Poder Judiciário Federal
Tribunal Regional do Trabalho da 9.ª Região

ALEXANDRE TETSUO YAMAUCHI 13/05/2026 SIOP TRT9

EDUARDO SILVEIRA ROCHA 13/05/2026 SGTIC TRT9

Demanda de Capacitação SGTIC 2/2026 (ID 17902156)

Documento:

Documento de formalização de demanda de atividade de capacitação aberta para servidores da área de Tecnologia da Informação e Comunicações do Tribunal Regional do Trabalho da 9ª Região, cujo valor do investimento seja inferior ao limite constante no inciso II do art. 75 da Lei 14.133/2021.

À Escola Judicial,

Considerando o Despacho ADG PROAD 1122/2025, que trata da operacionalização e implantação do Ato 312/2024 (“altera a Resolução Administrativa 176/2014, o qual estabelece diretrizes para a capacitação de servidores nas unidades de apoio indireto à atividade judicante neste Tribunal Regional, e altera dispositivos do Ato 305/2019”) e atribui à SGTIC a gerência e execução do Plano de Capacitação, incluindo as questões operacionais relacionadas às instruções, processamento, fiscalização e gestão das contratações.

Em atenção ao disposto nos artigos 23, 68, 72 e 74 da Lei 14.133/2021 (Lei de Licitações e Contratos Administrativos) e nos artigos 18 a 20 da Política nº 77/2023, que institui a Política de Governança de Contratações no âmbito do Tribunal Regional do Trabalho da 9ª Região, solicito a contratação do curso/evento:

1. Curso/Evento: Ethical Hacking Endpoint Protection Evasion - SIOP
2. Empresa promotora: GoHacking Cyber Security LTDA
3. CNPJ da empresa promotora: 44.699.669/0001-99
4. Dados bancários da empresa promotora:
   - Banco: Inter (077)
     Agência: 001
     Conta Corrente: 19953883-2
5. Data/período do curso/evento: 06 de julho a 22 de julho de 2026
6. Horário das atividades:
   - Segundas e quartas: 19h às 23h
   - Sábados: 09h às 17h
7. Carga horária do curso/evento: 40h
8. Modalidade de execução do curso/evento: (On-Line / Presencial / EAD): Curso online ao vivo
9. Local de realização do curso/evento: EAD/Online
10. Valor da inscrição do curso/evento: R$18.000,00

11. Há necessidade de deslocamento: Não
12. Se sim, de onde para onde e meio de transporte a ser utilizado: N/A
13. O curso/evento está aprovado no Plano Anual de Capacitação em vigor? Sim
14. Se sim, informe qual o documento de aprovação: Despacho SGTIC 1107/2025
15. Se não, informe qual a curso/evento aprovado será substituído pelo ora indicado:
16. Servidor(es) a ser(em) inscrito(s) no curso/evento:

ALEXANDRE TETSUO YAMAUCHI 13/05/2026 SIOP TRT9

EDUARDO SILVEIRA ROCHA 13/05/2026 SGTIC TRT9

- Rafael Mendes de Souza – Seção de Servidores Corporativos
- Oscar Luis Nagel - Seção de Servidores Corporativos
- Luis Guilherme Zanlourensi - Seção de Servidores Corporativos
- Charles Maske – Seção de Operação da Segurança da Informação
- Carlos Bruno Fischer – Subseção de Disponibilidade e Capacidade
- Alessandro de Souza - Subseção de Disponibilidade e Capacidade

17. Manifestação da conveniência e oportunidade da participação dos indicados no curso/evento:
    - O curso Ethical Hacking Endpoint Protection Evasion (EHEPE) apresenta técnicas ofensivas de evasão, com a análise das etapas de desenvolvimento de códigos e ferramentas capazes de burlar sistemas de defesa, bem como realiza um estudo de mecanismos de execução de shellcode em ambientes corporativos hardenizados.
      Milhões de dólares são gastos em empresas com soluções de Antivírus, Endpoint Detection and Response (EDR) e monitoramento, contudo a maioria desses controles é contornada por ameaças persistentes avançadas (Advanced Persistent Threats – APT) que, muitas vezes, utilizam técnicas, táticas e procedimentos (Tactics, Techniques and Procedures – TTP) customizados, fazendo com que toda a cadeia de proteção comprada e configurada seja burlada.
      Como os atacantes conseguem executar código malicioso mesmo com proteções ativadas e atualizadas? Como eles se movimentam dentro de uma rede sem deixar alertas em sistemas de detecção? Como eles conseguem contornar proteções como Applocker, Sysmon, ETW, LAPS, CLM dentre outras e serem bem-sucedidos na propagação de malwares dentro de uma rede corporativa? Como eles fazem para utilizar outros canais para exfiltração de dados e não serem pegos? Essas e outras perguntas serão respondidas nesse treinamento, que possui uma abordagem 100% prática, conduzido por laboratórios e exercícios que farão com que o aluno compreenda em detalhes os tópicos mencionados.
      O curso trabalha técnicas atuais de evasão de antivírus e hardening em ambientes atualizados. Serão apresentados TTP de ataques, bem como o desenvolvimento de outras ferramentas para execução de código malicioso, das mais simples até técnicas utilizadas por APT, pontos fundamentais tanto para atividades ofensivas (Pentesters, Red Team) quanto para as atividades de defesa (Blue Team, Threat Hunting, CSIRT, SOC).
      Diversos temas serão abordados, tais como: entendimento de antivírus, evasão de detecções por assinatura, evasão de detecções por heurística, P /Invoke, D/Invoke, Reflection, desenvolvimento de shellcode runners

/malwares, ofuscação, evasão de Applocker, evasão de LAPS, evasão de Applocker, movimentação lateral evasiva, evasão de AMSI, entre outros.
O conhecimento dessas técnicas e a capacidade de aplicar as medidas apropriadas de monitoramento e proteção são fundamentais para ampliar a segurança cibernética do ambiente de estações de trabalho (endpoint) do TRT9.

18. Justificativa da necessidade de participação do(s) servidor(es) no curso/evento:

Ataques cibernéticos em ambientes corporativos podem ter como início o comprometimento de endpoints: estações de trabalho, notebooks, servidores de rede, entre outros, usados para acesso e transferência de dados da organização.

Apesar do investimento em soluções voltadas para a proteção desses ativos, os invasores utilizam técnicas cada vez mais sofisticadas para contorná-las, representando um risco potencial para os ativos de informação da instituição.

Além do risco de vazamento de dados sensíveis, como informações cadastrais e dados processos ainda em andamentodicionalmente, o comprometimento do ambiente por atores maliciosos pode resultar na indisponibilidade dos recursos da rede, afetando diretamente a produtividade dos funcionários e trazendo prejuízos para a prestação jurisdicional, bem como para a reputação da organização.

A participação dos servidores indicados visa capacitá-los a implementar medidas de segurança para aumentar a resiliência dos endpoints em uso no TRT9 e identificar potenciais ameaças em seus estágios iniciais, contribuindo para a melhora da segurança cibernética, de modo geral.

19. Justificativa da escolha da empresa promotora do curso/evento:

A empresa GoHacking possui destaque na área de treinamentos em segurança cibernética, contando com equipe de instrutores com ampla experiência no mercado. O currículo dos profissionais da empresa inclui atuação em grandes organizações, certificações na área e participação como palestrantes nos principais eventos dedicados ao tema.

Ademais, seus cursos já foram contratados por diversas instituições públicas, inclusive algumas vinculadas à Justiça do Trabalho.

Outro ponto levado em consideração foi a abordagem prática presente nos treinamentos da empresa, pois é um fator que pode auxiliar na fixação dos conceitos, além de permitir aos participantes a aplicação dos conhecimentos em ambiente controlado.

No que diz respeito ao curso GoHacking Ethical Hacking Endpoint Protection Evaion, pode-se dizer que não foram identificadas no mercado brasileiro outras capacitações com essa proposta, considerando o conteúdo voltado principalmente para a segurança defensiva e entregue em português no formato online e ao vivo.

20. Conteúdo programático resumido do curso/evento:
    - Arquitetura do Windows
      Windows API

Funcionamento de Antivírus
P/Invoke e D/Invoke
Shellcode Runners, Crypters & Encoders
Técnicas de Evasão de Antivírus
Processo de Injeção de Código
Process Hollowing
Backdooring
DLL Injection e Reflective DLL Injection
Funcionamento do Antimalware Scan Interface (AMSI)
Bypass de AMSI
Powershell Obfuscation
Bypass de Constrained Language Mode (CLM)
Criação de Comando e Controle (C2) furtivos
Bypass de Network Proxies & DNS filtering
Bypass de Applocker
Técnicas de bypass com JSCRIPT
Bypass de Protected Process Light (PPL)
Enumeração de LAPS e leitura de senha
Event Tracing for Windows (ETW) patching
Desabilitando Sysmon
Binary Signing & Attributes for Evasion
Criação de Macros com Visual Basic for Applications (VBA)
VBA Obfuscation and Stomping

ALEXANDRE TETSUO YAMAUCHI 13/05/2026 SIOP TRT9

EDUARDO SILVEIRA ROCHA 13/05/2026 SGTIC TRT9

21. Objetivos do curso/evento:
    - Permitir aos participantes conhecer as princípais técnicas e ferramentas voltadas para contonar as proteções aplicadas às estações de trabalho, bem como as medidas correspondentes para prevenção e detecção.
22. Competências técnicas ou comportamentais atendidas com a participação no curso/evento:
    - Compreensão das principais técnicas e vetores de ataque ao ambiente de estações de trabalho
    - Conhecimento dos mecanismos de detecção e defesa dos principais ataques ao ambiente de estações de trabalho
23. A empresa promotora aceita a contratação por meio de Nota de Empenho e Carta Contrato? Sim
24. Foi realizada a reserva de vaga para os indicados? Sim
25. Servidor indicado para Fiscal do Contrato: RAFAEL MENDES DE SOUZA
26. Servidor indicado para Fiscal Substituto do Contrato: OSCAR LUIS NAGEL
27. Critérios de sustentabilidade da contratação:

(X) Ambiental - Divulgação do treinamento realizado por meio digital

(X) Ambiental - Uso exclusivo de materiais digitais (apostila, certificado, etc)

(X) Ambiental - Evento online - sem deslocamento do instrutor / treinandos

( ) Social - Evento dispõe de acessibilidade às pessoas com deficiência

( ) Social - Evento utiliza linguagem simples

( ) Outro:

A referida contratação será realizada na hipótese de Inexigibilidade prevista na letra f, inciso III, art. 74 da Lei 14.133/2021;

Em atendimento ao § 4º, art. 23, Lei 14.133/2021, que trata sobre a comprovação prévia de que os preços estão de acordo com os praticados no mercado nas hipóteses de contratação direta e ao inciso VII, art. 72, Lei 14.133/2021, que trata sobre a justificativa de preço no processo de contratação direta, entendemos que por se tratar de curso aberto e disponível para pessoas físicas ou jurídicas públicas e privadas com valor preestabelecido, consoante o § 1º, art. 7º da IN SEGES/ME n. 65, de 7 de julho de 2021, está comprovada a regularidade no preço ajustado ao valor de mercado, sem quaisquer indícios de superfaturamento.

Diante do exposto, a SECRETARIA DE INFRAESTRUTURA E OPERAÇÕES SIOP sugere:

A. que a participação dos servidores interessados seja deferida;

B. que a SECRETARIA DE INFRAESTRUTURA E OPERAÇÕES SIOP seja a unidade gestora do contrato;

C. que o servidor RAFAEL MENDES DE SOUZA seja nomeado Fiscal do Contrato e o servidor OSCAR LUIS NAGEL seja nomeado Fiscal Substituto do Contrato

D. que os servidores interessados providenciem a confirmação da inscrição diretamente com a empresa promotora, após a emissão da Nota de Empenho;

E. que os fiscais do contrato reiterem a necessidade de a empresa enviar a nota fiscal, após o término da prestação dos serviços, via Portal SIGEO da Justiça do Trabalho, disponível pelo link https://portal.sigeo.jt.jus.br/portal-externo;

F. que os servidores interessados tenham ciência sobre a responsabilidade de eventual ressarcimento ao erário dos valores investidos, em caso de não participação e/ou conclusão do evento, conforme o art. 33 do Ato 305/2019;

G. que os servidores interessados respondam ao Formulário de “Avaliação e Reação” em até 5 dias após o término da capacitação;

H. que os servidores providenciem junto à Coordenadoria de Gestão do Quadro de Pessoal a análise da possibilidade de averbação da capacitação para fins de Adicional de Qualificação por ações de treinamento (AQ-AT);

I. que o valor do investimento, R$ 18.000,00, seja suportado pela verba destinada para Capacitação da Área de TIC.

Curitiba, data conforme assinatura eletrônica

ALEXANDRE TETSUO YAMAUCHI

SECRETARIA DE INFRAESTRUTURA E OPERAÇÕES SIOP

ALEXANDRE TETSUO YAMAUCHI 13/05/2026 SIOP TRT9

EDUARDO SILVEIRA ROCHA 13/05/2026 SGTIC TRT9

DESPACHO

Ciente e de acordo.

À Escola Judicial para prosseguimento.

Notifiquem-se:

- os interessados para ciência e providências;

Curitiba, data conforme assinatura eletrônica

EDUARDO SILVEIRA ROCHA
Secretário-Geral de Tecnologia da Informação e Comunicações

Área Temática: Tecnologia da informação e comunicação - TI