TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Informação Nº 56 - TRE/PRESI/DG/SGP/COEDE/SECAL

Senhora Coordenadora,

Por meio do Memorando nº 25/2023, evento (0001901815), a Coordenadoria de Desenvolvimento e Infraestrutura - CODIN/STI/TRE-PI, através de seu Coordenador Rosemberg Maia Gomes**,** pleiteia a contratação do **Curso ANÁLISE FORENSE**, oferecido pela **Escola Superior de Redes**, a ser realizado no período de 09/10/2023 a 26/11/2023. O supracitado curso será realizado na modalidade EaD, para 04 (quatro) servidores deste Regional e possui carga horária de 40 h/a.

Trata-se de evento contemplado na relação de cursos previstos para o Plano Anual de Capacitação de TI 2023 (evento 0001794074), com previsão de custo no valor de **R$ 5.200,00 (cinco mil e duzentos reais).**

A Unidade demandante pleiteia que o curso deverá ser ministrado pela Escola Superior de Redes em virtude das razões expostas no doc. 0001901724. O curso será realizado na modalidade EAD, com carga horária de 40 h/a - 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 6 semanas); 2 (dois) encontros online por semana com o tutor (total de10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração, de acordo com a programação prevista na Proposta e Conteúdo Programático, documento acima citado.

Os objetivos do Curso estão explanados no Doc. 0001901724, dentre os quais constam: Utilizar ferramentas forenses em uma investigação; Elaborar uma cronologia, descrevendo cada evento do comprometimento investigado; Coletar informações relacionadas aos programas executados, às bibliotecas do sistema e portas relacionadas;Identificar o tipo de auditoria mais adequado para cada caso.

Seguem as demais informações complementares do evento:

EVENTO	**Curso Análise Forense**
Período Previsto	09/10/2023 a 26/11/2023
Modalidade	EaD
Carga Horária	40 h/a
Unidade Solicitante	Coordenadoria de Desenvolvimento e Infraestrutura - CODIN/STI/TRE-PI
Público Alvo	04 (quatro) Servidores da STI
Valor da contratação	R$ 5.200,00 (cinco mil e duzentos reais)
Dados da Empresa	Escola Superior de Redes Rede Nacional de Ensino e Pesquisa - RNP CNPJ: 03.508.097/0001-36

EVENTO	Curso Análise Forense

Segue, em anexo aos autos, para a devida instrução: a) Proposta do curso (0001901724), b) Projeto básico do curso, abaixo, c) Currículo (0001901726), d) Certidões Negativas 0001901771, 0001901777 e 0001901780; sem prejuízo de verificação pelos setores competentes da regularidade fiscal da empresa. Ademais, registramos que a empresa não apresentou notas de empenho referentes à contratação do curso por outros órgãos vez que não houve a realização da citada capacitação após a pandemia da COVID-19.

À consideração, para os encaminhamentos devidos, relembrando que à luz do art. 7º da Portaria TRE - PI nº. 338/2010, impõe-se a comunicação prévia das iniciativas para execução do Plano Anual de Capacitação à Direção-Geral.

À consideração, para os encaminhamentos devidos.

Cristiane Falcão Nogueira

TRE – PI/SGP/COEDE/SECADO

ANEXO

PROJETO BÁSICO

OBJETO:

Curso Análise Forense

JUSTIFICATIVA:

Capacitar os participantes para utilizar ferramentas forenses em uma investigação; elaborar uma cronologia, descrevendo cada evento do comprometimento investigado; cole programas executados, às bibliotecas do sistema e portas relacionadas; identificar o tipo de auditoria mais adequado para cada caso.

ESPECIFICAÇÃO DO SERVIÇO:

Contratação da **Escola Superior de Redes** para ministrar uma turma do **Curso Análise Forense**, na modalidade virtual - 5 (cinco) semanas de duração e mai (total de 6 semanas); 2 (dois) encontros online por semana com o tutor (total de10 encontros). Os encontros serão ao vivo e terão2 (duas) horas de duração;

O curso terá duração de 40 h/a.

Período de realização: 09/10/2023 a 26/11/2023.

Nível do Curso - Intermediário.

CONTEÚDO PROGRAMÁTICO:

- Princípios de análise forense
- Conceito de análise forense
- Motivação
- Modo de ação dos atacantes
- Tipos de sistemas comprometidos
- Procedimentos
- Cadeia de custódia de evidências
- Metodologia para análise forense
- Cadeia de custódia de evidências
- Ciência Forense
- Abordagens de coleta de evidências
- Cadeia de custódia e garantia de integridade
- Coleta de evidências – parte 1
- Importância da coleta de evidências
- Metodologia inicial de coleta – first responders
- Coleta de evidências – armazenamento em massa
- Coleta de evidências – memória
- Coleta de evidências – parte 2
- Coleta de evidências – rede / artefatos web: email e navegadores / log
- Análise de evidências – Disco
- Estrutura básica de sistemas de arquivos
- Análise de disco

- Ferramentas de recuperação de dados
- Análise de Memória
- Conceitos de memória volátil
- Análise de memória física
- Análise de memória virtualizada
- Análise de tráfego de rede
- Capturas de tráfego e TCP/IP
- Análise de tráfego de rede
- Análise de artefatos Web: e-mail e Navegadores
- Análise de Logs e Laudo Forense
- Importância dos logs em análise forense
- Tipos de arquivos de logs
- Análise de logs
- Laudo Forense
- Análise forense avançada em Windows
- Exercício de Capture-The-Flag contendo:
- Coleta de informações de: redes; registros do Windows; registros de eventos
- (logs)
- Análise de conteúdo do: Recycle.Bin; Clipboard e de arquivos
- Recuperação de dados ocultos ADS
- Análise do histórico de navegação
- Recuperação de senhas.

CONHECIMENTOS PRÉVIOS:

- Recomenda-se que o aluno tenha feito o curso Segurança de Redes e Sistemas, oferecido pela Escola Superior de Redes;
- Sólidos conhecimentos sobre o funcionamento de sistemas Linux e Windows e protocolo TCP/IP;
- Conhecimento básico sobre investigação de incidentes de segurança.

OBJETIVOS ESPECÍFICOS:

- Utilizar ferramentas forenses em uma investigação;
- Elaborar uma cronologia, descrevendo cada evento do comprometimento investigado;
- Coletar informações relacionadas aos programas executados, às bibliotecas do sistema e portas relacionadas;
- Identificar o tipo de auditoria mais adequado para cada caso.

PÚBLICO ALVO:

04 (quatro) Servidores da STI/TRE-PI.

FISCALIZAÇÃO:

A fiscalização do serviço referente ao curso em comento ficará a cargo da Coordenadoria de Desenvolvimento e Infraestrutura - CODIN/STI/TRE-PI, media em conformidade com a proposta apresentada.

PAGAMENTO:

O pagamento será mediante depósito na conta bancária da empresa contratada, após a apresentação da nota fiscal devidamente atestada pela Unidade Demanda

Documento assinado eletronicamente por **Cristiane Falcao Nogueira**, **Analista Judiciário**, em 28/08/2023, às 13:10, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001903673** e o código CRC **F782F584**.

0006293-32.2023.6.18.8000 0001903673v60

--