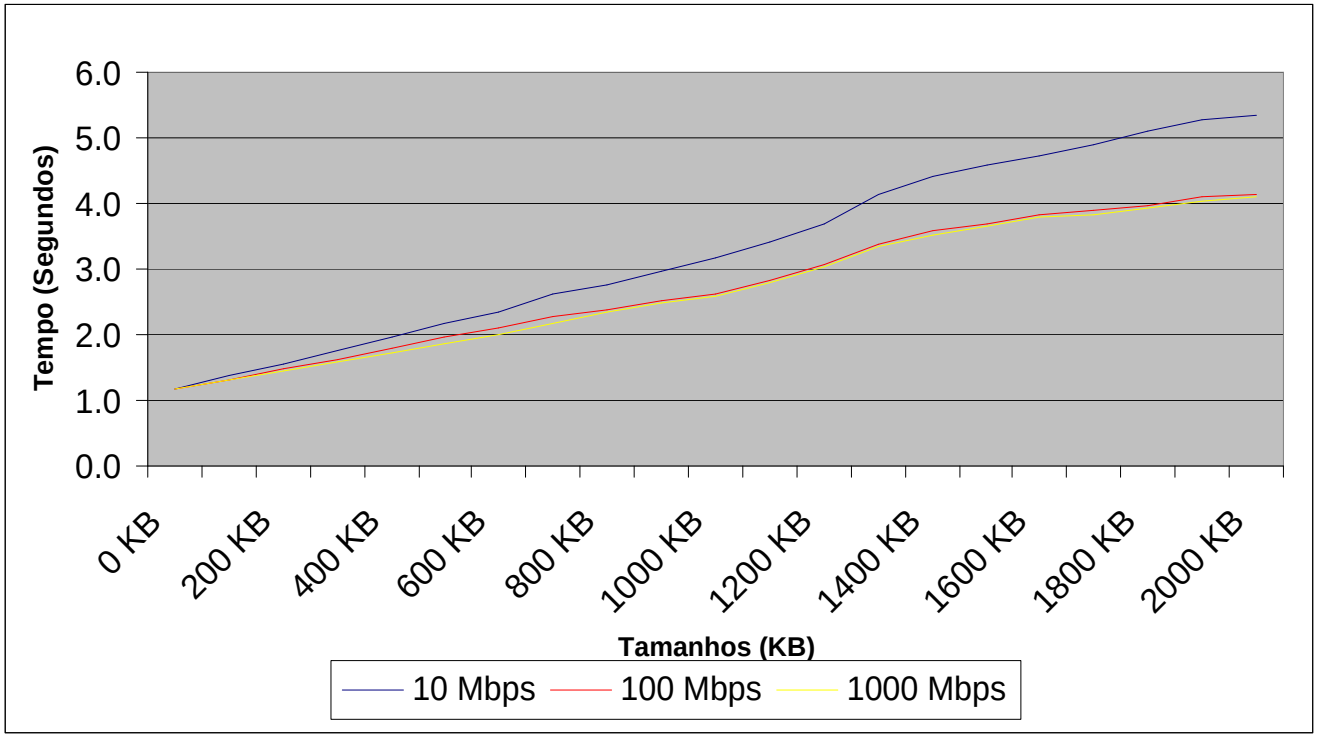




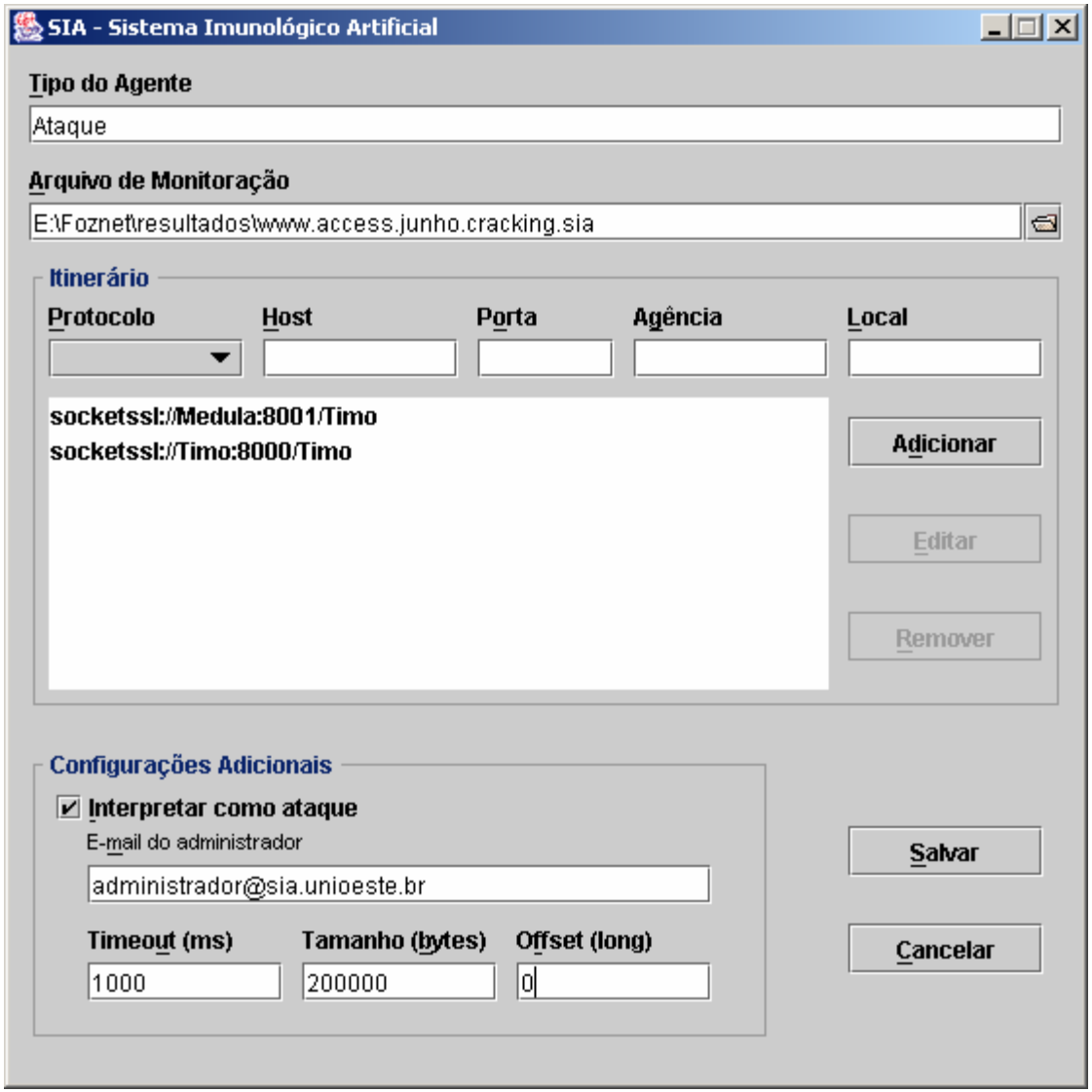
Classes de Agentes

- Monitoração (Células B)
- Distribuição (Células Plasma)
- Persistência (Robustez Imunológica)
- Reativos (Anticorpos)
- Banco de Dados (Memória Imunológica)

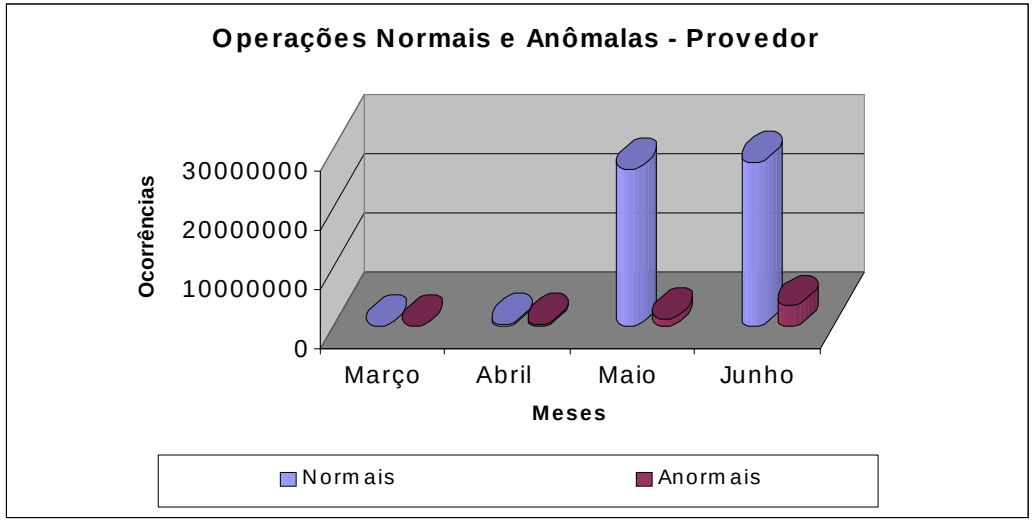
Performance dos Agentes

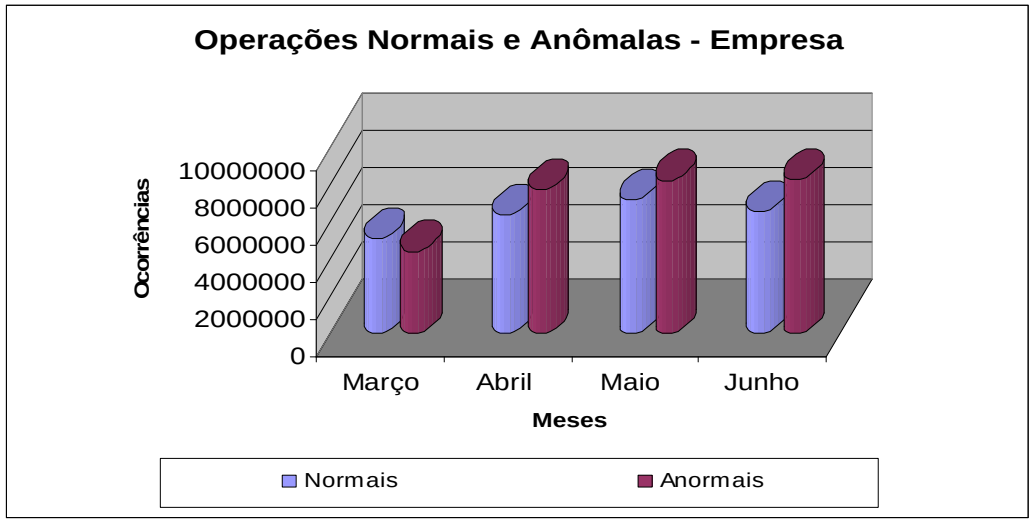


Configuração do Sistema



Estudos de Caso



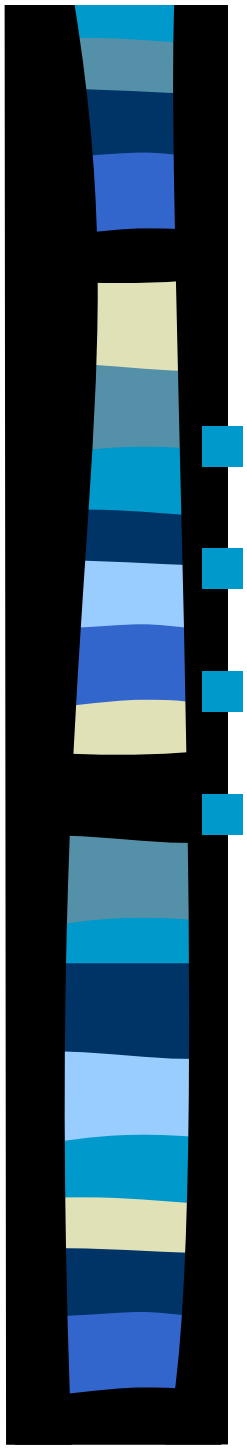


Contribuições

- Classificação dos eventos em normais e anormais
- Redução do número de registros reportados: 91,40% no Provedor e 46,87%
- Classificação dos Registros em Ataques, Violações e Eventos

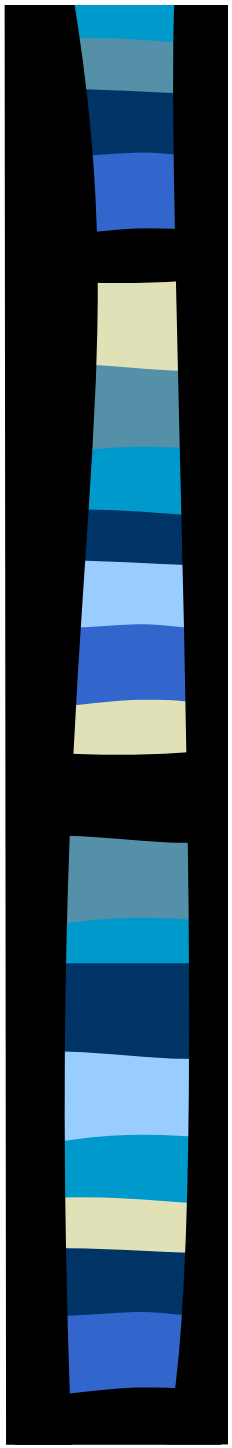
Contribuições

- Positivos Verdadeiros: 19,18% no Provedor e 5,33% na empresa
- Possibilidade de Realizar Estudos Estatísticos
- Mecanismos de Reação Pró-Ativos
- Estudo da Relação Segurança/Performance da Plataforma Grasshopper

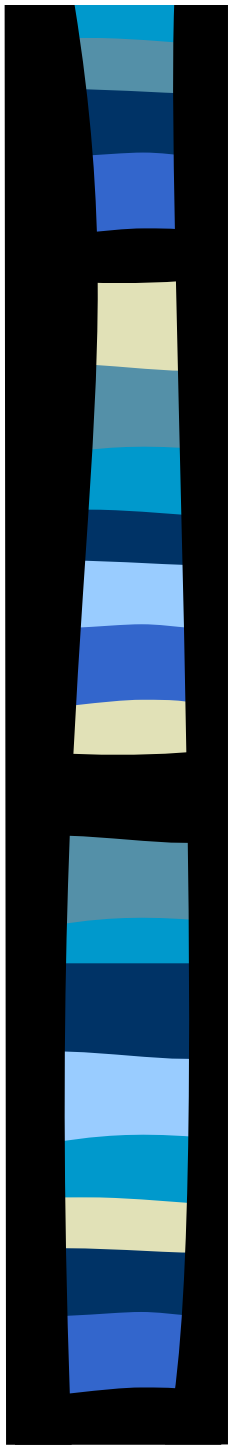


Considerações Finais

- Contribuições da Área de Pesquisa
- Otimização de Performance
- Contribuições do Estudo de Caso
- Projetos Futuros



Abordagem Baseada em Redes Neurais Artificiais

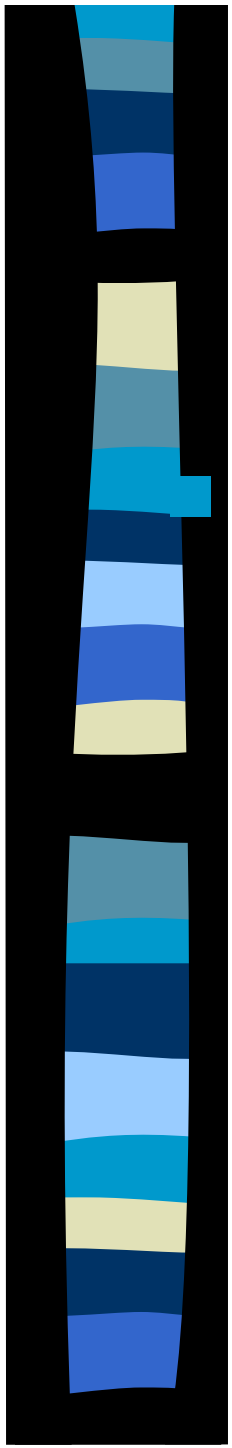


Roteiro

- Introdução
- Segurança de Redes
  - Detecção de Intrusão
- Inteligência Artificial
  - Reconhecimento de Padrões
- Modelo de um IDS Baseado em Redes Neurais Artificiais.

Segurança de Redes

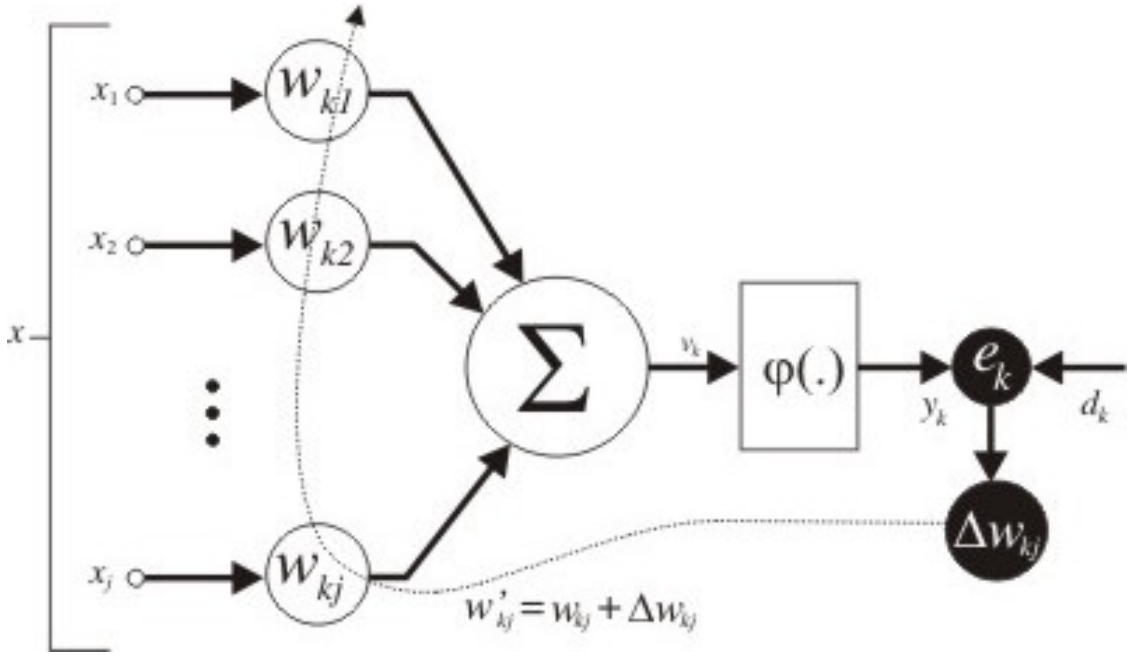
- **Dificuldades de IDS**
  - **Abuso ou Assinatura**
    - Novos Ataques
    - Variações do mesmo ataque
  - **Anomalia**
    - Altos índices de falsos positivos



Inteligência Artificial

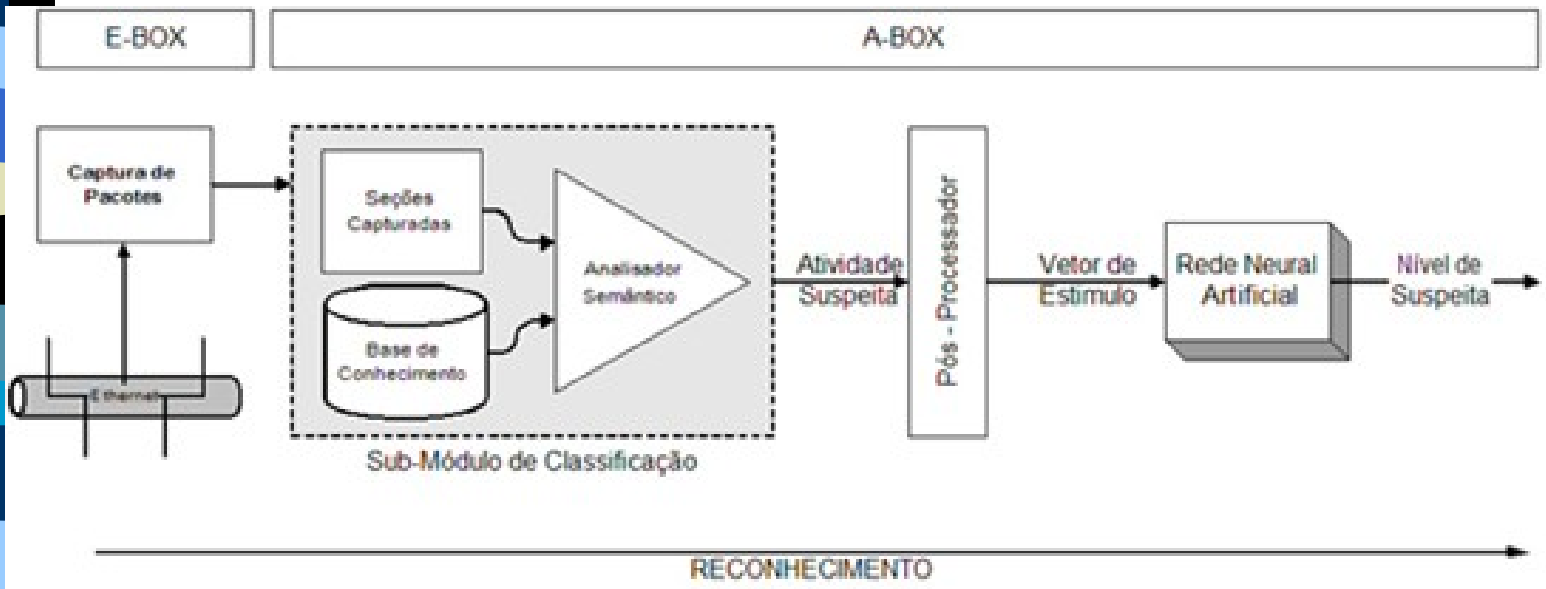
- Inspiração Biológica
  - Aprendizado de Máquina
  - Conexionismo
  - Redes Neurais Artificiais
    - Reconhecimento de Padrões
    - Generalização

Treinamento



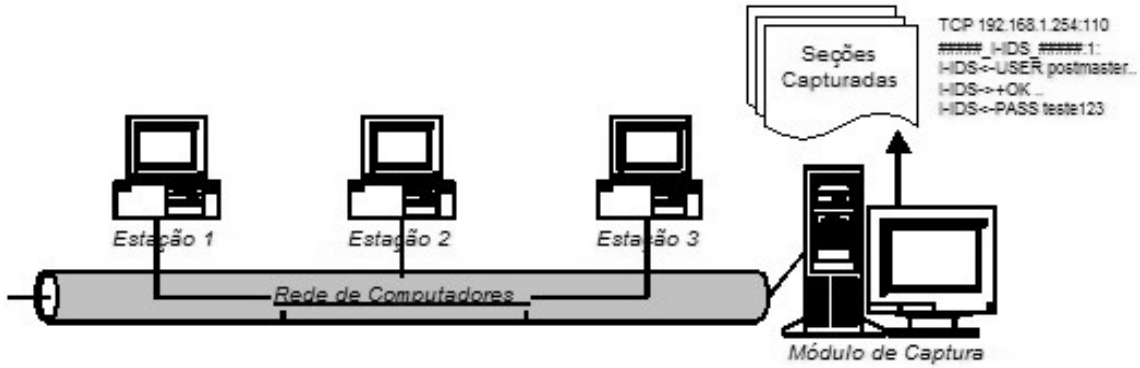
BackPropagation

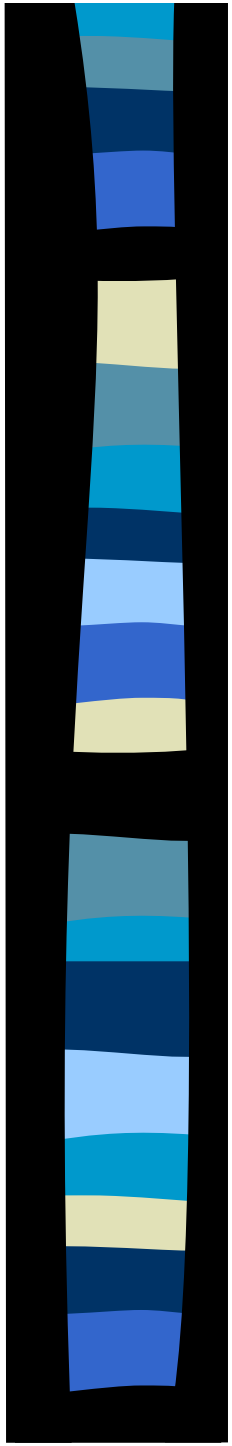
Modelo Neural de Detecção de Intrusos



Módulo de Captura

- Lib PCAP
- TCPDUMP / TCPFlow
- Estruturas na Memória e Geração de Arquivos por host.
- BroadCast (Modo Promíscuo)



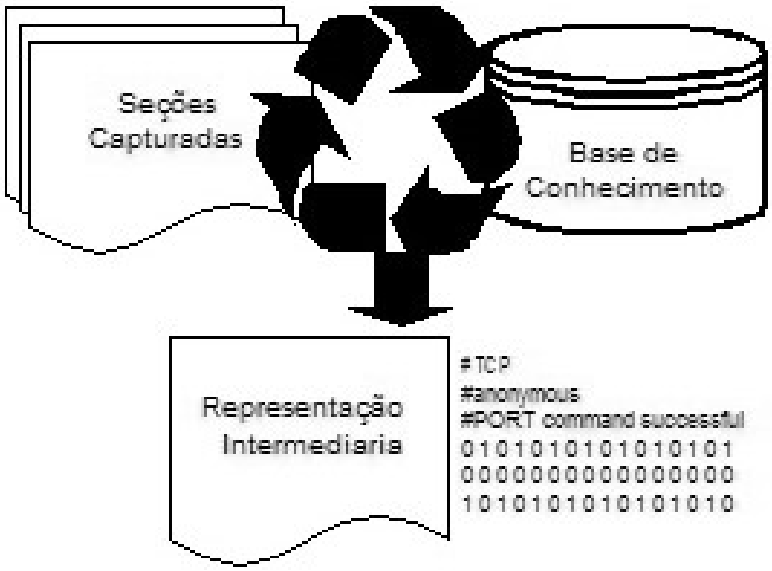


Exemplo de Seção Capturada

#####_I-IDS_#####
TCP 10.1.1.4:32772 -> 200.195.169.61:25
#####_I-IDS_#####:5:
I-IDS<-220 teste@foznet.com.br ESMTP Sendmail 8.7.5 ready
I-IDS->mail from " | /bin/mail mussoi@inf.ufsc.br < etc/passwd "
I-IDS<-250 " | /bin/mail mussoi@inf.ufsc.br < /etc/passwd ".
I-IDS<-.. sender ok.
I-IDS->rcpt tp: nobody
I-IDS<-250 Recipient ok.
I-IDS<-354 Enter mail, end with "." on a line by itself
I-IDS->data
I-IDS<-250 QAA23003 Message accept for delivery
I-IDS->quit
I-IDS<-teste@foznet.com.br closing connection
I-IDS:END

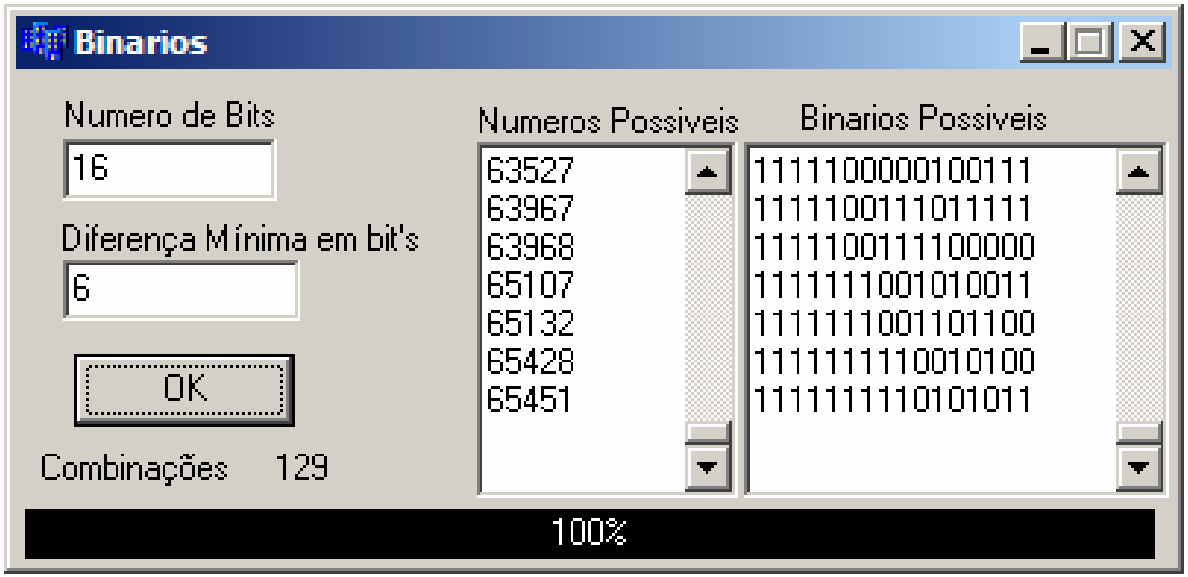
Analisador Semântico

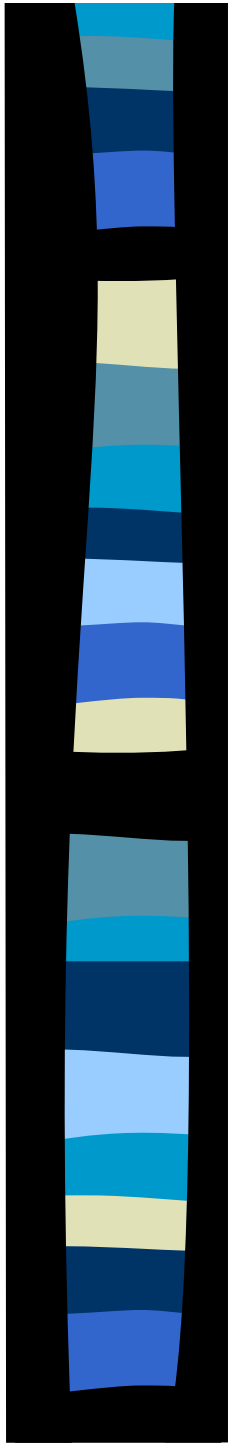
- Autômato Finito Simples
- Busca por Padrões entre as strings



Conversão de String p/ Binario

- 16 bits cada String
- Máximo de 16 Strings por seção
- Distância de Hamming
- Gerador de Binários





Base de Conhecimento

1 /etc/passwd
2 /etc/shadow
3 /etc/network/interfaces
4 /etc/fstab
5 rmdir
6 wget
7 Entering Passive Mode
8 nobody
9 command successful
10 |ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff|
11 |90 90 90 90 90 90 90 90 90|

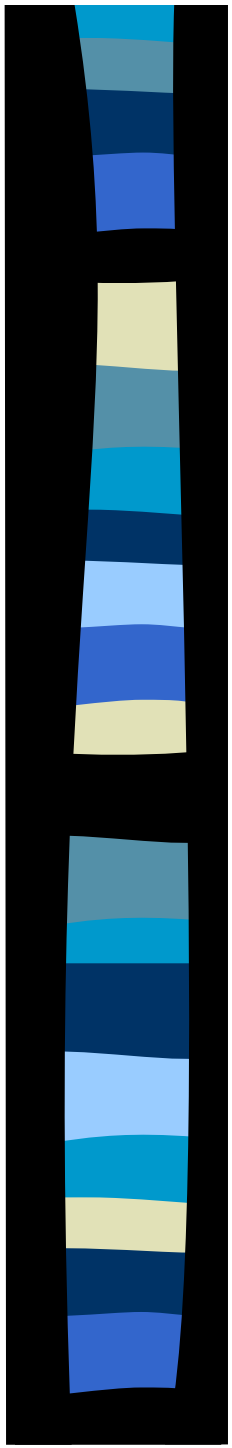
LBC

1 0000011001001010
2 0000011001110101
3 0000011110001101
4 0000011110110010
5 0000101010010100
6 0000101010101011
7 0000101101010011
8 0000101101101100
9 0000110011011111
10 0000110011100000
11 0000110100011000

Lista de Apoio

21 0000000011111110
23 0000111100001110
80 0000111111110001
53 0011001100110010

Portas



Representação Intermediária

- #6:6
- #TCP
- #25
- #| mail
- #sleep 2 ; echo quit
- #Syntax Error
- #| mail
- #sleep 2 ; echo quit
- #Invalid sender address
- 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
- 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0
- 0 1 0 1 1 1 0 1 1 0 1 1 0 0 0 1
- 0 0 0 0 0 1 1 1 1 0 0 0 1 1 0 1
- 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0
- 0 1 0 1 1 1 0 1 1 0 1 1 0 0 0 1
- 0 0 0 0 0 1 1 1 1 0 0 0 1 1 0 1
- 0 0 0 0 1 1 0 0 1 1 1 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

16 x 16

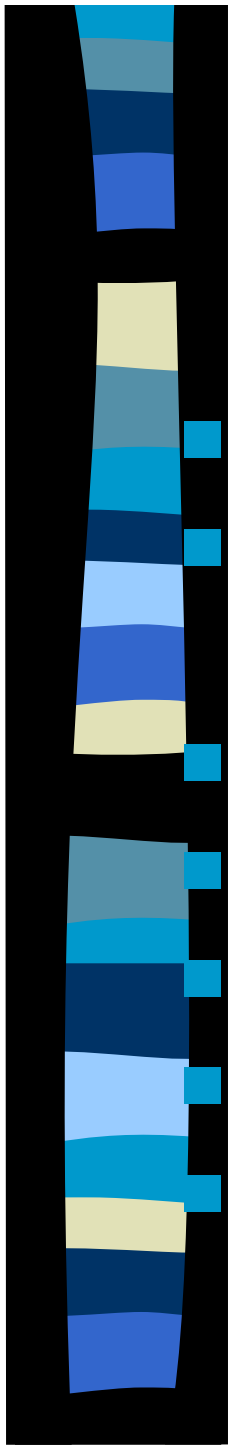
256 bits

Pós Processamento

- Transformação da representação intermediaria em

VETOR DE ESTIMULO

para a Rede Neural MLP-256-21-1



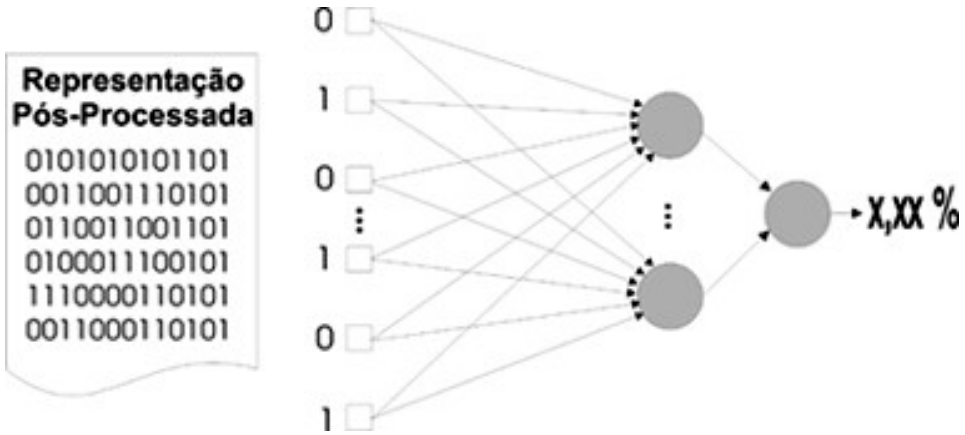
Rede Neural

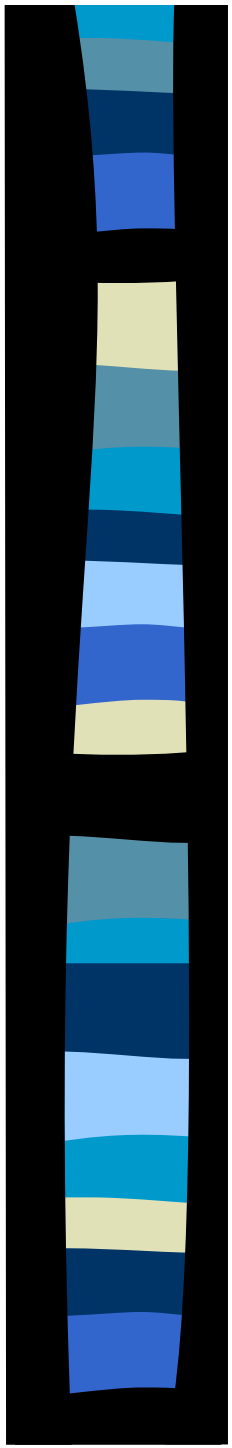
- Simuladores de Redes Neurais
- Biblioteca (neuro.h)

- MultiLayer Perceptron
- BackPropagation
- Função de ativação Tangente Hiperbólica
- Limiar de -1 a 1
- 256 – 21 – 1

Análise Neural

- Entrada
  - Representação Binária das seções suspeitas
- Saída
  - Nível de Suspeita (entre –1 e 1)





Definição de Padrões

Ataque

- Ferramentas de Ataque e Exploração
- Reprodução de Técnicas Documentadas
- Padrões ACME / UNESP

- Não Ataque
  - Monitoria de Atividades Normais
  - Simples Utilização de Serviços

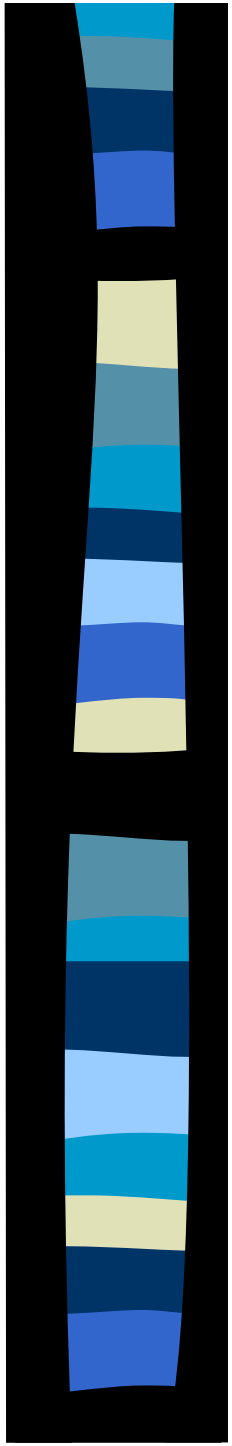
Experimentos

Porta	Seções Intrusivas	Seções Normais	Total
21	30	30	**60**
23	20	20	**40**
25	12	12	**24**
53	07	07	**14**
80	30	30	**60**
8080	06	06	**12**
Total Geral	**105**	**105**	**210**

Experimentos

Porta	Treinamento			Testes			Total
	Ataque	*Normal*	*Total*	*Ataque*	*Normal*	*Total*	
21	*23*	*23*	***46***	*07*	*07*	***14***	**60**
23	*15*	*15*	***30***	*05*	*05*	***10***	**40**
25	*09*	*09*	***18***	*03*	*03*	***06***	**24**
53	*05*	*05*	***10***	*02*	*02*	***04***	**14**
80	*23*	*23*	***46***	*07*	*07*	***14***	**60**
8080	*05*	*05*	***10***	*01*	*01*	***02***	**12**
Total Geral	***80***	***80***	***160***	***25***	***25***	***50***	**210**

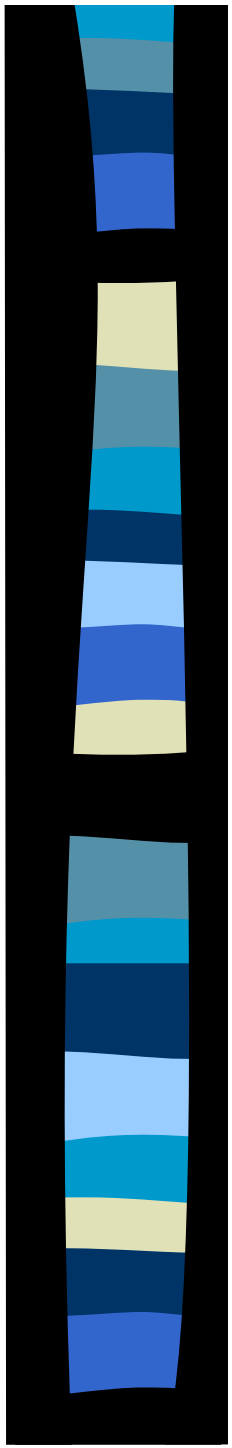
Formação Aleatória



Resultados

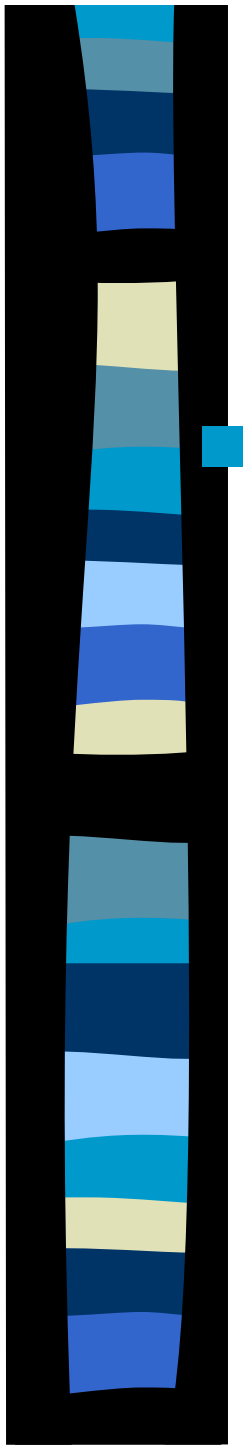
- Acertos de 100% sobre os padrões usados durante o treinamento.
- Acertos de ~= 75% sobre padrões não vistos durante o treinamento

- **Conjunto 1 : 24,52% de erro**
- **Conjunto 2 : 27,30% de erro**



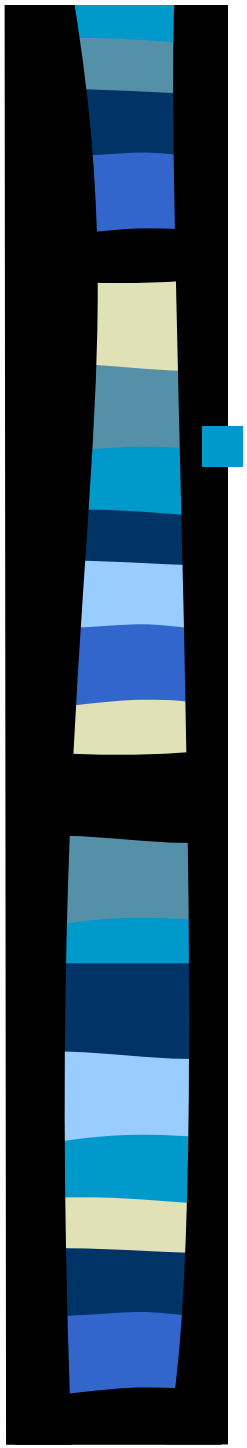
Conclusões

- Índices de Acertos Satisfatórios.
- Índice de Aceitação pode ser ajustado para controlar
  - Falsos Positivos e Falsos Negativos
- Problemas com Criptografia
- Problemas com Redes sem BroadCast



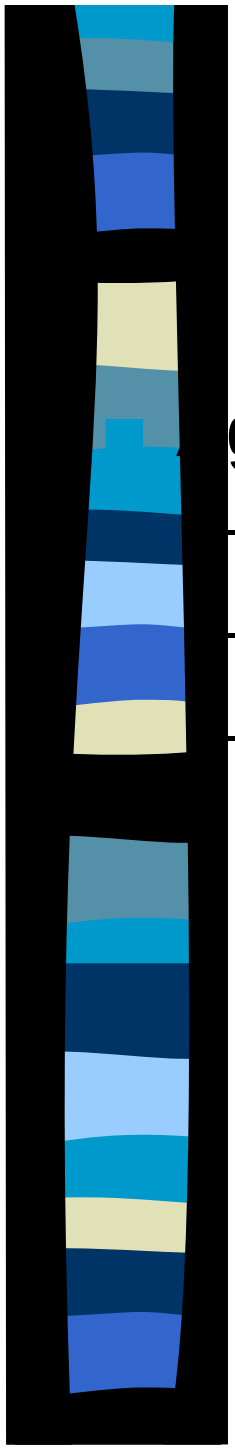
Links Importantes

- SIA:
  - *http://www.dca.fee.unicamp.br/~lnunes*
  - http://www.cs.kent.ac.uk/people/staff/jt6/aisbook/ais-researchers.htm
  - http://www.cs.unm.edu/~steveah/
  - http://mcb.harvard.edu/BioLinks.html



Links Importantes

- Segurança de Redes/Detecção de Intrusão
  - http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html
  - http://www.securitytechnet.com/security/ids-more.html
  - http://www.cerias.purdue.edu/coast/coast-library.html



Links Importantes

- gentes Móveis
  - http://www.cetus-links.org/oo_mobile_agents.html
  - http://have.itgo.com/index.html
  - http://www.agentland.com/Resources/9Research/Projects/more4.html