# 6
# Resultados

Os resultados obtidos com classificadores baseado em redes neurais MLP aqui desenvolvidos serão apresentados. O diagrama de Venn apresentado na figura 6.1 ilustra possíveis situações existentes no espaço de resultados dos modelos avaliado.

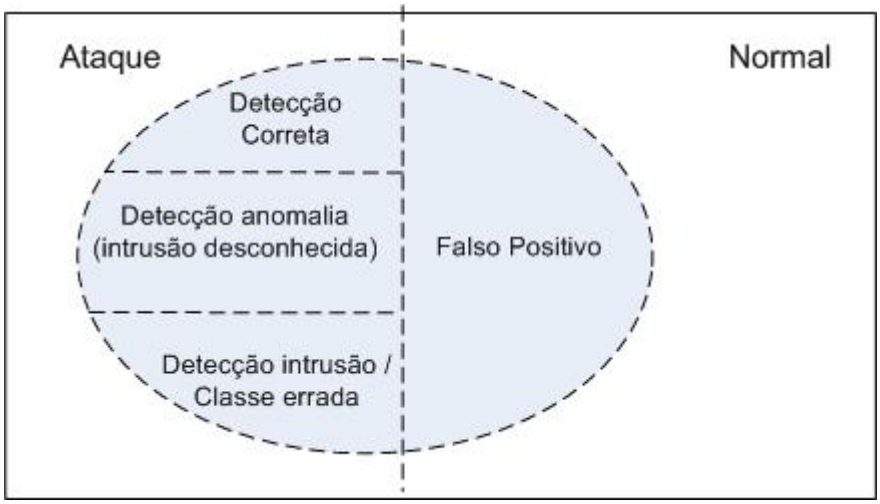


**Figura 6-1 – Diagrama Venn**

Os resultados obtidos serão apresentados através da matriz de confusão [35] gerada para cada classificador testado e da correspondente curva ROC – "*Receiver Operating Characteristics*".

## 6.1.
## Matriz de Confusão e Curvas ROC

A construção de uma matriz de confusão é uma técnica empregada para se analisar o desempenho de sistemas classificadores. A tabela 6.1 apresenta um exemplo de matriz de confusão para um classificador baseado em duas classes distintas.

| | | Previsto | |
|---|---|---|---|
| | | Negativo | Positivo |
| Real | Negativo | **a** | **b** |
| | Positivo | **c** | **d** |

**Tabela 6-1 : Exemplo de Matriz de Confusão**

Para esta matriz de confusão temos definidos os seguintes parâmetros :

- **a** corresponde ao número de previsões corretas que uma instância é negativa
- **b** corresponde ao número de previsões incorretas que uma instância é positiva
- **c** corresponde ao número de previsões incorretas que uma instância é negativa.
- **d** corresponde ao número de previsões corretas que uma instância é positiva.

Utilizando os parâmetros **a,b,c** e **d** podemos classificar os seguintes indicadores associados ao classificador em análise :

- 
- Precisão global (“*accuracy*” ou AC) corresponde a proporção de previsões corretas do classificador. É determinado pela equação :

$$AC = \frac{a+d}{a+b+c+d}$$

- Taxa de acerto (*recall* ou *True positive rate* - *TP*) é a proporção de casos positivos que foram corretamente identificados pelo classificador. É determinada pela equação :

$$TP = \frac{d}{c+d}$$

- A taxa de falso positivo (FP) consiste na proporção de casos negativos que foram incorretamente classificados como positivos. Determinada por :

$$FP = \frac{b}{a+b}$$

- A taxa de verdadeiro negativo (TN) consiste na proporção de casos negativos que foram corretamente classificados como tal. Determinada por :

$$TN = \frac{a}{a+b}$$

- A taxa de falso negativo (FN) é a proporção de casos positivos que foram incorretamente classificados como negativos. Dada por :

$$FN = \frac{c}{c+d}$$

- Finalmente a precisão ("*precision*" P) é a proporção de casos positivos que foram previstos corretamente dados por :

$$P = \frac{d}{b+d}$$



Adicionalmente, para cada sistema avaliado será apresentada a curva ROC (*Receiver Operating Characteristics*) tradicional associada a sua matriz de confusão. Curvas ROC são curvas que apresentam a taxa de verdadeiro positivo (TP) do sistema versus a taxa de falso positivo (FP) do sistema quando se varia um limiar de decisão/ajuste do classificador. Será empregado também uma variação da curva ROC utilizando a precisão (AC) versus taxa de falso positivo

Para redes neurais empregaremos curvas ROC para os cenários de classificação binária (saída identificando se conexão é normal ou intrusiva apenas). O limiar de decisão é variado de [-1;1] e todos os parâmetros são

recalculados. O resultado é uma matriz com os diversos parâmetros – AC,FP,FN,TP,TN e P – calculados para vários valores do limiar de decisão.

## 6.2. Classificador Binário

Para um classificador binário, capaz de distinguir se o padrão apresentado é um padrão de ataque ou um padrão normal, a saída da rede neural foi ajustada, no intervalo [-1 1] para gerar (–1) para padrão considerado intrusão e (1 ) para padrão considerado normal. As matrizes de confusão apresentadas consideram limiar de decisão *th* = 0. Para as redes com esta características efetuamos o treinamento com todas as possibilidades de entrada – todas as variáveis, apenas as características intrínsecas, apenas as características temporais, apenas as características especialistas – com o objetivo de avaliar qual grupo de características exerce maior influência no desempenho da rede. Foram avaliados os seguintes cenários.

### 6.2.1. Características intrínsecas como entrada

Apenas as nove variáveis associadas às características intrínsecas do TCP/IP foram utilizadas para treinar e avaliar as redes neurais. Redes MLP com duas camadas escondidas (10 neurônios escondidos por camada) foram treinadas com os cinco subconjuntos de treinamento e avaliadas com todos os registros da base de testes e avaliação.

## Conjunto de treinamento DS1

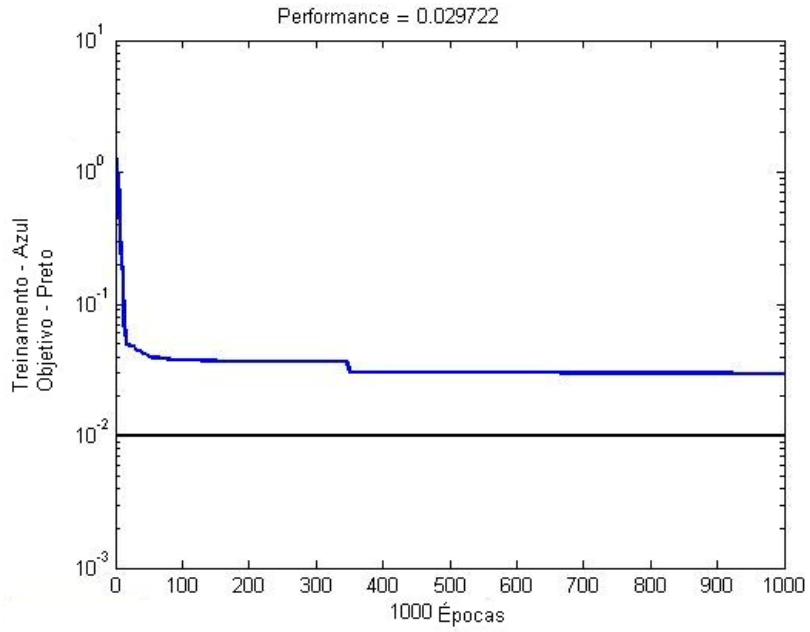


**Figura 6-2 : Treinamento 1. DS1**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60227 | 366 |
| | Intrusão | 24518 | 225918 |

**Tabela 6-2 : CM 1. DS1**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9200 |
| TP | 0.9021 |
| FP | 0.0060 |
| TN | 0.9940 |
| FN | 0.0979 |
| P | 0.9984 |

**Tabela 6-3 : Parâmetros 1. DS1**

## Conjunto de treinamento DS2

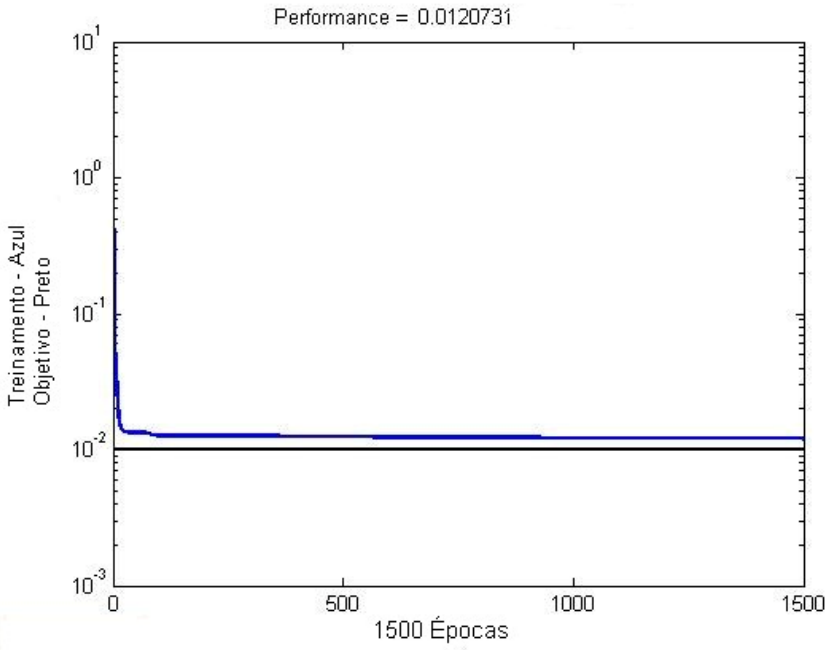


**Figura 6-3 : Treinamento 1. DS2**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60049 | 544 |
| | Intrusão | 24127 | 226309 |

**Tabela 6-4 : CM 1. DS2**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9207 |
| TP | 0.9037 |
| FP | 0.0090 |
| TN | 0.9910 |
| FN | 0.0963 |
| P | 0.9976 |

**Tabela 6-5 : Parâmetros 1. DS2**

## Conjunto de treinamento DS3

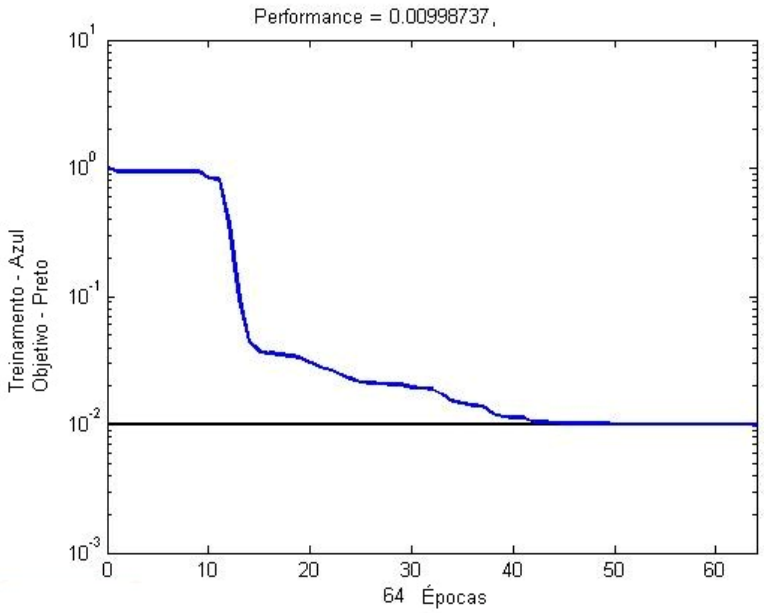


**Figura 6-4 : Treinamento 1. DS3**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60425 | 168 |
| | Intrusão | 66852 | 183584 |

**Tabela 6-6 : CM 1. DS3**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.7845 |
| TP | 0.7331 |
| FP | 0.0028 |
| TN | 0.9972 |
| FN | 0.2669 |
| P | 0.9991 |

**Tabela 6-7 : Parâmetros 1. DS3**

## Conjunto de treinamento DS4

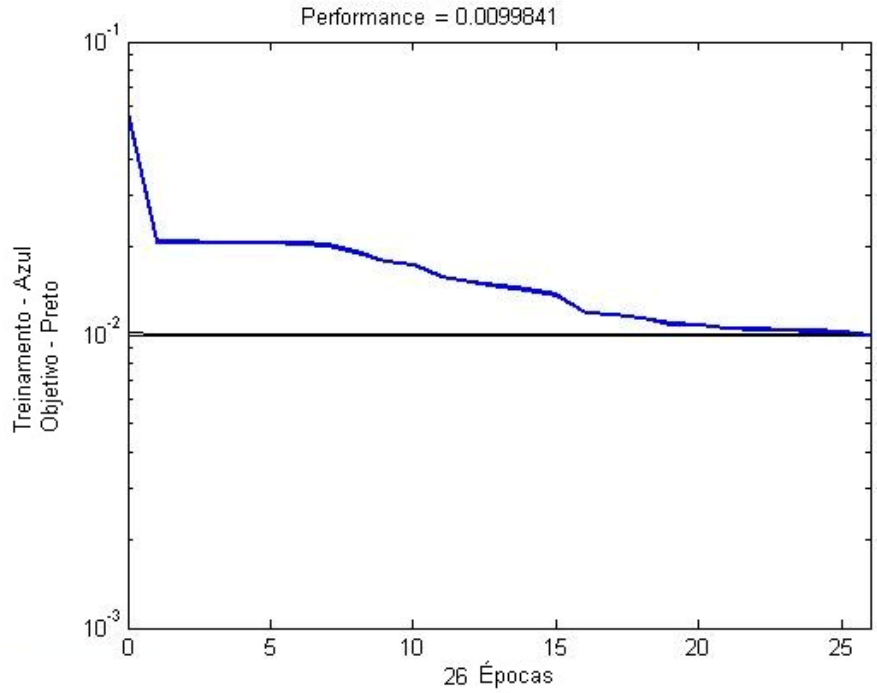


**Figura 6-5 : Treinamento 1. DS4**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60345 | 248 |
| | Intrusão | 246729 | 3707 |

**Tabela 6-8 : CM 1. DS4**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.2059 |
| TP | 0.0148 |
| FP | 0.0041 |
| TN | 0.9959 |
| FN | 0.9852 |
| P | 0.9373 |

**Tabela 6-9 : Parâmetros 1. DS4**

## Conjunto de treinamento DS5

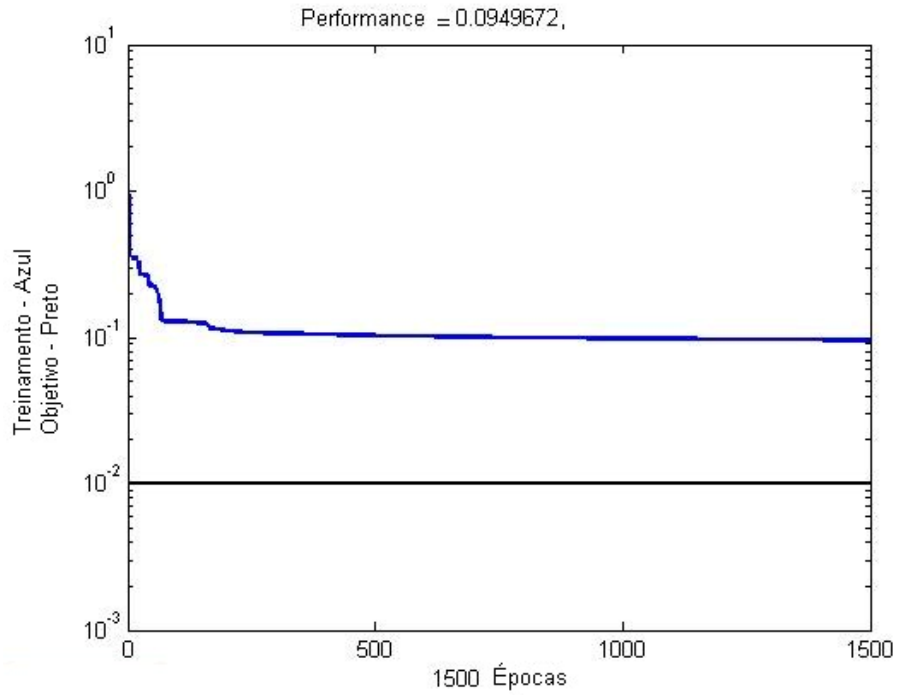


**Figura 6-6 : Treinamento 1. DS5**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59403 | 1190 |
| | Intrusão | 247068 | 3368 |

**Tabela 6-10 : CM 1. DS5**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.201817 |
| TP | 0.013449 |
| FP | 0.019639 |
| TN | 0.980361 |
| FN | 0.986551 |
| P | 0.738921 |

**Tabela 6-11 : Parâmetros : 1. DS5**

## Curvas ROC

Variando o limiar de decisão *th* temos condição de alterar a resposta do sistema classificador. As curvas ROC e sua variação apresentadas a seguir ilustram o comportamento dos parâmetros TP e AC em relação ao parâmetro FP quando se varia o limiar de decisão *th* de -1 a 1 em passos de 0,1 e nova matriz de confusão é determinada para cada novo limiar.

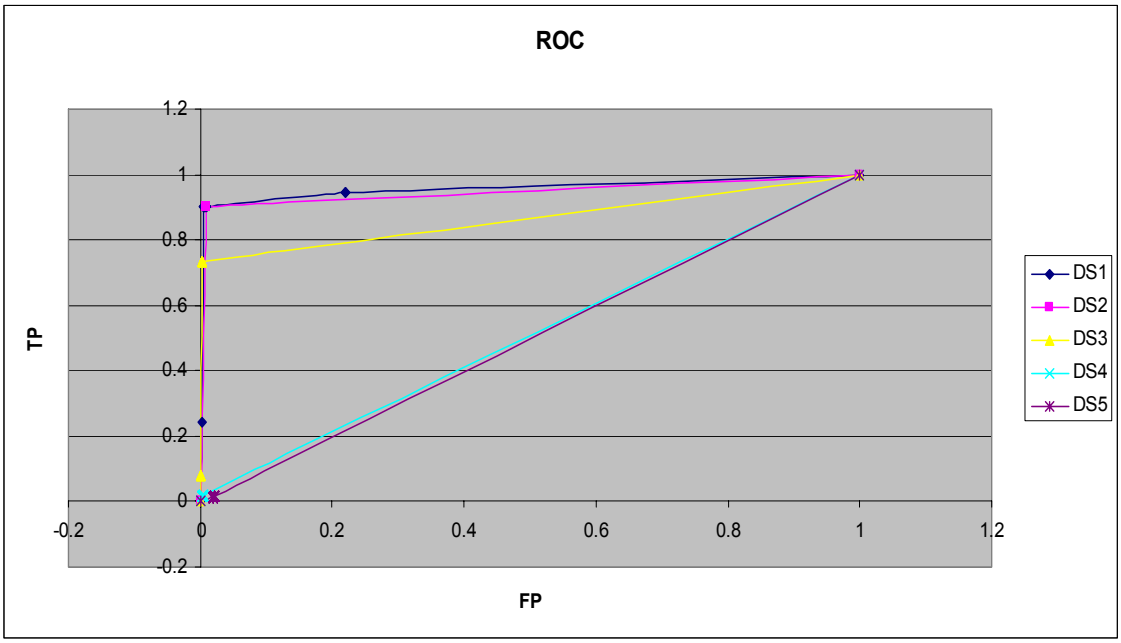


**Figura 6-7 : 1. ROC : TP x FP**

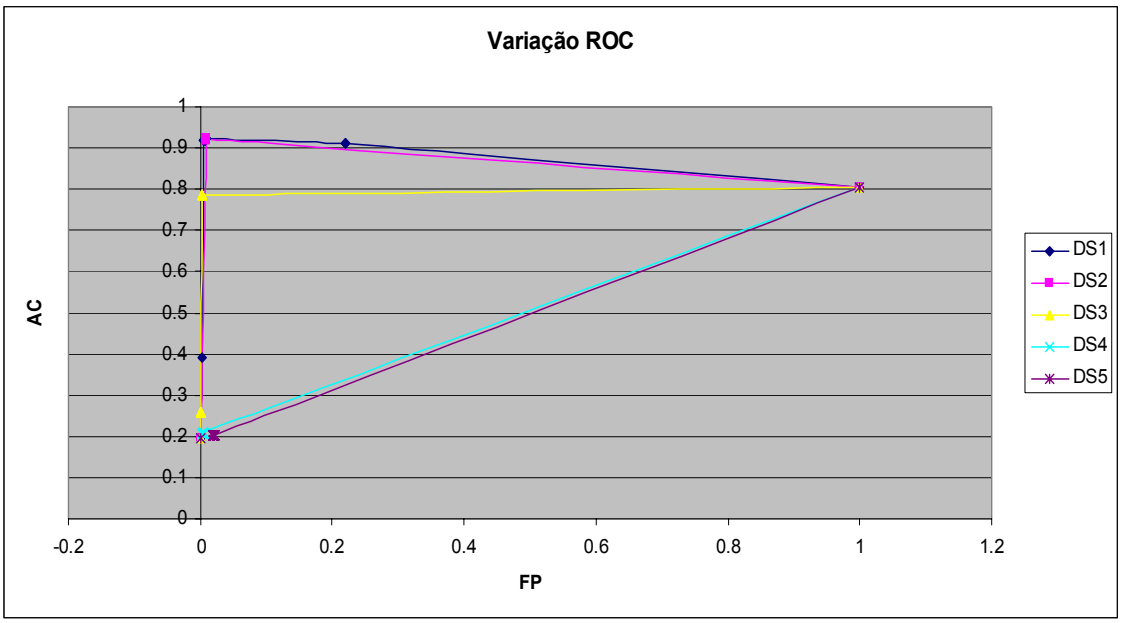


**Figura 6-8 : 1. Variação ROC – AC x FP**

A comparação entre o desempenho da mesma rede neural, quando treinada com subconjuntos diferentes mostra claramente a importância dos dados de treinamento. Como esperado, o melhor desempenho ocorreu quando a rede foi treinada com subconjunto 1, que contém a totalidade dos padrões de ataque e intrusão. A rede apresentou pior desempenho para os subconjuntos 4 e 5, que contém ataques apenas das classes U2R e R2L respectivamente. Como estas classes possuem um menor número de ocorrências para cada padrão de ataque, esta queda também era esperada. Importante ressaltar que para o subconjunto 5 o treinamento da rede neural não convergiu para o objetivo desejado.

### 6.2.2. Todas as características como entrada

Para este cenário, as 41 variáveis que identificam um registro foram utilizadas para treinar e validar uma rede neural MLP 41-15-15-1 (41 entradas, 2 camadas com 15 neurônios em cada e 1 saída). Como o vetor de entrada teve um aumento significativo o número de elementos processadores nas camadas ocultas foi aumentado.

## Conjunto de treinamento DS1

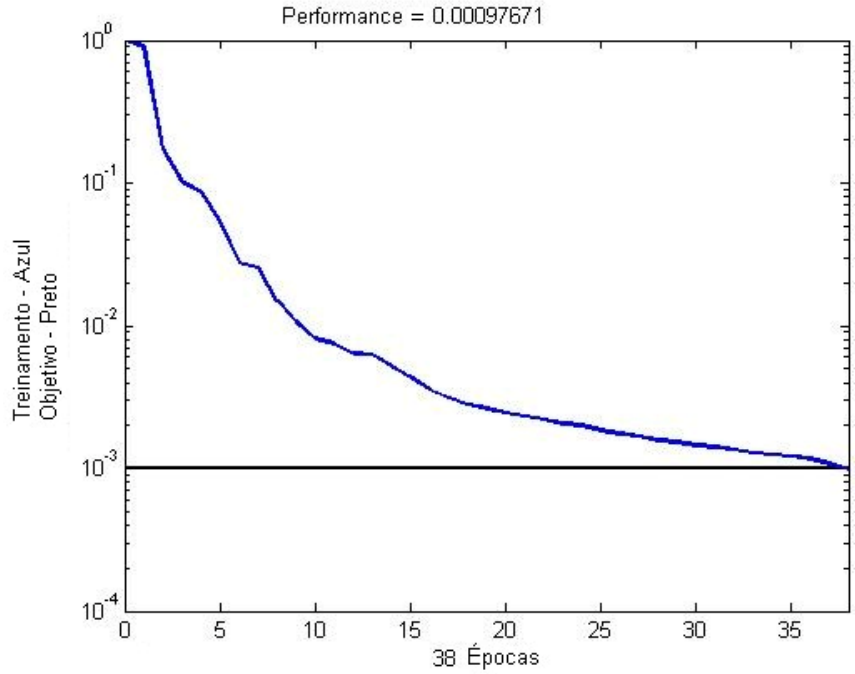


**Figura 6-9 : Treinamento 2. DS1**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59783 | 810 |
| | Intrusão | 22530 | 227906 |

**Tabela 6-12 : Parâmetros 2. DS1**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9250 |
| TP | 0.9100 |
| FP | 0.0134 |
| TN | 0.9866 |
| FN | 0.0900 |
| P | 0.9965 |

**Tabela 6-13 : Parâmetros 2. DS1**

## Conjunto de treinamento DS2

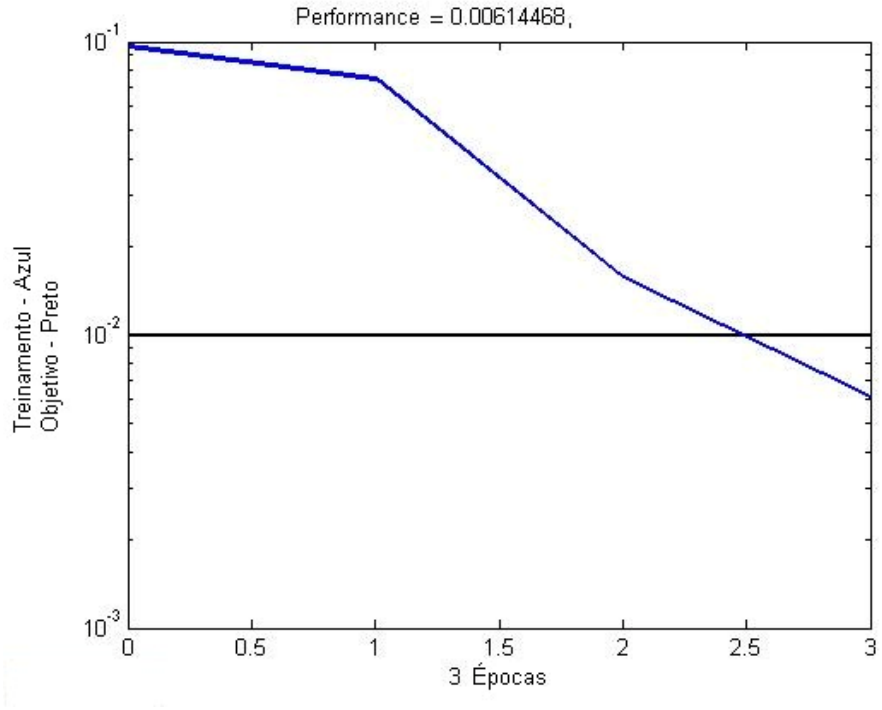


**Figura 6-10 : Treinamento 2. DS2**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60361 | 232 |
| | Intrusão | 189597 | 60839 |

**Tabela 6-14 : CM 2. DS2**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.3897 |
| TP | 0.2429 |
| FP | 0.0038 |
| TN | 0.9962 |
| FN | 0.7571 |
| P | 0.9962 |

**Tabela 6-15 : Parâmetros 2. DS2**

## Conjunto de treinamento DS3

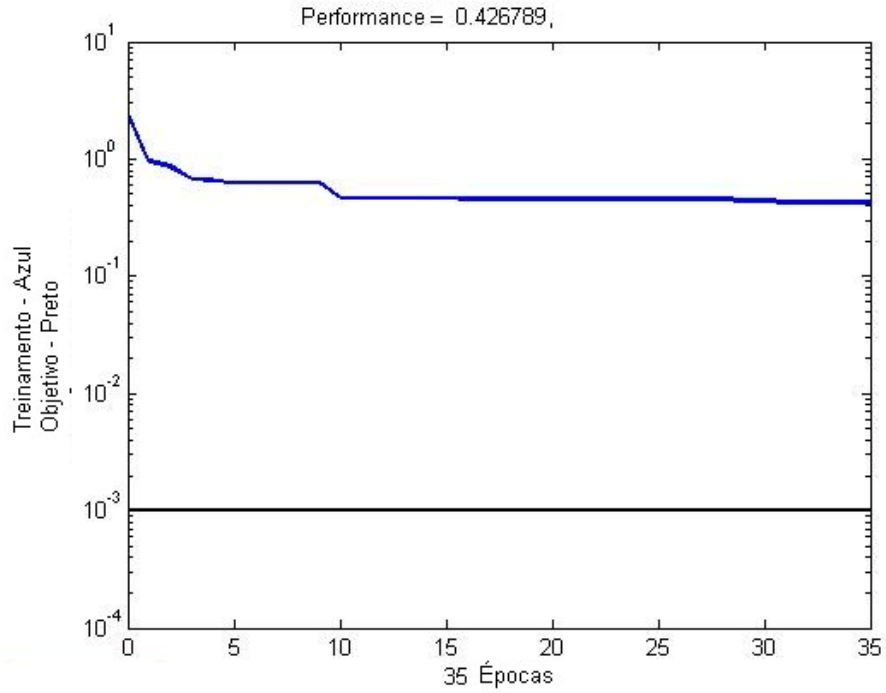


**Figura 6-11 : Treinamento 2. DS3**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 45009 | 15584 |
| | Intrusão | 57504 | 192932 |

**Tabela 6-16 : CM 2. DS3**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.7650 |
| TP | 0.7704 |
| FP | 0.2572 |
| TN | 0.7428 |
| FN | 0.2296 |
| P | 0.9253 |

**Tabela 6-17 : Parâmetros 2. DS3**

## Conjunto de treinamento DS4

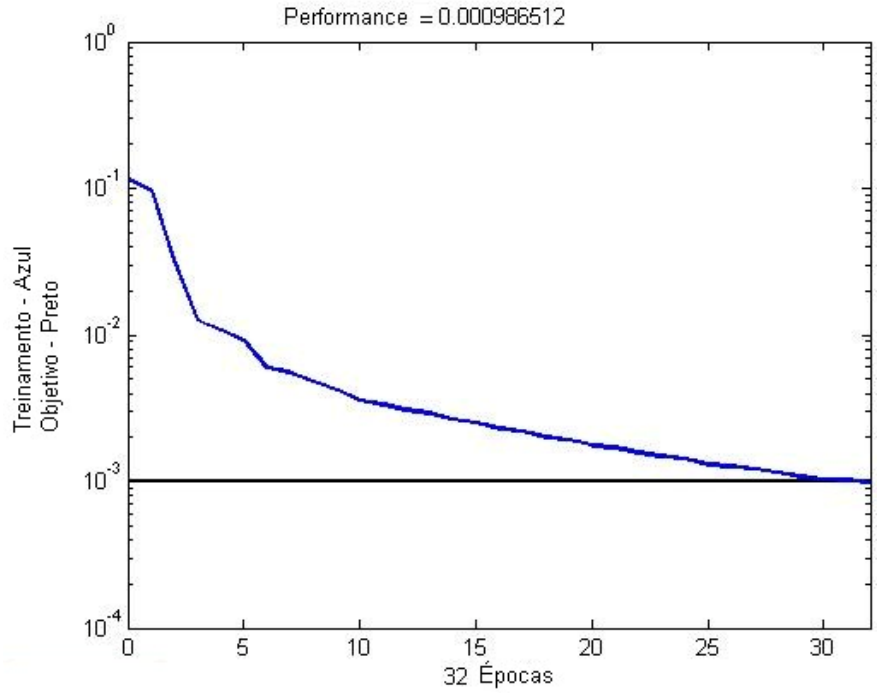


**Figura 6-12 : Treinamento 2. DS4**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60558 | 35 |
| | Intrusão | 250157 | 279 |

**Tabela 6-18 : CM 2. DS4**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.1956 |
| TP | 0.0011 |
| FP | 0.0006 |
| TN | 0.9994 |
| FN | 0.9989 |
| P | 0.8885 |

**Tabela 6-19 : Parâmetros 2. DS4**

## Conjunto de treinamento DS5

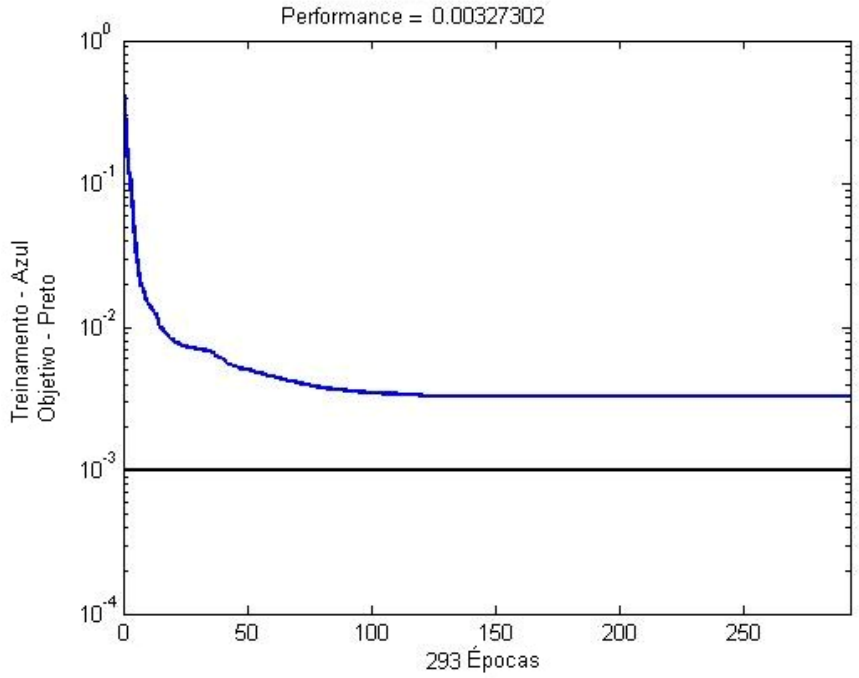


**Figura 6-13 : Treinamento 2. DS5**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60509 | 84 |
| | Intrusão | 248946 | 1490 |

**Tabela 6-20 : CM 2. DS5**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.1993 |
| TP | 0.0059 |
| FP | 0.0014 |
| TN | 0.9986 |
| FN | 0.9941 |
| P | 0.9466 |

**Tabela 6-21 : Parâmetros 2. DS5**

## Curvas ROC

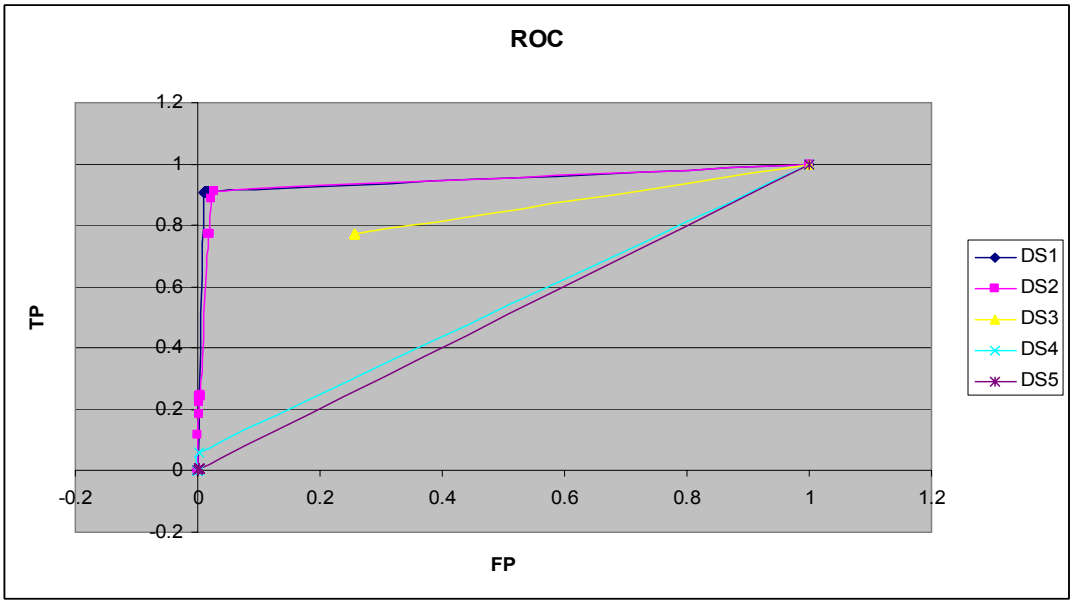


**Figura 6-14 : 2. ROC – TP x FP**

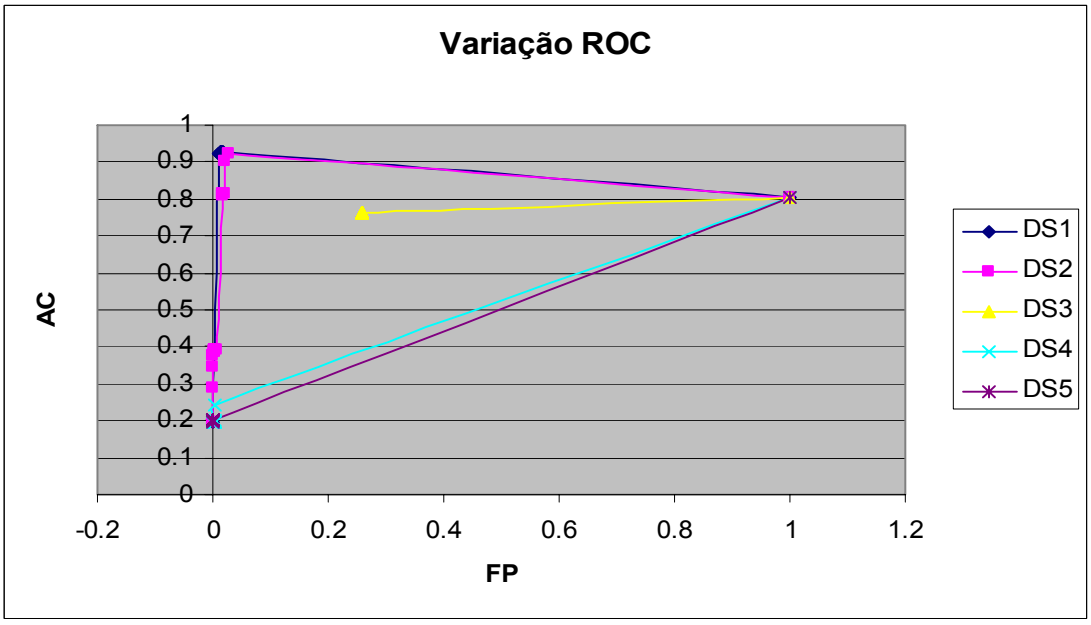


**Figura 6-15 : 2. Variação ROC – AC x FP**

Neste grupo de simulações, novamente ficou evidente a importância dos dados de treinamento para o desempenho da rede. O maior número de elementos de entrada (41 variáveis neste caso) indicaria, em análise preliminar, que este grupo de redes teria desempenho melhor que o 1º grupo – que teve

apenas as características intrínsecas como entrada. Entretanto, este melhor desempenho não foi comprovado na prática. O desempenho para subconjunto 1 foi ligeiramente inferior para a rede com 41 entradas em relação a rede com apenas 9 entradas.

O desempenho da rede para o subconjunto 2 foi péssimo pela análise da matriz de confusão com limiar de decisão em zero. Entretanto, analisado a curva ROC para este mesmo cenário, verifica-se que o desempenho geral foi similar ao mesmo caso para o 1º grupo. Este fato ilustra a importância do limiar de decisão. Mantendo-o em zero, temos uma rede com péssimo desempenho quando treinada com o subconjunto 2. Deslocando este limiar, atingimos índices de acerto bem mais aceitáveis.

### 6.2.3. Características Especialistas como Entrada

Apenas as 13 características geradas através de especialista – ver tabela 5.2 - foram utilizadas para treinar as redes neurais neste cenário. Uma rede MLP 13-15-15-1 (13 entradas, 2 camadas ocultas com 15 elementos processadores cada e uam saída) foi empregada.

#### Conjunto de treinamento DS1

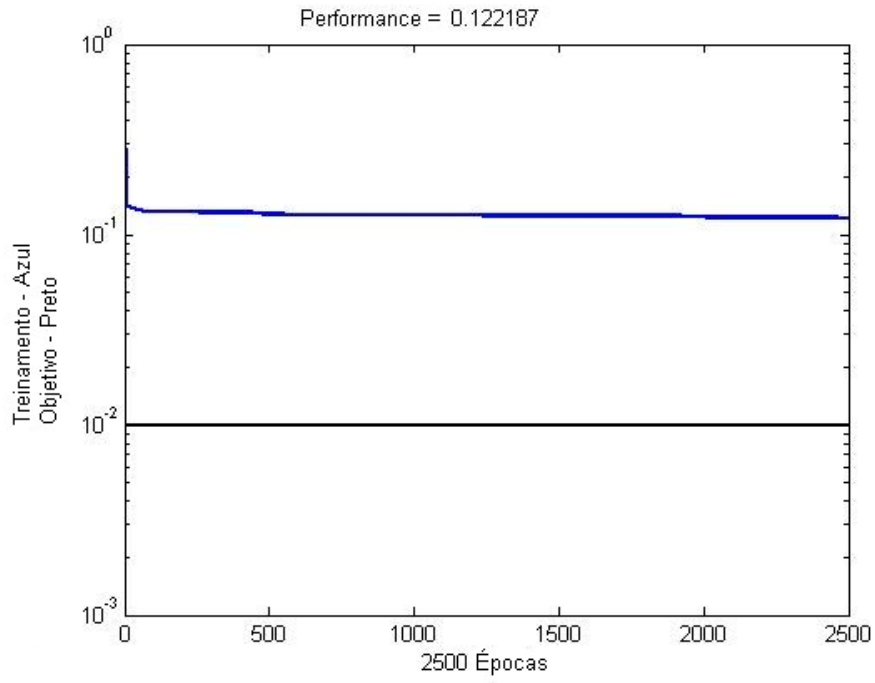


**Figura 6-16 : Treinamento 3. DS1**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 58643 | 1950 |
| | Intrusão | 25206 | 225230 |

**Tabela 6-22 : CM 3. DS1**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9127 |
| TP | 0.8994 |
| FP | 0.0322 |
| TN | 0.9678 |
| FN | 0.1006 |
| P | 0.9914 |

**Tabela 6-23 : Parâmetros 3. DS1**



## Conjunto de treinamento DS2

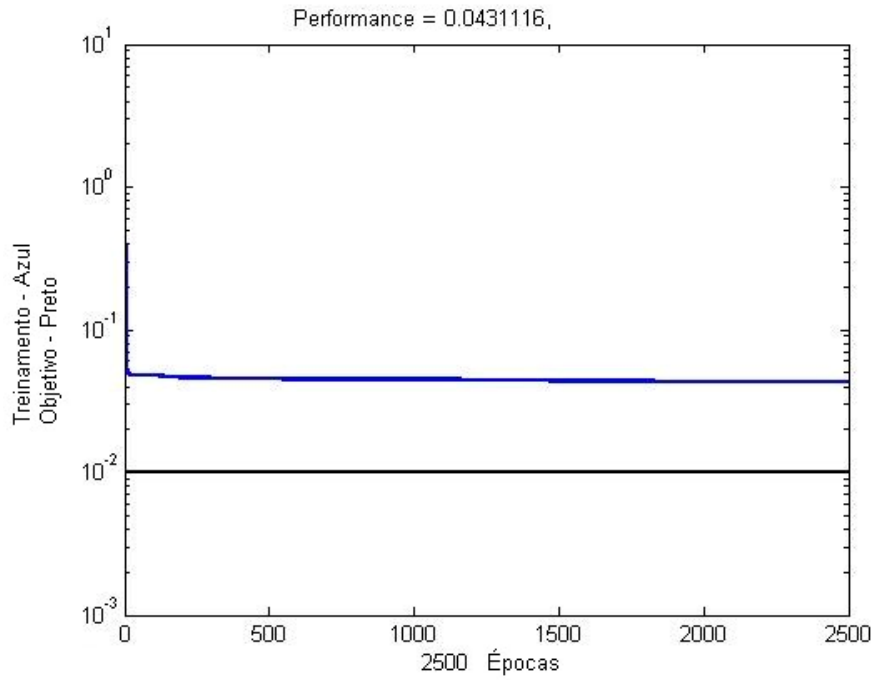


**Figura 6-17 : Treinamento 3. DS2**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59895 | 698 |
| | Intrusão | 112722 | 137714 |

**Tabela 6-24 : CM 3. DS2**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.6353 |
| TP | 0.5499 |
| FP | 0.0115 |
| TN | 0.9885 |
| FN | 0.4501 |
| P | 0.9950 |

**Tabela 6-25 : Parâmetros 3. DS2**



## Conjunto de treinamento DS3

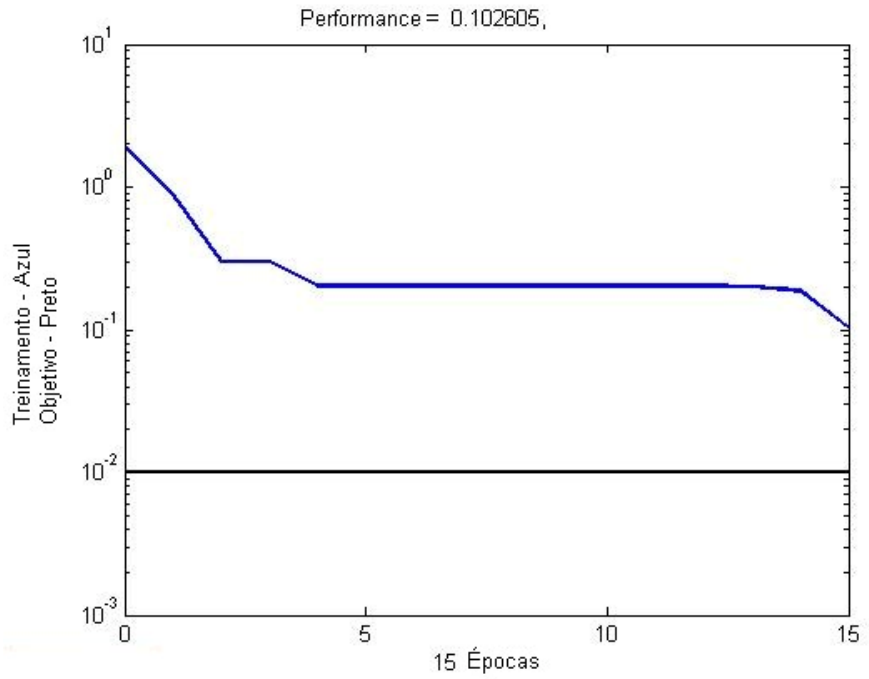


**Figura 6-18 : Treinamento 3. DS3**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59122 | 1471 |
| | Intrusão | 27233 | 223203 |

**Tabela 6-26 : CM 3. DS3**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9077 |
| TP | 0.8913 |
| FP | 0.0243 |
| TN | 0.9757 |
| FN | 0.1087 |
| P | 0.9935 |

**Tabela 6-27 : Parâmetros 3. DS3**



## Conjunto de treinamento DS4

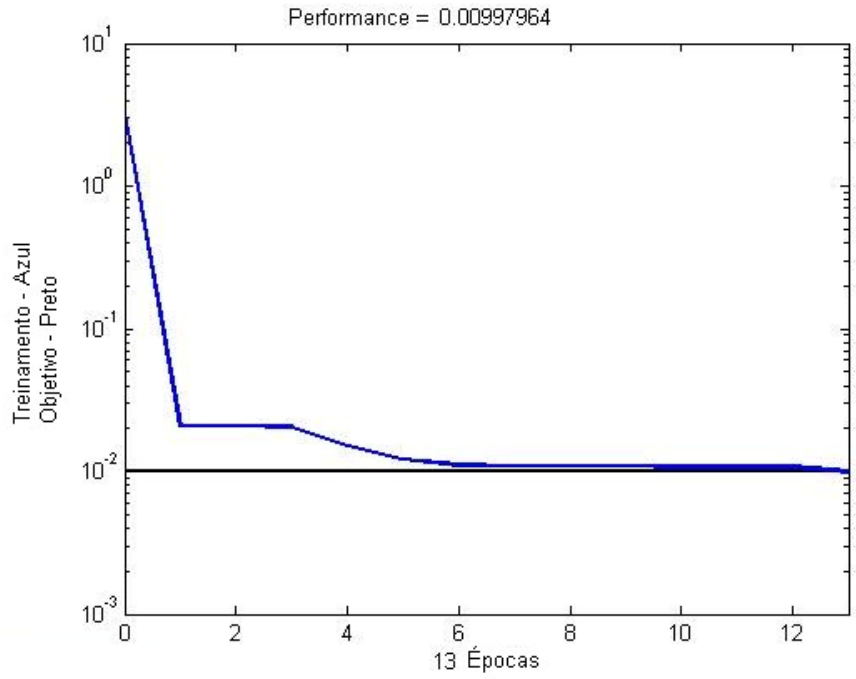


**Figura 6-19 : Treinamento 3. DS4**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60574 | 19 |
| | Intrusão | 250412 | 24 |

**Tabela 6-28 : CM 3. DS4**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.1948 |
| TP | 0.0001 |
| FP | 0.0003 |
| TN | 0.9997 |
| FN | 0.9999 |
| P | 0.5581 |

**Tabela 6-29 : Parâmetros 3. DS4**



## Conjunto de treinamento DS5

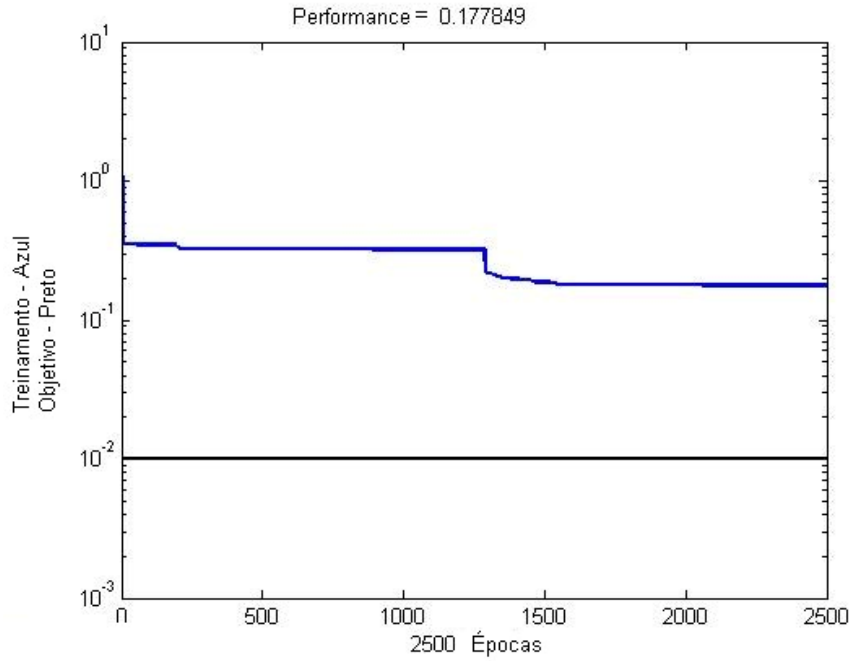


**Figura 6-20 : Treinamento 3. DS5**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60445 | 148 |
| | Intrusão | 246546 | 3890 |

**Tabela 6-30 : CM 3. DS5**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.2068 |
| TP | 0.0155 |
| FP | 0.0024 |
| TN | 0.9976 |
| FN | 0.9845 |
| P | 0.9633 |

**Tabela 6-31 : Parâmetros 3. DS5**

## Curvas ROC

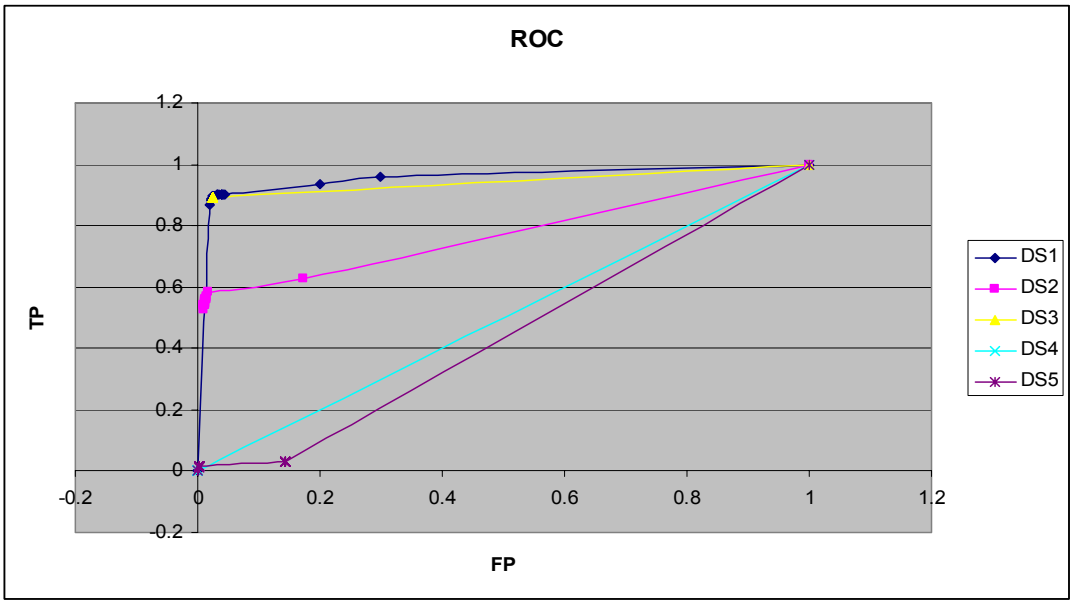


**Figura 6-21 : 3. ROC – TP x FP**

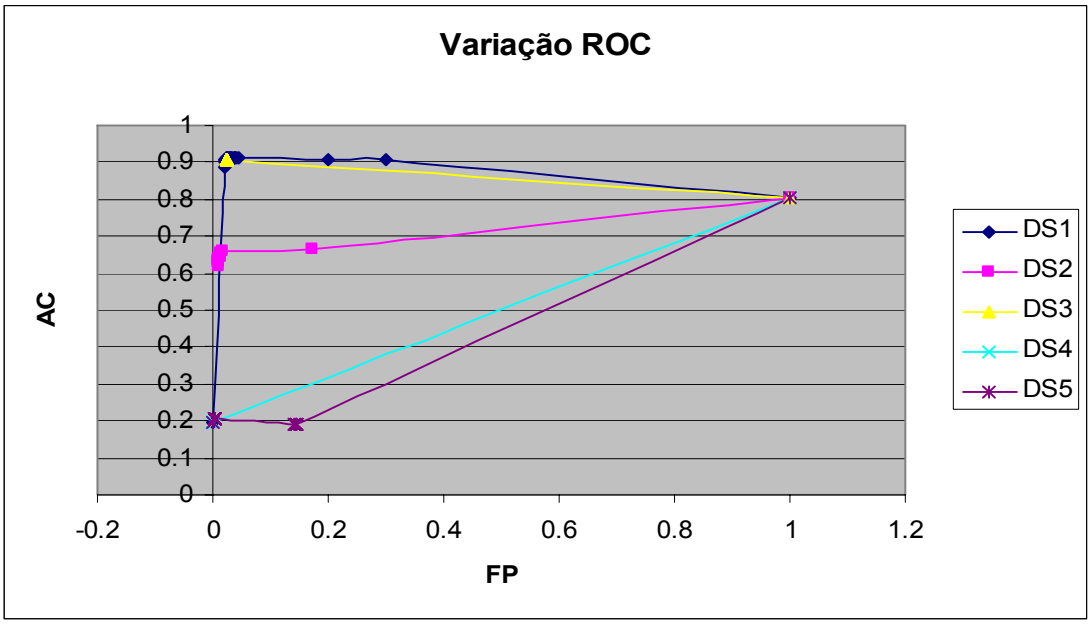


**Figura 6-22 : 3. Variação ROC – AC x FP**

Neste grupo, observamos uma queda no desempenho da rede para a maioria dos subconjuntos. Esta queda esta associada também a uma dificuldade de convergência do processo de treinamento das redes

Observa-se, entretanto, que as 13 características especialistas quando combinadas com um treinamento com o subconjunto 3 – padrões normais e apenas padrões da classe negação de serviço – resultam numa melhora significativa nos índices desta rede, quando comparada aos 2 grupos anteriores. Paralelamente, observa-se uma queda nos índices da rede quando treinada com o subconjunto 2 – normal e reconhecimento apenas. É possível inferir que as características especialistas são mais importantes para a detecção de padrões de negação de serviços.

### 6.2.4. Características Temporais como Entrada

Para este cenário, as 19 características temporais obtidas através de janela de 2 segundos – tabela 5.3 - foram utilizadas para treinar as redes neurais neste cenário. Uma rede MLP 19-15-15-1 (19 entradas, 2 camadas ocultas com 15 elementos processadores cada e uam saída) foi empregada.

### Conjunto de treinamento DS1

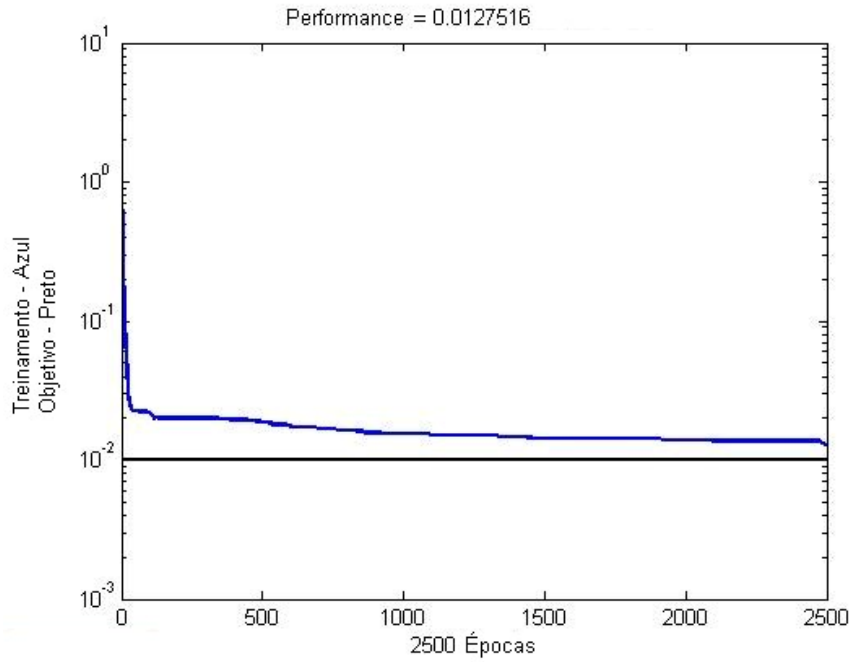


**Figura 6-23 : Treinamento 4. DS1**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59339 | 1254 |
| | Intrusão | 55348 | 195088 |

**Tabela 6-32 : CM 4. DS1**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.8180 |
| TP | 0.7790 |
| FP | 0.0207 |
| TN | 0.9793 |
| FN | 0.2210 |
| P | 0.9936 |

**Tabela 6-33 : Parâmetros 4. DS1**

## Conjunto de treinamento DS2

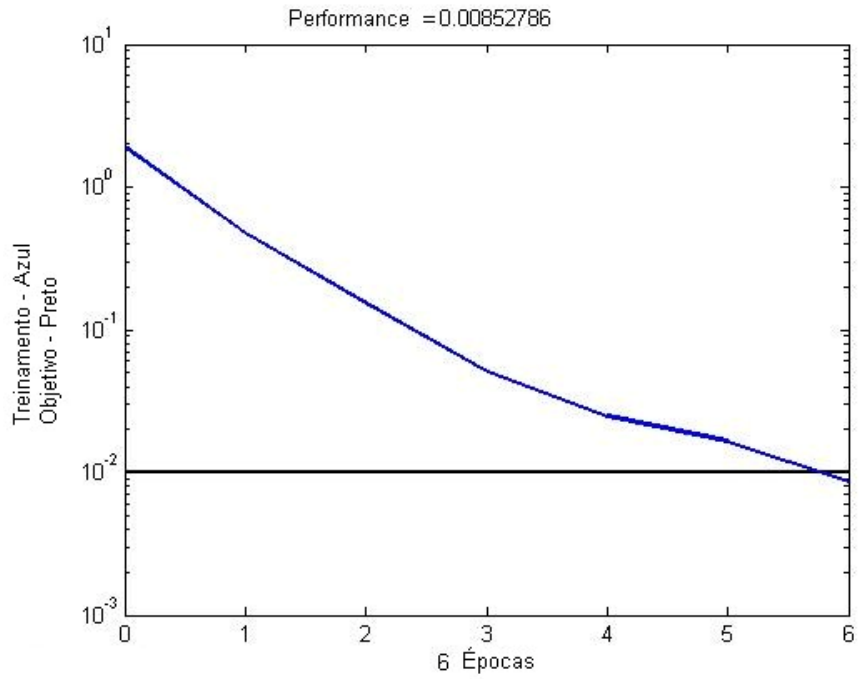


**Figura 6-24 : Treinamento 4. DS2**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60372 | 221 |
| | Intrusão | 188624 | 61812 |

**Tabela 6-34 : CM 4. DS2**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.3928 |
| TP | 0.2468 |
| FP | 0.0036 |
| TN | 0.9964 |
| FN | 0.7532 |
| P | 0.9964 |

**Tabela 6-35 : Parâmetros 4. DS2**

### Conjunto de treinamento DS3

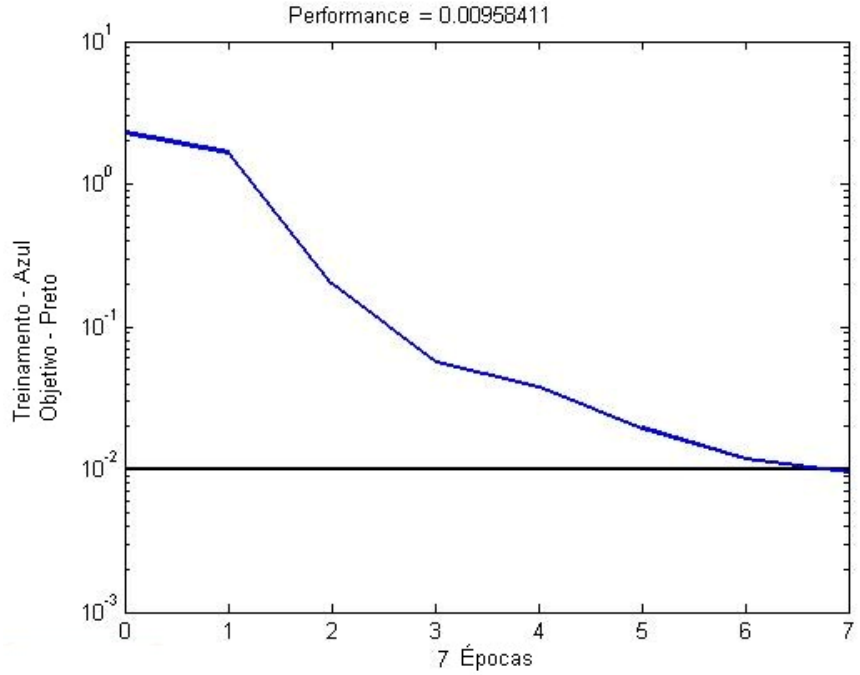


**Figura 6-25 : Treinamento 4. DS3**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 59793 | 800 |
| | Intrusão | 25654 | 224782 |

**Tabela 6-36 : CM 4. DS3**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9149 |
| TP | 0.8976 |
| FP | 0.0132 |
| TN | 0.9868 |
| FN | 0.1024 |
| P | 0.9965 |

**Tabela 6-37 : Parâmetros 4. DS3**

## Conjunto de treinamento DS4

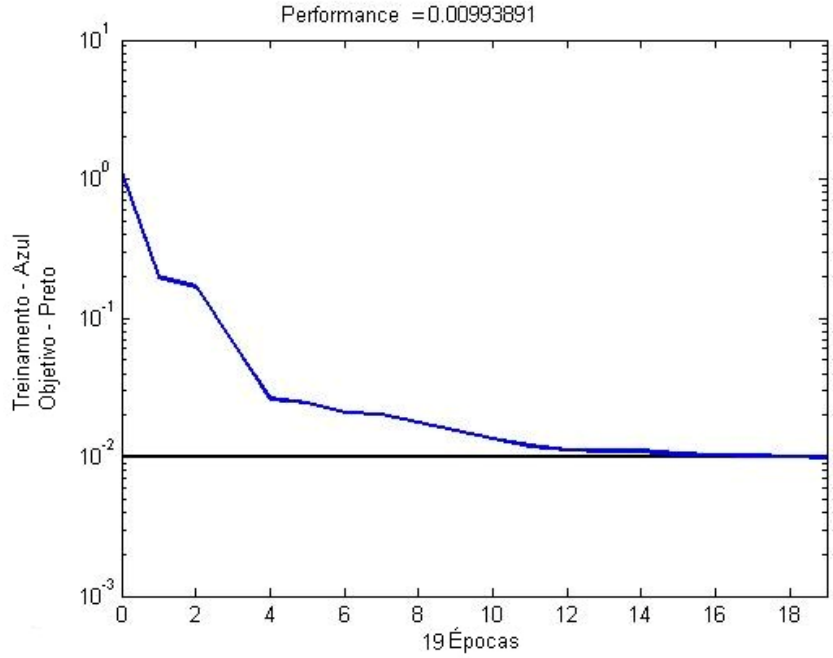


**Figura 6-26 : Treinamento 4. DS4**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60513 | 80 |
| | Intrusão | 249480 | 956 |

**Tabela 6-38 : CM 4. DS4**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.1976 |
| TP | 0.0038 |
| FP | 0.0013 |
| TN | 0.9987 |
| FN | 0.9962 |
| P | 0.9228 |

**Tabela 6-39 : Parâmetros 4. DS4**

## Conjunto de treinamento DS5

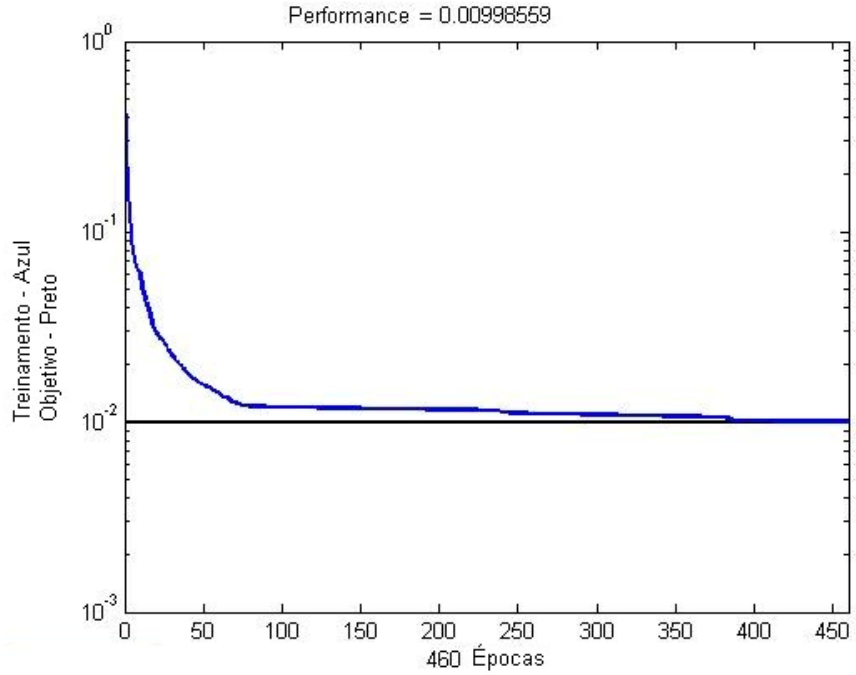


**Figura 6-27 : Treinamento 4. DS5**

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60294 | 299 |
| | Intrusão | 195529 | 54907 |

**Tabela 6-40 : CM 4. DS5**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.3704 |
| TP | 0.2192 |
| FP | 0.0049 |
| TN | 0.9951 |
| FN | 0.7808 |
| P | 0.9946 |

**Tabela 6-41 : Parâmetros 4. DS5**

## Curvas ROC

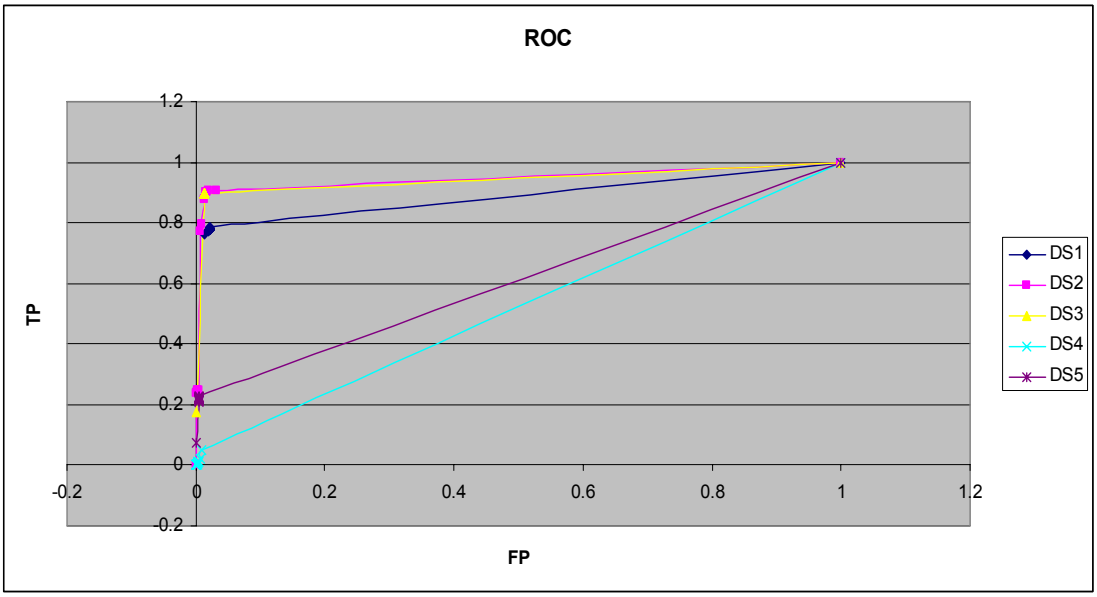


**Figura 6-28 : 4. ROC – TP x FP**



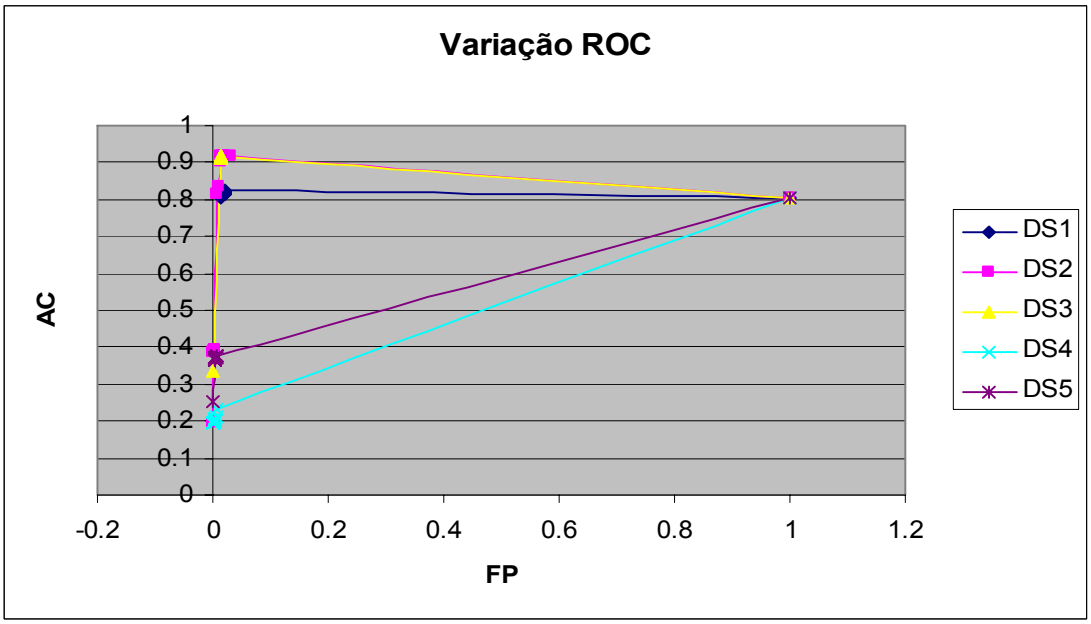


**Figura 6-29 : 4. Variação ROC – AC x FP**

Neste grupo, foi obtido um desempenho razoável com destaque para a rede treinada com o subconjunto 2. Pela característica dos padrões de ataque da classe de reconhecimento esperava-se uma relação forte com as características obtidas através de janela temporal. Alguns padrões da classe negação de serviço apresentam esta dependência, mas não são todos.

## 6.3.
## Classificador por Classes

Uma rede neural MLP foi treinada e avaliada para distinguir, para cada padrão de entrada apresentado, se o mesmo pertence a classe normal ou, caso seja um padrão de ataque / intrusão, determinar em qual das quatro classes de ataque – DoS, reconhecimento, usuário para super-usuário e remoto para local – o padrão pertence.Neste cenário, a rede foi treinada utilizando todas as 41 características para cada vetor de entrada e apenas o conjunto DS1 de treinamentos foi utilizado. A utilização de apenas parte das características do vetor de entradas para o treinamento desta rede não foi empregada uma vez que, para detectar com precisão a classe, é esperado que a rede precisará do máximo de informação disponível para seu aprendizado.

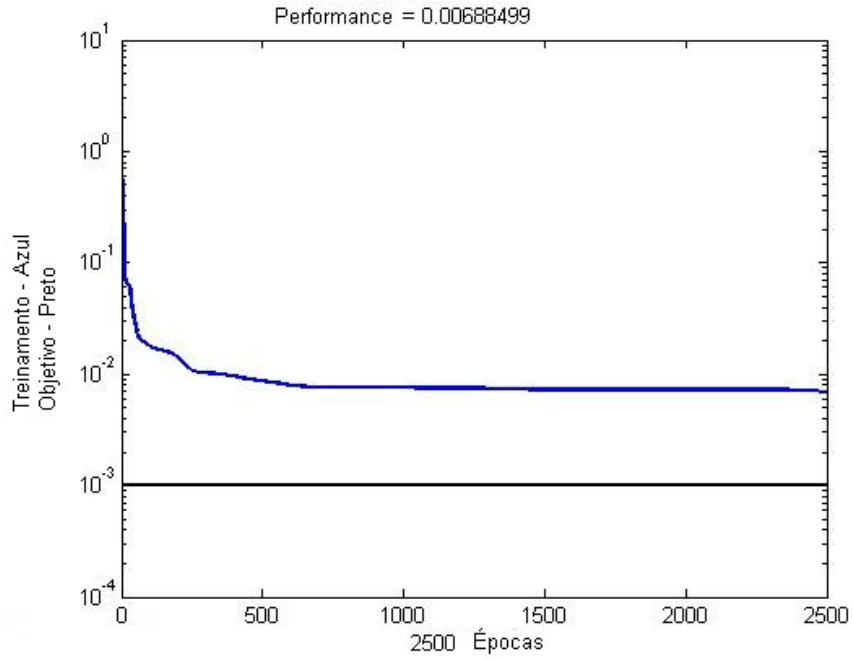


**Figura 6-30 : Treinamento RN por classe – DS1**

| | | Previsto | | | | | |
|---|---|---|---|---|---|---|---|
| | | Normal | R2L | DoS | U2R | Probe | Taxa detecção |
| Real | Normal | 59314 | 1 | 215 | 1 | 150 | 0.9939 |
| | R2L | 14960 | 149 | 40 | 2 | 75 | 0.0098 |
| | DoS | 6626 | 19 | 222781 | 0 | 121 | 0.9705 |
| | U2R | 39 | 7 | 1 | 7 | 1 | 0.1273 |
| | Probe | 580 | 0 | 243 | 0 | 2586 | 0.7586 |
| | Precisão geral (AC - “Accuracy”) | | | | | | 0.9250 |

**Tabela 6-42 : CM por classe - DS1**

Para este cenário é possível realizar a comparação dos resultados obtidos pela rede neural treinada com resultados do concurso KDDCup 1999. 24 participantes utilizaram a mesma base de dados para treinamento e testes e empregaram diversas técnicas de mineração de dados e descoberta de conhecimento para classificar um registro de conexão dentro da classe correta. A técnica vencedora [36], baseada em árvores de decisão e na ferramenta de mineração de dados C5, apresentou a seguinte matriz de confusão como resultado.

| | | Previsto | | | | | |
|---|---|---|---|---|---|---|---|
| | | Normal | R2L | DoS | U2R | Probe | Taxa detecção |
| Real | Normal | 60262 | 243 | 78 | 4 | 6 | 0,9950 |
| | R2L | 14527 | 294 | 0 | 8 | 1360 | 0,0840 |
| | DoS | 5299 | 1328 | 223226 | 0 | 0 | 0,9710 |
| | U2R | 168 | 20 | 0 | 30 | 10 | 0,1320 |
| | Probe | 511 | 3471 | 184 | 0 | 0 | 0,8339 |
| | Precisão geral (AC - “Accuracy”) | | | | | | 0.9250 |

**Tabela 6-43 : CM para técnica ganhadora do KDDCup 1999**

Os resultados obtidos pela rede neural foram bastante próximos do obtido pela técnica vencedora. Vantagem razoável foi notada para a técnica baseada em árvore de decisão apenas na detecção das classes R2L e reconhecimento (*Probe*).

## 6.4. Classificador Preciso para Classe DoS

Existem 6 padrões de intrusão da classe Negação de Serviço presentes na base de dados de treinamento. A base de dados para testes possui quatro novos padrões para esta mesma classe. Neste cenário uma rede neural MLP foi treinada para realizar a classificação precisa de padrões de ataque para a classe negação de serviço apenas. A saída da rede treinada será capaz de identificar o padrão de entrada como normal, como um dos 6 padrões presentes na base de treinamento ou como um outro padrão de ataque desconhecido (classe "Outros"). Duas redes – configuração 41-20-15-8 – foram empregadas neste cenário : a primeira foi treinada com o subconjunto de treinamento DS1 e a segunda com o subconjunto DS3 (que possui apenas padrões normais e da classe DoS).

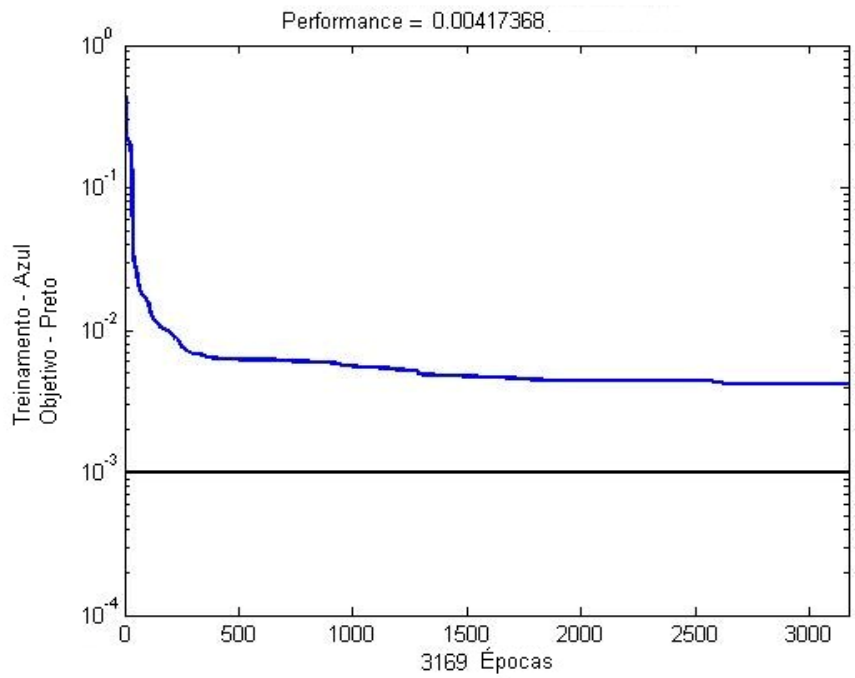


**Figura 6-31 : Treinamento RN Classe DoS – DS1**

| | | Previsto | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | Neptune | Smurf | Pod | Land | TearDrop | Back | Taxa Detecção |
| Real | Normal | 60198 | 233 | 0 | 4 | 108 | 0 | 0 | 0 | 0.9935 |
| | Outros | 22448 | 4286 | 270 | 4 | 3 | 0 | 0 | 0 | 0.1579 |
| | Neptune | 1 | 67 | 57927 | 0 | 0 | 0 | 0 | 0 | 0.9987 |
| | Smurf | 1 | 0 | 0 | 163959 | 49 | 0 | 0 | 0 | 0.9992 |
| | Pod | 2 | 0 | 0 | 1 | 84 | 0 | 0 | 0 | 0.9655 |
| | Land | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Teardrop | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Back | 1098 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | | | 0.9210 |

**Tabela 6-44 : CM Classe DoS – DS1**



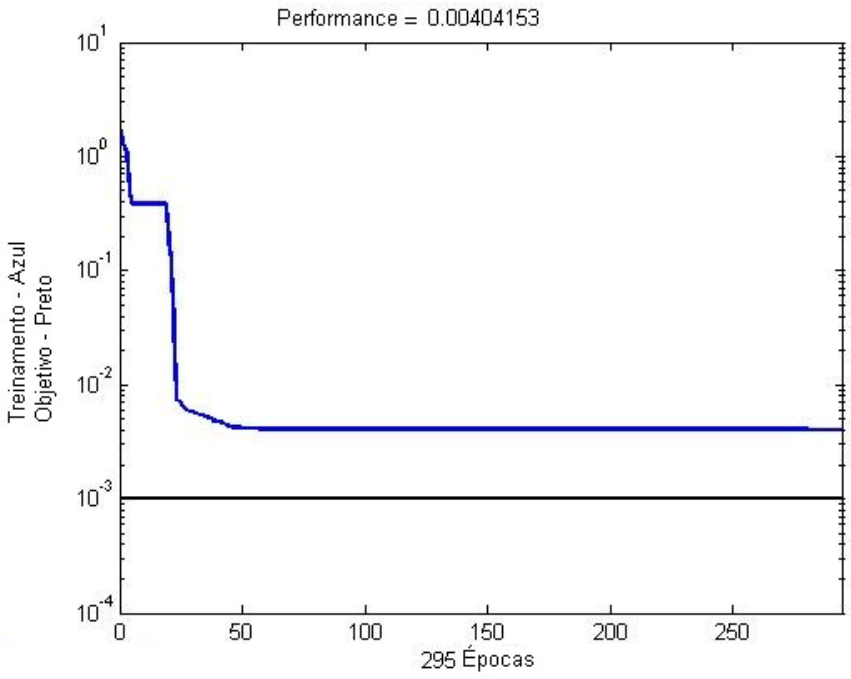


**Figura 6-32 : Treinamento RN Classe DoS – DS3**

| | | Previsto | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | Neptune | Smurf | Pod | Land | TearDrop | Back | Taxa Detecção |
| Real | Normal | 59909 | 0 | 17 | 0 | 0 | 0 | 0 | 0 | 0.9887 |
| | Outros | 24409 | 0 | 2185 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Neptune | 15 | 0 | 57968 | 0 | 0 | 0 | 0 | 0 | 0.9994 |
| | Smurf | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Pod | 78 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Land | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Teardrop | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Back | 1098 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | | | 0.3790 |

**Tabela 6-45 : CM Classe DoS - DS3**

Estas redes foram treinadas para tentar uma identificação precisa, dentro da classe negação de serviço, do padrão exato de ataque apresentado na sua entrada. Fico evidente que a eficiência da rede depende do treinamento com dados de entrada contendo todos os padrões (subconjunto 1). Ainda assim, a rede não conseguiu identificar corretamente nenhum caso dos padrões Land, Teardrop e Back. É importante observar que este padrões de ataque podem ser facilmente identificados por um sistema de detecção de intrusão baseado em conhecimento (sistema especialista com regras codificadas).

## 6.5. Classificador Preciso para Classe Reconhecimento

A classe de padrões de ataque de reconhecimento (“Probe”) possui 4 padrões de ataques presentes na base de treinamento e 6 na base de testes. Uma rede neural MLP – 41-20-15-6 - foi treinada – utilizando os subconjuntos DS1 e DS2 - para identificar padrões apresentados na sua entrada como pertencentes a normal, a um dos 4 padrões da classe reconhecimento ou a uma categoria de padrão intrusivo desconhecido (outros).

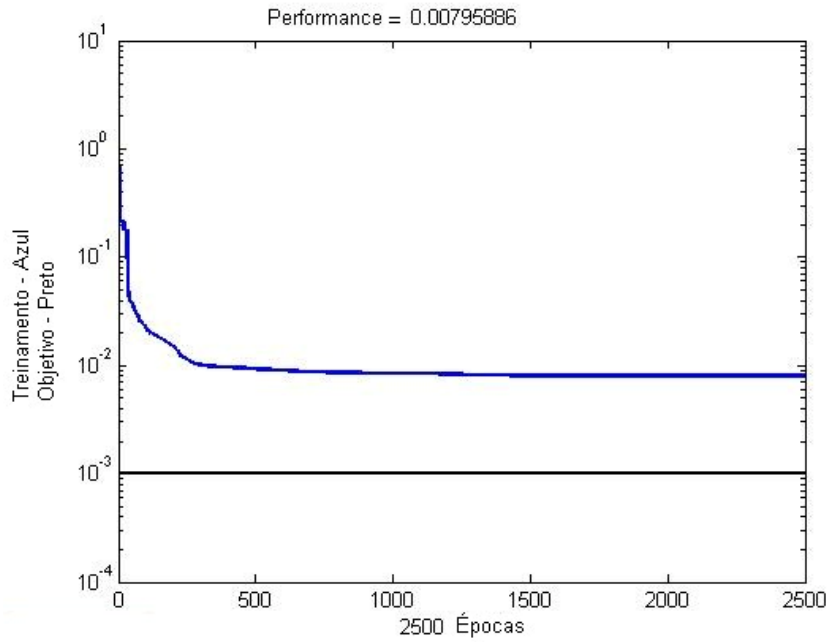


**Figura 6-33 : Treinamento RN Classe "Probe" – DS1**



| | | Previsto | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | mscan | ipsweep | nmap | satan | Taxa Detecção |
| Real | Normal | 60093 | 220 | 71 | 29 | 0 | 0 | 0.9917 |
| | Outros | 23250 | 223688 | 64 | 156 | 0 | 0 | 0.7290 |
| | mscan | 0 | 9 | 319 | 2 | 0 | 0 | 0.3029 |
| | ipsweep | 0 | 6 | 0 | 235 | 0 | 0 | 0.7680 |
| | nmap | 0 | 0 | 0 | 0 | 84 | 0 | 1.0000 |
| | satan | 86 | 0 | 1 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – "Accuracy") | | | | | | | 0.9144 |

**Tabela 6-46 : CM Classe Reconhecimento – DS1**

| | | Previsto | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | mscan | ipsweep | nmap | satan | Taxa Detecção |
| Real | Normal | 60481 | 0 | 86 | 0 | 0 | 0 | 0.9982 |
| | Outros | 206319 | 0 | 940 | 0 | 0 | 0 | 0.0000 |
| | mscan | 4 | 0 | 326 | 0 | 0 | 0 | 0.3096 |
| | ipsweep | 306 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | nmap | 84 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | satan | 227 | 0 | 27 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – "Accuracy") | | | | | | | 0.1955 |

**Tabela 6-47 : CM Classe Reconhecimento – DS2**

Como na rede com classificação precisa para a classe negação de serviço, a rede neste cenário apresentou uma precisão geral razoável quando treinada com o subconjunto 1 e muito ruim quando treinada com o subconjunto 2. Não existe boa correlação entre as características especialistas e padrões específicos da classe reconhecimento. Novamente, pelo menos um padrão de ataque (satan) não foi identificado corretamente.

## 6.6. Classificador Preciso para Classe U2R

Rede neural MLP – 41-20-15-6 – foi treinada para identificar os 4 padrões da classe U2R presentes na base de treinamento com precisão. A rede foi treinada com os subconjuntos DS1 e DS4 – DS4 possui apenas registros da classe U2R e normais.

Para esta classe de ataques a rede não foi capaz de detectar precisamente os padrões. Quando treinada com o subconjunto DS1 conseguiu operar apenas como classificador binário detectando conexões como normal ou intrusão. Para a versão treinada com o subconjunto DS4 a rede conseguiu identificar corretamente apenas padrões da classe normal.



| | | Previsto | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | mscan | ipsweep | nmap | satan | Taxa Detecção |
| Real | Normal | 60155 | 406 | 0 | 0 | 0 | 0 | 0.9928 |
| | Outros | 23670 | 226635 | 0 | 0 | 0 | 0 | 0.9051 |
| | rootkit | 7 | 6 | 0 | 0 | 0 | 0 | 0.0000 |
| | perl | 2 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | loadmodule | 1 | 1 | 0 | 0 | 0 | 0 | 0.0000 |
| | buffer_overflow | 17 | 5 | 0 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | 0.9221 |

**Tabela 6-48 : CM Classe U2R – DS1**

| | | Previsto | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | mscan | ipsweep | nmap | satan | Taxa Detecção |
| Real | Normal | 60593 | 0 | 0 | 0 | 0 | 0 | 1.0000 |
| | Outros | 250397 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | rootkit | 13 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | perl | 2 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | loadmodule | 2 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | buffer_overflow | 22 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | 0.1948 |

**Tabela 6-49 : CM Classe U2R – DS4**

## 6.7. Classificador Preciso para Classe R2L

Para a classe remoto para local – R2L – existem 8 padrões distintos de ataque na base de dados de treinamento. Uma rede neural MLP 41-20-15-10 foi treinada para detectar estes 8 padrões, além de padrões representando conexões normais e uma última classe representando todos os outros ataques e intrusões.

| | | Previsto | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | Warezmaster | Guess_passwd | Multihop | Imap | Spy | ftp_write | Warezclient | Phf | Taxa Detecção |
| Real | Normal | 59503 | 1048 | 2 | 2 | 2 | 0 | 0 | 3 | 0 | 1 | 0.9820 |
| | Outros | 18798 | 225536 | 0 | 23 | 1 | 0 | 0 | 2 | 0 | 1 | 0.8795 |
| | warezmaster | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | guess_passwd | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | multihop | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | imap | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | spy | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | ftp_write | 15 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0.0000 |
| | warezclient | 4356 | 8 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | phf | 492 | 10 | 0 | 1 | 8 | 0 | 0 | 511 | 0 | 68 | 0.5667 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | | | | | 0.8933 |

**Tabela 6-50 : CM Classe R2L - DS1**

| | | Previsto | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Normal | Outros | Warezmaster | Guess_passwd | Multihop | Imap | Spy | ftp_write | Warezclient | Phf | Taxa Detecção |
| Real | Normal | 60563 | 0 | 0 | 23 | 0 | 0 | 0 | 0 | 1 | 0 | 0.9995 |
| | Outros | 244178 | 0 | 0 | 74 | 0 | 0 | 11 | 0 | 3 | 0 | 0.0000 |
| | warezmaster | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | guess_passwd | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | multihop | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | imap | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | spy | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | ftp_write | 15 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | warezclient | 4363 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0000 |
| | phf | 906 | 0 | 0 | 26 | 0 | 0 | 2 | 0 | 0 | 0 | 0.0000 |
| | Precisão Geral (AC – “Accuracy”) | | | | | | | | | | | 0.1910 |

**Tabela 6-51 : CM Classe R2L – DS5**

A tentativa de identificação precisa para as classes R2L e U2R não apresentou desempenho satisfatório em nenhum caso. O número reduzido de ocorrências de padrões destas duas classe é uma explicação para a falha da rede aprender corretamente estes padrões. Em uma situação real, o percentual de pacotes representando ataques desta classe é usualmente muito inferior ao percentual de padrões normais, negação de serviço ou reconhecimento. Mesmo para um alto número de intrusões, pois a natureza dos ataques desta classe envolve, tipicamente, poucos pacotes por ataque.

Esta péssimo desempenho torna necessário a utilização de outras técnicas em conjunto com sistemas de redes neurais.

## 6.8. Comitê de Redes Especialistas

Comitê de redes neurais especialistas são sistemas que combinam as respostas de várias redes para gerar uma resposta final. O objetivo é que esta combinação gere uma resposta final melhor que a resposta individual de qualquer rede pertencente ao comitê. Utilizando as diversas redes treinadas como classificadores binários, como um comitê, efetuou-se a análise do resultado final quando as saídas individuais são combinadas pela média e pelo voto majoritário (o padrão é considerado uma intrusão quando a maioria das redes o considera uma intrusão).

### 6.8.1. Decisão por voto majoritário

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60591 | 2 |
| | Intrusão | 228727 | 21709 |

**Tabela 6-52 : CM Comitê por voto majoritário**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.2646 |
| TP | 0.0867 |
| FP | 0.0000 |
| TN | 1.0000 |
| FN | 0.9133 |
| P | 0.9999 |

**Tabela 6-53 : Parâmetros Comitê por voto majoritário**

Este comitê apresentou um excelente desempenho para identificar padrões normais (errou apenas em 2 casos). Entretanto, seu desempenho com limiar em zero foi muito ruim para identificar intrusões. Ajustando o limiar, como mostrado na curva ROC a seguir, as taxas de acerto se tornam razoáveis. Entretanto os resultados obtidos por esta combinação de redes especialistas não é melhor que várias redes individuais.



### 6.8.2. Decisão pela Média

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60592 | 1 |
| | Intrusão | 217232 | 33204 |

**Tabela 6-54 : CM Comitê pela média**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.3016 |
| TP | 0.1326 |
| FP | 0.0000 |
| TN | 1.0000 |
| FN | 0.8674 |
| P | 1.0000 |

**Tabela 6-55 : Parâmetros Comitê pela média**

Novamente, uma excelente capacidade de detectar padrões normais e uma péssima capacidade de detectar intrusões com limiar th = 0. A curva ROC mostra que esta rede tem bom desempenho geral quando limiar é ajustado.

### 6.8.3. Decisão por algoritmo adaptativo proposto

Foi desenvolvido um algoritmo adaptativo de combinação de redes neurais. O princípio deste algoritmo foi selecionar de forma adaptativa quais redes devem ter direito a voto no processo final baseado em análise empírica e processo de tentativa e erro. O algoritmo faz uso da rede neural que identifica a classe do padrão (normal, reconhecimento, negação de serviços, U2R e R2L) e do comitê baseado na média. A lógica do algoritmo proposta esta esquematizada a seguir :

Se ( RN_Classe = Normal ) & (Comitê_Média (P1,th) = “Normal”)

– Resposta = Normal

- Senão Se (RN_Classe = ( DoS ou Probe )) &
- ( Comitê_Média (P2,th) = “Ataque”)
  - Resposta = Intrusão
- Senão Se (RN_Classe = (R2L ou U2R)) & ( Comitê_Media(P3,th) = “Ataque”)
  - Resposta = Intrusão
- Senão

  Resposta = Resposta ( Comitê_Média, th )

A matriz de confusão e parâmetros associados indicam que o algoritmo proposto conseguiu o melhor desempenho para o limiar de decisão th=0. Apenas um caso de padrão normal não foi identificado corretamente e quase 95% dos casos de intrusão também foram acertadamente identificados.

| | | Previsto | |
|---|---|---|---|
| | | Normal | Intrusão |
| Real | Normal | 60592 | 1 |
| | Intrusão | 14309 | 236075 |

**Tabela 6-56 : CM para Algoritmo de decisão proposto**

| Parâmetros Associados | Valor |
|---|---|
| AC | 0.9540 |
| TP | 0.9429 |
| FP | 0.0000 |
| TN | 1.0000 |
| FN | 0.0571 |
| P | 1.0000 |

**Tabela 6-57 : Parâmetros para Algoritmo de decisão proposto**

### 6.8.4. Curvas ROC

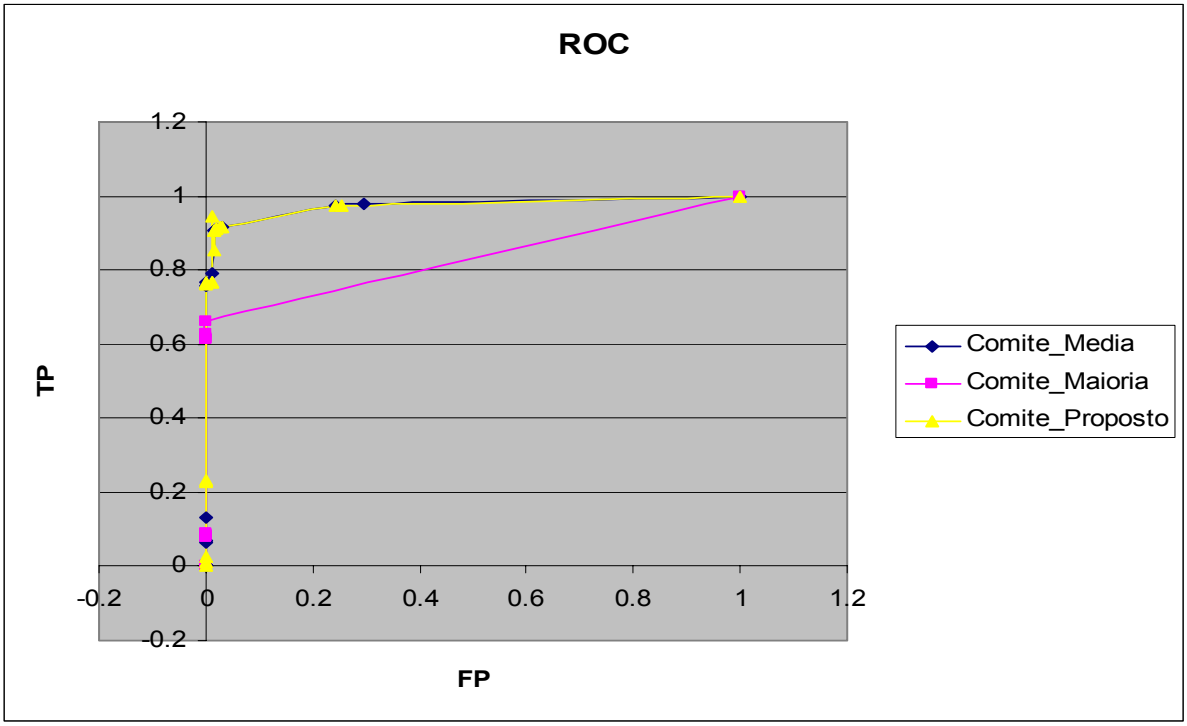


**Figura 6-34 : ROC para Comitês – TP x FP**

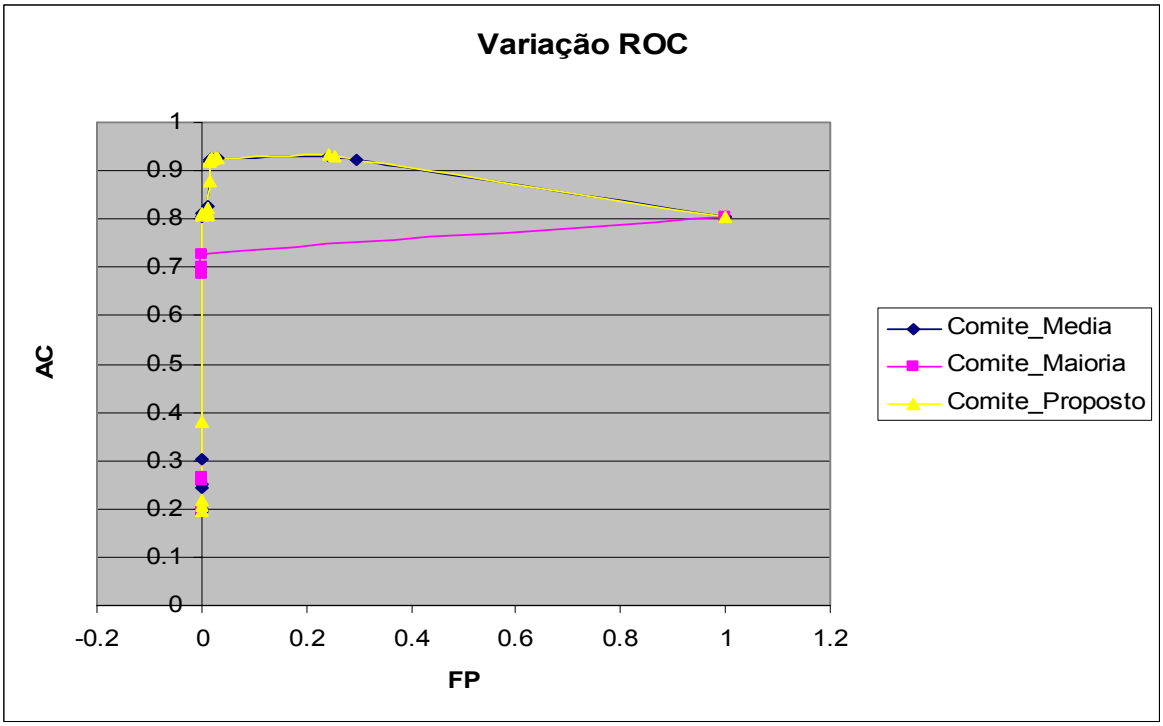


**Figura 6-35 : Variação ROC para Comitês – AC x FP**

As curvas ROC mostram que o comitê pela média consegue um desempenho muito similar ao algoritmo proposto. Este tem, entretanto, a vantagem de fornecer o melhor desempenho sem necessitar de ajustes no limiar de decisão.