



ESTUDO TÉCNICO PRELIMINAR Nº 003/2023-NSI/STI

Unidade Interessada: NÚCLEO DE SEGURANÇA DA INFORMAÇÃO / SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Assunto: Contratação do Curso Oficial do Cert® Division ***“Advanced Topics in Incident Handling – ATIH”***.

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento de demandas, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

OBJETO DA CONTRAÇÃO

O presente estudo tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de ação de treinamento/capacitação destinada às atividades de Gestão de Incidentes e Segurança Cibernética, via inscrição de 02 (dois) Servidores do TRE AM no Curso Oficial do Cert® Division ***“Advanced Topics in Incident Handling – ATIH”***.

O curso ocorrerá no modelo presencial, em São Paulo/SP, no período de 23 a 27 de outubro de 2023, com carga horária de 40 (quarenta) horas-aula, em turma previamente selecionada e aprovada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.Br.

ESTUTO TÉCNICO PRELIMINAR

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

O Tribunal Regional Eleitoral do Amazonas possui ambiente informatizado composto por diversas bases de dados, tecnologias, sistemas e usuários que, juntos, se mostram em elevada complexidade para gestão da segurança da informação.

Junto com a transformação digital, fruto da evolução tecnológica, observamos cada vez mais vulnerabilidades, riscos e ameaças que são exploradas por hackers para acesso indevido a informações e apropriação/destruição de dados.

De acordo com o relatório de violação de dados de janeiro de ano 2023 da Identity Theft Resource Center - ITRC, houve exposição de registros, sensíveis ou não, em centenas de vazamentos:

Number of 2022 Compromises								
Total Data Compromises: 1,802 Compromises; 422,143,312 Victims				Compromises by Industry: Q4 2022/2022 YTD vs. Full Years 2021 & 2020				
Data Breaches: 1,774 Data Breaches; 392,180,551 Victims		Data Exposures: 18 Data Exposures; 7,146,425 Victims		Compromises	Victims	Compromises	Victims	2021
Education	35	695,961	100	1,745,226	125	1,687,192	42	974,054
Financial Services	75	1,628,050	268	27,146,354	279	19,978,108	138	2,687,084
Government	22	717,793	74	1,739,462	66	3,244,455	47	1,100,526
Healthcare	89	9,429,886	344	26,259,933	330	30,853,767	306	9,700,238
Hospitality	13	131,181	34	69,235,147	33	238,445	17	22,365,384
Manufacturing & Utilities	70	341,430	249	23,897,836	222	49,782,583	70	2,896,627
Non-Profit/NGO	20	265,389	71	980,021	86	2,339,646	31	37,528
Professional Services	60	1,304,938	224	6,248,711	184	22,729,391	144	73,012,145
Retail	15	102,870	65	792,195	102	7,212,912	53	10,710,681
Technology	34	229,840,738	86	248,564,988	79	44,684,180	67	142,134,883
Transportation	11	630,817	36	3,991,847	44	569,684	21	1,208,292
Other	68	7,239,325	251	11,541,592	308	79,660,479	172	43,391,302
Unknown	-	-	-	-	4	35,232,664	-	-
Totals	512	252,328,378	1,802	422,143,312	1,862	298,213,506	1,108	310,218,744

Tab. 1 – Data Breach Analysis: Year End 2022. Fonte: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report+

Nos últimos anos, o Brasil vem registrando incidentes de segurança cibernética graves que afetaram diretamente os usuários brasileiros. Em 2020, por exemplo, um ataque de *ransomware* afetou mais de 200 órgãos governamentais brasileiros, incluindo o Ministério da Educação. Em 2021 e 2022 foram



registrados diversos outros incidentes de segurança cibernética relacionados ao roubo de informações confidenciais dos usuários, inclusive no âmbito do Poder Judiciário.

Mais recentemente, foi noticiado por um Tribunal Regional Eleitoral a exploração de vulnerabilidade em sua rede, cuja instalação de um *ransomware* acarretou no sequestro de grande quantidade de dados.

Diante desse cenário complexo, é imprescindível o treinamento e qualificação de uma equipe dedicada ao monitoramento, prevenção e reposta a incidentes de segurança no âmbito do TRE AM.

2. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

Os cursos de capacitação em cibersegurança foram indicados para compor o Plano Anual de Capacitação 2023, em elaboração pelo Núcleo de Gestão e Governança da SGP (Pad. nº 420/2023, Doc. nº 17119/2023).

3. REQUISITOS DA CONTRATAÇÃO

Os requisitos específicos para a presente contratação constarão do Termo de Referência correspondente.

4. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

Encontram-se previamente aprovados pela contratada, 02 (dois) Servidores para participar do curso.

5. LEVANTAMENTO NO MERCADO

Trata-se de curso exclusivo, cuja participação é reservada à candidatos que tenham realizado o curso *Foundations of Incident Management* – FIM, ou ter completado o curso *Fundamentals of Incident Handling*, além de serem avaliados e selecionados pela Empresa contratada.

Não foram encontradas no mercado local ações de treinamento que atendam a necessidade da unidade requerente.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Inscrição individual: R\$ 3.300,00 (três mil e trezentos reais)

Valor Total: R\$ 6.600,00 (seis mil e seiscentos reais)

Inclusas neste valor todas as despesas diretas ou indiretas da Empresa contratada, decorrentes do fornecimento do serviço.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

O curso ***Advanced Topics in Incident Handling - ATIH*** é destinado à pessoal técnico de Grupos de Segurança e Resposta a Incidentes (CSIRTs), em *Security Operations Centers* (SOC's) e outras áreas relacionadas com atividades de Gestão de Incidentes de Segurança Cibernética, tenham realizado o curso *Foundations of Incident Management* – FIM, abordando técnicas para detecção e resposta, tanto de ataques comumente usados, quanto ataques e ameaças emergentes.

Este curso baseia-se fortemente nas ferramentas e métodos discutidos no curso *Foundations of Incident Management* – FIM e fornece passos que *incident handlers* podem seguir para responder a ameaças e ataques complexos, incluindo ameaças persistentes (APTs).

Durante o curso os participantes, através de exercícios interativos, discussões e exercícios em grupo, os irão identificar e analisar um conjunto de eventos e, com auxílio dos instrutores, propor estratégias de resposta apropriadas. Os participantes também terão contato com atividades mais avançadas relacionadas com tratamento de incidentes, como *threat hunting*, análise de artefatos e *malware*, análise de vulnerabilidades e comunicação e publicação de informações.

Serão abordados:

- revisão do ciclo de vida do tratamento de incidentes;
- ameaças avançadas persistentes (APTs);
- revisão das técnicas e categorias de análise de malware e de artefatos;
- causas fundamentais das vulnerabilidades;
- tratamento de vulnerabilidades;
- análise, coordenação e resposta a major events e incidentes complexos;



-
- desenvolvimento de publicações e comunicações eficazes.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se justifica o parcelamento da contratação, em face de seu valor e da execução imediata do serviço, após a contratação, no presente exercício.

9. DEMONSTRATIVOS DOS RESULTADOS PRETENDIDOS

Após o curso, os participantes estão capacitados à:

- detectar e caracterizar vários tipos de ataques;
- desenvolver estratégias para analisar e responder a eventos e incidentes complexos em sua organização;
- compreender os diversos métodos para analisar artefatos encontrados em sistemas comprometidos e as dificuldades envolvidas nesta análise;
- executar atividades de *threat hunting*, incluindo a definição dos objetivos;
- obter experiência prática na coordenação de tarefas de tratamento de vulnerabilidades;
- formular e entregar publicações e comunicações eficazes, tais como alertas, relatórios pós-ação e briefings para a alta gestão.

10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Em conformidade com o princípio da economicidade, considerando a disponibilidade orçamentária, será realizada a análise de custo-benefício da contratação do curso, considerando o custo, as necessidades de cibersegurança da organização e os conhecimentos e habilidades necessárias para implementar as medidas de cibersegurança no TRE AM.

Será elaborado o Termo de Referência.

Serão verificadas a regularidade fiscal da empresa, sua idoneidade, capacidade técnica e formação de seu corpo pedagógico.

O Termo de Referência, bem como este Estudo Técnico Preliminar e demais artefatos do processo da contratação, serão submetidos à análise jurídica para suporte da apreciação da contratação pela Alta Administração.

Uma vez aprovados, será providenciada a devida publicidade ao ato contratual e emitida a Nota de Empenho (compromisso de pagamento).

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não há no âmbito deste TRE-AM contratações correlatas e/ou interdependentes que conflitem com o objeto da presente contratação.

12. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

Sendo o objeto da contratação executado em outra Unidade da Federação, não haverá utilização de outros recursos materiais no TRE-AM.

13. POSICIONAMENTO CONCLUSIVO

O curso ***“Advanced Topics in Incident Handling – ATIH”*** complementa ao curso ***“Foundations of Incident Management – FIM”*** para o treinamento/capacitação da equipe de resposta e tratamento de incidentes do TRE AM, constituído pela Portaria TRE AM nº 146/2021.

A capacitação dos servidores responsáveis pelo monitoramento, resposta e tratamento de incidentes está em conformidade com as Resoluções CNJ nºs 370 e 391/2021 e a Portaria TRE AM nº 146/2021, bem como ao Tema “Riscos, Segurança da Informação e Proteção de Dados” dos quesitos de avaliação do iGOVTic 2023 para obtenção do Prêmio de Qualidade do Poder Judiciário.

Ante os diversos casos de exploração de vulnerabilidades e sequestro de dados em todos os seguimentos, faz-se necessário a manutenção de ambiente virtual seguro, com protocolos que garantam o monitoramento e a pronta resposta à eventual exploração de vulnerabilidades, através do uso de tecnologias e da qualificação de servidores.