

## **Proposta ESR/RNP nº6821/2022**

Ao

Sr. Rosemberg Maia Gomes

Tribunal Regional Eleitoral do Piauí - TRE-PI

### **I - Apresentação da Escola Superior de Redes RNP**

Excelência em ensino na área de Tecnologia da Informação e Comunicação. Esta é a proposta da Escola Superior de Redes (ESR). Há mais de 25 anos gerenciando a Internet acadêmica nacional, a Rede Nacional de Ensino e Pesquisa (RNP) criou a Escola Superior de Redes com o objetivo de disseminar o conhecimento em tecnologias da informação e comunicação. A formação é prática com atividades em laboratório de informática que são desenvolvidas para refletir as situações, problemas e desafios encontrados no dia a dia do profissional de redes.

A Rede Nacional de Ensino e Pesquisa (RNP), através da rede Ipê, provê serviço Internet com facilidades de trânsito nacional e internacional em uma infraestrutura com alta largura de banda e suporte a aplicações avançadas.

Os cursos da Escola Superior de Redes foram elaborados para que sua empresa aumente a eficiência no uso de redes digitais e no conjunto de aplicações de comunicação e colaboração, que permitem reduzir custos operacionais, para trazer mais agilidade para os negócios e garantir maior segurança das informações.

### **II - Área temática**

#### **Segurança**

As notáveis vantagens trazidas pela Internet, como o comércio eletrônico e as transações bancárias on-line, facilitam a nossa vida, mas ao mesmo tempo atraem riscos que tem forte impacto na área de segurança da informação. A metodologia da ESR é capacitar o aluno para pensar preventivamente e tratar os incidentes quando não for possível evitá-los. As atividades práticas refletem a realidade do analista de segurança ao lidar com incidentes de segurança e investigações forenses, tornando-o um profissional valorizado nas corporações.

[esr.rnp.br](http://esr.rnp.br)

(61) 3243-4337

(61) 3243-4340

(61) 3243-4341 fax

### III - Cursos oferecidos

Curso	Local	Data prevista
Correlacionamento de eventos com Graylog (SEG35)	ESR EaD	07/11 a 18/12/2022

### IV - Público alvo

Servidores de TI do Tribunal Regional Eleitoral do Piauí da Secretaria da Coordenação de Desenvolvimento e Infraestrutura.

### V - Material didático

- ▲ A ESR oferecerá apenas materiais digitais no Ambiente Virtual de Aprendizagem (AVA) para todos os treinamentos da proposta, e inclui: conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro online;
- ▲ Os conteúdos dos cursos no AVA ficarão disponíveis permanentemente para os alunos;
- ▲ O aluno terá acesso a agenda do curso no AVA, com todas as informações das atividades propostas.

### VI - Número de vagas

Serão oferecidas 2 (dois) vagas, conforme cronograma proposto.

### VII - Carga horária

- ▲ O curso *Correlacionamento de eventos com Graylog (SEG35)* é dividido em 10 sessões de aprendizagem, totalizando 40 horas cada turma;
- ▲ A carga horária dos cursos da ESR são distribuídas em 50% de aulas EaD síncrona e 50% de auto estudo, conforme ementa.

### VIII - Infraestrutura

- ▲ Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- ▲ Para os encontros online recomendamos o uso de fones de ouvido com microfone;
- ▲ As aulas EaD são síncronas e com interação, podendo ser por Teams, zoom, webconf ou similar;
- ▲ O conteúdo do curso é acessado diretamente no Ambiente Virtual de Aprendizagem (AVA) do curso;
- ▲ O acesso à plataforma EaD da ESR é de responsabilidade do aluno;

- ▲ A ESR não fornecerá equipamentos ou link de internet para realização do curso.

## IX - Pré-matricula

Após a validação desta proposta, o responsável pelo aceite deverá realizar as pré-matrículas dos colaboradores no endereço encaminhado pela Escola Superior de Redes RNP.

Somente as inscrições realizadas por este endereço serão consideradas válidas.

## X - Local e horário da realização do curso

**Local: ESR EaD**

**Turma:**

- ▲ **Correlacionamento de eventos com Graylog (SEG35):** 07/11 a 18/12/2022 – Modalidade EaD. Este curso possui 10 encontros online, às quartas e sextas-feiras de 16h às 18h, nos dias: 09, 11, 16, 18, 23, 25 e 30 de Novembro e 02, 07 e 09 de Dezembro de 2022. Encontros sujeitos a alteração.

As aulas ficarão gravadas e serão disponibilizadas no AVA (Ambiente Virtual de Aprendizagem) após 24 horas de sua realização, disponíveis permanentemente. Alertamos que o fato de assisti-las fora do horário do Encontro Online (ao vivo), não contará como presença no curso.

## XI - Instrutoria

- ▲ Os tutores da Escola Superior de Redes RNP possuem sólida formação acadêmica e profissional.

## XII - Certificado de participação

Para conclusão do curso do **portfólio ESR** e acesso ao certificado é necessário:

- ▲ Entregar no mínimo 50% das tarefas;
- ▲ Ter 50% de presença no total de encontros online;
- ▲ Obter média 6,0 (seis) no Questionário de Avaliação final;

Não é possível a postergar a data final de entrega de atividades: os alunos que não finalizarem as tarefas obrigatórias serão reprovados.

Os certificados da ESR são online, disponíveis no perfil de cada participante em PDF, com URL para verificação de autenticidade.

### XIII - Investimento

Curso	Valor unit. (R\$)	Desconto (%)	Qtde.	Valor total (R\$)
Correlacionamento de eventos com Graylog (SEG35)	2.000,00	0,00000	2	4.000,00
Total geral de vagas e investimento			2	4.000,00

O investimento total para 2 (dois) pessoas é de R\$ 4.000,00 (quatro mil Reais), inclusos os impostos: COFINS 7,60% e ISS 5%.

### XIV - Forma de pagamento

O pagamento deverá ser efetuado da seguinte forma:

- ▲ Nota de empenho emitida pela instituição contratante e encaminhada a Escola Superior de Redes RNP.

Após o término do curso o setor financeiro da Rede Nacional de Ensino e Pesquisa encaminhará a nota fiscal emitida em 02 (duas) vias, com o valor total do curso.

#### Dados da RNP

##### Rede Nacional de Ensino e Pesquisa - RNP

CNPJ: 03.508.097/0001-36

Inscrição Municipal: 283810-9

Endereço: Rua Lauro Müller, 116 - sala 1103

Botafogo - Rio de Janeiro - RJ

22290-906

#### Dados bancários

Banco do Brasil

Agência: 1769-8

Conta Corrente: 127000-1

Ressaltamos que pelo fato da RNP ser uma Organização Social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e ao Ministério da Educação (MEC) a mesma é dispensada de licitação, conforme a Lei 8.666, Artigo 24, Inciso XXIV. A RNP possui inscrição no SICAF.



## XV - Condições gerais da proposta

### Aceitação

A aceitação da proposta poderá ser inicialmente enviada via e-mail para [atendimento@esr.rnp.br](mailto:atendimento@esr.rnp.br), aos cuidados de *Leandro Marcos de Oliveira Guimarães*.

No ato da aceitação da proposta a Empresa Contratante deverá fornecer a Escola os seguintes dados: Razão Social, CNPJ, Inscrição Estadual e/ou Municipal ou se isento, nome e cargo da pessoa responsável, endereço completo, e-mail, telefones, lista dos participantes, nome e endereço do contato para envio da nota fiscal.

### Validade

A proposta é válida até dia 04/11/2022.

### Início da turma

Quórum: ocupação mínima 15 alunos. Caso não seja atendido o quórum, a ESR deverá comunicar, com 20 (vinte) dias de antecedência do início do curso, o cancelamento da turma.

### Não comparecimento

O aluno que não comparecer ao curso na data de início sem prévia comunicação ou não atingir a frequência mínima exigida no item XII desta proposta, será contabilizado e cobrado, não fazendo jus à restituição de valores ou ao crédito de valores já pagos, sendo devido pelo **Contratante** o pagamento da referida vaga.

Brasília, 01 de Setembro de 2022

Atenciosamente,

**Leandro Marcos de Oliveira Guimarães**

Diretor Adjunto da Escola Superior de Redes

Escola Superior de Redes RNP

[atendimento@esr.rnp.br](mailto:atendimento@esr.rnp.br)

(61) 3243-4337 / 4355

(61) 3243-4341 fax

Nome e assinatura do responsável

---

**Sr. Rosemberg Maia Gomes**

Data do aceite

\_\_\_\_/\_\_\_\_/\_\_\_\_

# A experiência de quem trouxe a internet para o Brasil agora mais perto de você

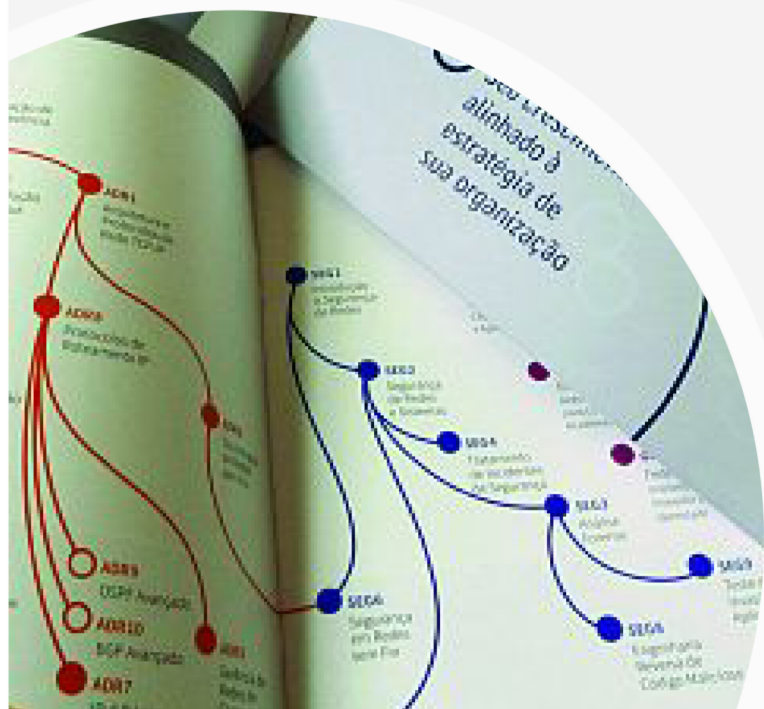
## A Escola

A Escola Superior de Redes da RNP privilegia um ensino totalmente prático. Os laboratórios são montados de forma a proporcionar ao aluno um ambiente com os mesmos recursos e ferramentas que ele encontra no mercado de trabalho, bem como as atividades propostas espelham o dia-a-dia do profissional de Tecnologia da Informação e Comunicação. Os laboratórios estão conectados à Internet por meio do backbone de alta velocidade da Rede Nacional de Ensino e Pesquisa (RNP).

Cursos práticos voltados para o crescimento do profissional de TI

Cursos práticos intensivos em Tecnologias da Informação e Comunicação (TIC) nas seguintes áreas:

- ▲ Segurança



# Conheça as ferramentas de segurança e aprenda como evitar e tratar incidentes de segurança.

## Segurança

As notáveis vantagens trazidas pela Internet, como o comércio eletrônico e as transações bancárias on-line, facilitam a nossa vida, mas ao mesmo tempo atraem riscos que tem forte impacto na área de segurança da informação. A metodologia da ESR é capacitar o aluno para pensar preventivamente e tratar os incidentes quando não for possível evitá-los. As atividades práticas refletem a realidade do analista de segurança ao lidar com incidentes de segurança e investigações forenses, tornando-o um profissional valorizado nas corporações.

### Correlacionamento de eventos com Graylog

Este curso possui 10 encontros online, às quartas e sextas-feiras de 16h às 18h, nos dias: 09, 11, 16, 18, 23, 25 e 30 de Novembro e 02, 07 e 09 de Dezembro de 2022. **Encontros sujeitos a alteração**

Duração: 40h





**Este curso possui 10 encontros online, às quartas e sextas-feiras de 16h às 18h, nos dias: 09, 11, 16, 18, 23, 25 e 30 de Novembro e 02, 07 e 09 de Dezembro de 2022. Encontros sujeitos a alteração**

## **Correlacionamento de eventos com Graylog**

O curso ensina o aluno sobre os aspectos teóricos e legais sobre a gestão de logs e retenção de dados, e como operacionalizar esses procedimentos com o SIEM open source Graylog. Além da instalação, configuração e manutenção da ferramenta, também são tratados tópicos como a criação de filtros e pipelines de processamento de eventos, construção de dashboards amigáveis e alertas administrativos.

### **Características**

#### **DURAÇÃO:**

- ▲ 5 semanas de duração e mais uma semana de encerramento (total de 6 semanas);
- ▲ 2 encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 horas de duração;

#### **SISTEMA DE AVALIAÇÃO:**

**Para conclusão do curso e acesso ao certificado é necessário:**

- ▲ Obter média 6,0 (seis) no Questionário de Avaliação final;
- ▲ Entregar no mínimo 50% das tarefas;
- ▲ Ter 50% de presença no total de encontros online.

#### **MATERIAL:**

- ▲ O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários ou simulados materiais extras e vídeo do encontro online.

#### **TÉCNICA:**

- ▲ Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;



- ▲ Para os encontros online recomendamos o uso de fones de ouvido com microfone.

### Competências desenvolvidas

- ▲ Compreender a importância da coleta e correlacionamento de eventos em larga escala, do ponto de vista da segurança da informação, para organizações de todos os portes.
- ▲ Instalar, configurar, integrar e realizar procedimentos de manutenção em um cluster SIEM Graylog.
- ▲ Configurar sistemas diversos para envio de registros para processamento pelo SIEM Graylog.
- ▲ Criação de filtros, pipelines de processamento e lookup tables para viabilizar indexação de informações complexas.
- ▲ Pesquisar, correlacionar, criar alertas e dashboards para eventos coletados.

### Conhecimentos prévios

- ▲ Recomenda-se que o aluno possua conhecimentos avançados em operação de servidores Linux em linha de comando, bem como servidores Windows.
- ▲ Conhecimentos básicos em segurança da informação.
- ▲ Noções básicas de processamento de arquivos-texto, expressões regulares e programação.

### Investimento

- ▲ R\$ 2.000,00

### Programa do curso

- ▲ Introdução à gestão de logs
- ▲ Arquitetura e instalação do Graylog
- ▲ Usuários, papéis e integração com sistemas externos
- ▲ Coleta e ingestão de logs
- ▲ Expressões regulares, padrões GROK e filtros
- ▲ Pipelines de processamento e lookup tables
- ▲ Plugins, Content Packs e geolocalização de informações
- ▲ Pesquisando registros
- ▲ Configuração de alertas e dashboards
- ▲ Procedimentos de manutenção, backup e atualização



esr.rnp.br





### Segurança

Correlacionamento de eventos com Graylog  
(SEG35)

### Investimento

R\$ 2.000,00



[esr.rnp.br](http://esr.rnp.br)



**RNP**

