



PODER JUDICIÁRIO DO ESTADO DO PIAUÍ
COMISSÃO DE LICITAÇÃO Nº 02 - CPL2

Pça Des. Edgard Nogueira s/n - Bairro Cabral - Centro Cívico - CEP 64000-830
Teresina - PI - www.tjpi.jus.br

Contrato Nº 140/2021 - PJPI/TJPI/PRESIDENCIA/SECGER/SLC/CPL2

CONTRATO ADMINISTRATIVO

Processo SEI nº 21.0.000091636-3

Contratação Direta por Inexigibilidade

CONTRATO ADMINISTRATIVO FIRMADO ENTRE A ESCOLA JUDICIÁRIA DO PIAUÍ - EJUD E A EMPRESA REDE NACIONAL DE ENSINO E PESQUISA - RNP, PARA MINISTRAR CURSOS, NA ÁREA DE TIC, NA MODALIDADE EAD - ENSINO À DISTÂNCIA, PARA OS SERVIDORES DO TRIBUNAL DE JUSTIÇA ATUANTES NA STIC, NA FORMA ABAIXO:

A ESCOLA JUDICIÁRIA DO PIAUÍ - EJUD, com sede na Rua Professor Joca Vieira, nº 1449, Bairro Jóquei Club - Prédio da EJUD - CEP 64048-301, em Teresina, Estado do Piauí, inscrita no CNPJ nº 21.732.903/0001-37, neste ato representada pelo seu Diretor-Geral, Desembargador **SEBASTIÃO RIBEIRO MARTINS**, doravante designado simplesmente **CONTRATANTE**, no uso das atribuições que lhe são conferidas pelo Regimento Interno, daqui por diante denominado **CONTRATANTE**, e do outro lado a empresa **REDE NACIONAL DE ENSINO E PESQUISA- RNP**, inscrita no CNPJ nº 03.508.097/0001-36, representada neste ato pelo Senhor **LEANDRO MARCOS DE OLIVEIRA GUIMARÃES**, Diretor Adjunto da Escola Superior de Redes, portador do CPF nº 0012.992.507-18 e RG nº 08.944.551-4 Detran/RJ, situada na Rua Lauro Müller, nº 116, sala 1103, Botafogo, Rio de Janeiro- RJ, CEP: 22290-906, telefone/fax (61) 3243-4337/ (61) 98109-9955, *e-mail*: atendimento@esr.rnp.br, doravante denominada **CONTRATADA**, firmam este **CONTRATO**, resultante de procedimento de Contratação Direta por Inexigibilidade, com base no inciso II, Artigo 25 c/c Artigo 13, VI da Lei nº 8.666/93, vinculado ao Processo Administrativo SEI nº 21.0.000091636-3, e mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Tem por objeto a contratação da empresa **REDE NACIONAL DE ENSINO E PESQUISA - RNP**, pessoa jurídica inscrita no CNPJ nº 03.508.097/0001-36, para ministrar cursos, na área de TIC, na modalidade **EAD - Ensino a Distância**, para os servidores do Tribunal de Justiça atuantes na STIC.

1.2. Integram e complementam este instrumento, como se aqui estivessem transcritos integralmente, os documentos abaixo relacionados:

a) Termo de Referência Nº 116/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC (2708229); e

b) Proposta Pedagógica para curso (2761081).

1.3. Em função da natureza deste Contrato, poderão ser criados, durante sua vigência, outros anexos, para reunir documentos afins relativos a outros serviços, que sejam solicitados, bem como alterações promovidas nos anexos, os quais, devidamente assinados pelas Partes, igualmente passarão a integrá-lo nos termos descritos no item 1.2.

CLÁUSULA SEGUNDA – DO CONTEÚDO MÍNIMO DOS CURSOS

2.1. Segurança de Redes e Sistemas (EaD) - 40 h/a

2.1.1. Fundamentos de segurança

2.1.1.1. Da divisão de grupos;

2.1.1.2. Topologia geral de rede;

2.1.1.3. Configuração do Virtualbox;

2.1.1.4. Detalhamento das configurações de rede;

2.1.1.5. Configuração da máquinas virtuais;

2.1.1.6. Configuração de firewall e NAT;

2.1.1.7. Teste de conectividade das VMs;

2.1.1.8. Instalação do Virtualbox Guest Additions nas VMs Windows;

2.1.1.9. Instalação do Virtualbox Guest Additions nas VMs Linux;

2.1.1.10. Exercitando os fundamentos de segurança;

2.1.1.11. Normas e políticas de segurança.

2.1.2. Explorando vulnerabilidades em redes

2.1.2.1. Transferindo arquivos da máquina física para as VMs;

2.1.2.2. Sniffers para captura de dados;

2.1.2.3. Ataque SYN flood;

2.1.2.4. Ataque Smurf;

2.1.2.5. Levantamento de serviços usando o nmap;

2.1.2.6. Realizando um ataque com o Metasploit em ambiente Windows;

2.1.2.7. Realizando um ataque com o Metasploit em ambiente Linux;

2.1.2.8. Realizando um ataque de dicionário com o medusa;

2.1.3. Firewall

2.1.3.1. Trabalhando com chains no iptables;

2.1.3.2. Firewall stateful;

2.1.3.3. Configurando o firewall FWGW1-G: tabela filter;

2.1.3.4. Configurando o firewall FWGW1-G: tabela nat;

2.1.3.5. Revisão final da configuração do firewall FWGW1-G.

2.1.4. Serviços básicos de segurança

2.1.4.1. Configuração do servidor de log remoto;

2.1.4.2. Configuração do servidor de hora;

2.1.4.3. Monitoramento de serviços.

2.1.5. Sistema de detecção/prevenção de intrusos

- 2.1.5.1. Instalação do Snort;
- 2.1.5.2. Configuração inicial do Snort;
- 2.1.5.3. Configurando atualizações de regras de forma automática com o PuledPork;
- 2.1.5.4. Processando arquivos de log do Snort com o Barnyard2;
- 2.1.5.5. Visualizando eventos com o Snorby;
- 2.1.5.6. Integração dos serviços com o sistema;
- 2.1.5.7. Gerando alertas para o IDS;
- 2.1.5.8. Referências.
- 2.1.6. Autenticação, autorização e certificação digital**
- 2.1.6.1. Uso de criptografia simétrica em arquivos;
- 2.1.6.2. Uso de criptografia assimétrica em arquivos;
- 2.1.6.3. Uso de criptografia assimétrica em e-mails;
- 2.1.6.4. Criptografia de partições e volumes;
- 2.1.6.5. Autenticação usando sistema OTP.
- 2.1.7. Redes privadas virtuais e inspeção de tráfego**
- 2.1.7.1. Interceptação ofensiva de tráfego HTTPS com o mitmproxy;
- 2.1.7.2. Inspeção corporativa de tráfego HTTPS usando o Squid;
- 2.1.7.3. VPN SSL usando o OpenVPN.
- 2.1.8. Auditoria de segurança da informação**
- 2.1.8.1. Instalação do Nessus;
- 2.1.8.2. Realizando um scan em SO Linux;
- 2.1.8.3. Realizando um scan em SO Windows;
- 2.1.8.4. Efeitos do firewall em um scan;
- 2.1.8.5. Auditoria de servidores web.
- 2.1.9. Configuração segura de servidores Windows**
- 2.1.9.1. Uso do Microsoft Security Compliance Toolkit;
- 2.1.9.2. Configuração do controlador de domínio Active Directory;
- 2.1.9.3. Configuração do firewall para o Active Directory;
- 2.1.9.4. Adição de clientes ao Active Directory;
- 2.1.9.5. Adição de usuários ao Active Directory;
- 2.1.9.6. Distribuição de configurações via GPOs;
- 2.1.9.7. Instalação e configuração do WSUS;
- 2.1.9.8. Configuração de clientes no WSUS.
- 2.1.10. Configuração segura de servidores Linux**
- 2.1.10.1. Análise de rootkits;
- 2.1.10.2. Inserção de senha no bootloader;
- 2.1.10.3. Remoção de serviços desnecessários;
- 2.1.10.4. Controle granular de acesso a comandos;

- 2.1.10.5. Controle de uso do binário su;
- 2.1.10.6. Controle de acesso à console do sistema;
- 2.1.10.7. Exigência de parâmetros mínimos de senha;
- 2.1.10.8. Controle de logoff automático;
- 2.1.10.9. Desabilitando a combinação de teclas CTRL + ALT + DEL.

2.2. Tratamento de Incidentes de Segurança (EaD) - 40 h/a

- 2.2.1. Definições e fundamentos de CSIRTs;
- 2.2.2. Gerenciamento do CSIRT;
- 2.2.3. Riscos e ameaças;
- 2.2.4. Processo de tratamento de incidentes;
- 2.2.5. Aspectos operacionais da resposta a incidentes;
- 2.2.6. Identificação de contatos;
- 2.2.7. Análise de Logs;
- 2.2.8. Ferramentas para análise de incidentes;
- 2.2.9. Dinâmica de tratamento de incidentes.

2.3. Teste de Invasão de Aplicações Web (EaD) - 40 h/a

- 2.3.1. Arquitetura e tecnologias de aplicações web;
- 2.3.2. Criptografia: cifras simétricas, cifras assimétricas, funções de hash criptográficas, MACs, assinaturas digitais, certificados digitais e SSL/TLS;
- 2.3.3. Tipos de pentest e metodologia para teste de invasão;
- 2.3.4. Injeção de SQL com acesso à plataforma subjacente, especificidades dos SGBDs e injeção de SQL às cegas;
- 2.3.5. Injeção em LDAP, XML, SMTP e injeção de comandos;
- 2.3.6. Transporte de credenciais por canais inseguros;
- 2.3.7. Enumeração de usuários;
- 2.3.8. Política de senhas fortes não implementadas pela aplicação;
- 2.3.9. Falhas na programação ou projeto do mecanismo de autenticação;
- 2.3.10. Mecanismos de recuperação de senhas vulneráveis;
- 2.3.11. Condições de corrida no mecanismo de autenticação;
- 2.3.12. Testes sobre o gerenciamento de sessões;
- 2.3.13. Cross-Site Scripting (XSS) e CSRF;
- 2.3.14. Teste dos mecanismos de autorização;
- 2.3.15. Testes dos mecanismos criptográficos;
- 2.3.16. Teste completo e relatórios.
- 2.3.17. Fundamentos e as metodologias de uma análise de risco;
- 2.3.18. Tópicos principais para a construção de uma política de segurança;
- 2.3.19. A navegação na Internet e as ameaças atuais;
- 2.3.20. Navegação segura na Internet;
- 2.3.21. Programas de segurança de um computador pessoal.

2.4. Hardening em Linux (EaD) - 40 h/a

2.4.1. Sessão 1: Instalação e configurações iniciais

2.4.1.1. Criação de máquina virtual no Virtualbox;

2.4.1.2. Configuração do LVM;

2.4.1.3. Clonando máquinas virtuais;

2.4.1.4. Operações avançadas com LVM;

2.4.1.5. Criptografia de partições.

2.4.2. Sessão 2: Firewall e DNS

2.4.2.1. Criação da VM de firewall e DNS primário;

2.4.2.2. Configuração do servidor DNS primário e Secundário;

2.4.2.3. Configuração do DNSSEC.

2.4.3. Sessão 3: Autenticação centralizada

2.4.3.1. Configuração do servidor LDAP;

2.4.3.2. Configurando uma autoridade certificadora (CA) para o SSH integrada ao LDAP;

2.4.3.3. Restringindo login por grupos e usuários;

2.4.3.4. Bloqueando tentativas de brute force contra o SSH.

2.4.4. Sessão 4: Controles de segurança

2.4.4.1. Requisitos de senha na base LDAP;

2.4.4.2. Configuração do servidor de arquivos NFS e quotas de disco;

2.4.4.3. Uso de ACLs localmente e via NFS

2.4.5. Sessão 5: Gestão de configuração

2.4.5.1. Instalação e configuração inicial do Ansible;

2.4.5.2. Uso de roles no Ansible;

2.4.5.3. Versionamento de configuração com git.

2.4.6. Sessão 6: Registro e correlacionamento de eventos

2.4.6.1. Criação da VM de gestão de logs;

2.4.6.2. Configuração do NTP;

2.4.6.3. Registro de comandos digitados com SnoopyLog;

2.4.6.4. Instalação e configuração inicial do Graylog.

2.4.7. Sessão 7: Hardening de sistemas web

2.4.7.1. Configuração do servidor de banco de dados;

2.4.7.2. Configuração do servidor web www1 e ww2 com balanceador de carga.

2.4.8. Sessão 8: Isolamento de processos e containerização

2.4.8.1. Criação da VM docker1 e VM docker2;

2.4.8.2. Trabalhando com containers e registry externo;

2.4.8.3. Construindo serviços com o Docker;

2.4.8.4. Operando com múltiplos membros no cluster;

2.4.8.5. Adicionando novos serviços ao cluster;

2.4.8.6. Configurando a persistência dos dados.

2.4.9. Sessão 9: Criação de sistemas Linux customizados

2.4.9.1. Criação da VM de build com uma distribuição mínima;

2.4.9.2. Utilizando um repositório local de pacotes.

2.4.10. Sessão 10: Módulos de segurança do kernel, auditoria e detecção de intrusão

2.4.10.1. Instalação do AppArmor;

2.4.10.2. Auditoria automatizada de sistemas usando o OpenSCAP;

2.4.10.3. Detecção de intrusão local utilizando o OSSEC.

2.5. PenTest + EaD (parceria oficial CompTIA) - 40 h/a

2.5.1. Planejamento e Escopo dos Testes de Penetração;

2.5.2. Conduzindo Reconhecimento Passivo;

2.5.3. Realizando Testes Não-Técnicos;

2.5.4. Conduzindo Reconhecimento Ativo;

2.5.5. Analisando Vulnerabilidades;

2.5.6. Penetrando Redes;

2.5.7. Exploitando Vulnerabilidades Baseadas no Host;

2.5.8. Testando Aplicações;

2.5.9. Completando as Tarefas Pós-Exploit;

2.5.10. Analisando e Reportando os Resultados do Pen Test.

2.6. CySA + EaD (parceria oficial CompTIA) - 40 h/a

2.6.1. Explicando a importância dos controles de segurança e da segurança;

2.6.2. Utilizando inteligência e dados de ameaças;

2.6.3. Analisando o monitoramento de segurança;

2.6.4. Coleta e consulta de dados de monitoramento de segurança;

2.6.5. Utilizando forense Digital e técnicas de análise de indicadores;

2.6.6. Aplicando procedimentos de resposta a incidentes;

2.6.7. Aplicando mitigação de risco e estruturas de segurança;

2.6.8. Executando o gerenciamento de vulnerabilidades;

2.6.9. Aplicação de soluções de segurança para gerenciamento de infraestrutura;

2.6.10. Noções básicas sobre privacidade e proteção de dados;

2.6.11. Aplicando Soluções de Segurança para Software Assurance;

2.6.12. Aplicando soluções de segurança para nuvem e automação.

2.7. Security + EaD (parceria Oficial CompTIA) - 40 h/a

2.7.1. Comparando funções de segurança e controles de segurança;

2.7.2. Explicando os atores de ameaças e a inteligência sobre ameaças;

2.7.3. Realizando Avaliações de Segurança;

2.7.4. Identificando Engenharia Social e Malware;

2.7.5. Resumindo os conceitos básicos de criptografia;

- 2.7.6. Implementando infraestrutura de chave pública;
- 2.7.7. Implementando controles de autenticação;
- 2.7.8. Implementando controles de gerenciamento de identidade e conta;
- 2.7.9. Implementando uma rede segura;
- 2.7.10. Implementando dispositivos de segurança de rede;
- 2.7.11. Implementando protocolos de rede seguros;
- 2.7.12. Implementando Soluções de Segurança de Host;
- 2.7.13. Implementando Soluções Móveis Seguras;
- 2.7.14. Resumindo os conceitos de aplicativos seguros;
- 2.7.15. Implementando soluções de nuvem seguras;
- 2.7.16. Explicando os conceitos de privacidade e proteção de dados;
- 2.7.17. Executando a Resposta ao Incidente;
- 2.7.18. Explicando a perícia digital;
- 2.7.19. Resumindo os conceitos de gerenciamento de risco;
- 2.7.20. Implementando Resiliência da Cibersegurança;
- 2.7.21. Explicando a segurança física.

2.8. CASP + (CAS-003) EaD (parceria Oficial CompTIA) - 40 h/a

- 2.8.1. Apoio à governança de TI e gerenciamento de riscos;
- 2.8.2. Aproveitando a colaboração para apoiar a segurança;
- 2.8.3. Usando pesquisa e análise para proteger a empresa;
- 2.8.4. Integrando Técnicas Avançadas de Autenticação e Autorização;
- 2.8.5. Implementação de técnicas criptográficas;
- 2.8.6. Implementando controles de segurança para hosts;
- 2.8.7. Implementando controles de segurança para dispositivos móveis;
- 2.8.8. Implementando Segurança de Rede;
- 2.8.9. Implementando Segurança no Ciclo de Vida de Desenvolvimento de Sistemas e Software;
- 2.8.10. Integrando ativos em uma arquitetura corporativa segura;
- 2.8.11. Conduzindo avaliações de segurança;
- 2.8.12. Resposta e recuperação de incidentes.

2.9. Cibersegurança EaD (parceria oficial Ascend) - 40 h/a

- 2.9.1. Threat and Vulnerability Management;
- 2.9.2. Intelligence Sources;
- 2.9.3. Indicator Management;
- 2.9.4. Threats; Attack Frameworks;
- 2.9.5. The Cyber Kill Chain;
- 2.9.6. Threat Research;
- 2.9.7. Threat Modeling;
- 2.9.8. Vulnerability Identification;

- 2.9.9.** Remediation and Mitigation;
- 2.9.10.** Web App Scanners;
- 2.9.11.** Assessment Tools and Techniques;
- 2.9.12.** Attack Type;
- 2.9.13.** Vulnerabilities;
- 2.9.14.** Threats and Vulnerabilities Associated with Specialized Technology;
- 2.9.15.** More Specialized Technologies;
- 2.9.16.** Cloud Service Security;
- 2.9.17.** Cloud Service Weaknesses;
- 2.9.18.** Software and Systems Security;
- 2.9.19.** Asset Management;
- 2.9.20.** Object Tracking and Containment;
- 2.9.21.** Object Tracking and Containment Continued;
- 2.9.22.** Identity and Access Management;
- 2.9.23.** Honeypot;
- 2.9.24.** Cryptography;
- 2.9.25.** Encryption and Active Defense;
- 2.9.26.** Software Security Platforms;
- 2.9.27.** Formal Methods;
- 2.9.28.** Service Oriented Architecture;
- 2.9.29.** Hardware Root of Trust;
- 2.9.30.** Trusted Foundry and Processors;
- 2.9.31.** Trusted Technology;
- 2.9.32.** Security Operations and Monitoring;
- 2.9.33.** Analyses and Trends;
- 2.9.34.** Endpoints;
- 2.9.35.** Memory;
- 2.9.36.** Network;
- 2.9.37.** Logs;
- 2.9.38.** Firewall Logs;
- 2.9.39.** Intrusion;
- 2.9.40.** Impact Analysis and SIEM;
- 2.9.41.** Email Security;
- 2.9.42.** Security Tools I;
- 2.9.43.** Security Tools II;
- 2.9.44.** Security Tools III;
- 2.9.45.** Threat Hunting;
- 2.9.46.** Automation Concepts;

- 2.9.47. Automation Protocols;
- 2.9.48. Incident Response;
- 2.9.49. Incident Response Process;
- 2.9.50. Response Coordination;
- 2.9.51. Data Criticality Factors;
- 2.9.52. Incident Response- Preparation;
- 2.9.53. Incident Response- Detection and Analysis;
- 2.9.54. Incident Response- Containment;
- 2.9.55. Incident Response- Post-Incident Activities;
- 2.9.56. Host-Related Indicators of Compromise;
- 2.9.57. Network-Related Indicators of Compromise;
- 2.9.58. Application-Related Indicators of Compromis;
- 2.9.59. Data Exfiltration;
- 2.9.60. Basic Digital Forensic Techniques;
- 2.9.61. Forensic Tools Continued;
- 2.9.62. Forensic Procedures;
- 2.9.63. Compliance and Assessment;
- 2.9.64. Data Privacy and Protection;
- 2.9.65. Data Ownership and Retention;
- 2.9.66. Data Controls Preface;
- 2.9.67. Data Controls and Identification;
- 2.9.68. Risk Analysis and Calculation;
- 2.9.69. Risk Prioritization;
- 2.9.70. Training and Exercises;
- 2.9.71. Frameworks;
- 2.9.72. Policies and Procedures;
- 2.9.73. Data;
- 2.9.74. Audits and Assessments.

2.10. Planejamento de Contratações de TI no Judiciário (EaD) - 40 h/a

- 2.10.1. Sistemas Orçamentários da União
- 2.10.2. Sistemas Orçamentários do Judiciário
- 2.10.3. Planejamento Estratégico do Judiciário
- 2.10.4. Planejamento Estratégico de Tecnologia da Informação e Comunicação – PETIC
- 2.10.5. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC
- 2.10.6. A Resoluções do CNJ
- 2.10.7. A Resolução 182/2013
- 2.10.8. Acórdãos 1603/2008, 145/2011, 54/2012 e 1233/2012
- 2.10.9. Outros modelos de Contratação de TIC

- 2.10.10. Origem
- 2.10.11. Modelo SISP
- 2.10.12. Modelo CFJ
- 2.10.13. Compreensão da resolução 182
- 2.10.14. Discussão da Resolução
- 2.10.15. Esquema de processo Glossário
- 2.10.16. Impedimentos de contratações
- 2.10.17. Atribuições dos atores envolvidos
- 2.10.18. Plano de Contratações
- 2.10.19. Fases de Elaboração
- 2.10.20. Estudos Preliminares
- 2.10.21. Elaboração do DOD
- 2.10.22. Análise de Viabilidade da Contratação
- 2.10.23. Sustentação do Contrato Estratégia da Contratação
- 2.10.24. Análise de Riscos
- 2.10.25. Conceituação de Riscos
- 2.10.26. Riscos do Planejamento da Contratação
- 2.10.27. Riscos da Contratação Riscos da Execução Contratual
- 2.10.28. Projeto Básico ou Termos de Referência
- 2.10.29. Checklist de TR
- 2.10.30. Auditoria
- 2.10.31. Ordens de Serviços
- 2.10.32. Elaboração de OS
- 2.10.33. Termos de Recebimento
- 2.10.34. Elaboração de TR provisório
- 2.10.35. Elaboração de TR definitivo
- 2.10.36. Gestão da Execução do Contrato
- 2.10.37. Recomendações e formulários
- 2.11. Correlacionamento de eventos com Graylog - 40 h/a**
- 2.11.1. Introdução à gestão de logs
- 2.11.2. Arquitetura e instalação do Graylog
- 2.11.3. Usuários, papéis e integração com sistemas externos
- 2.11.4. Coleta e ingestão de logs
- 2.11.5. Expressões regulares, padrões GROK e filtros
- 2.11.6. Pipelines de processamento e lookup tables
- 2.11.7. Plugins, Content Packs e geolocalização de informações
- 2.11.8. Pesquisando registros
- 2.11.9. Configuração de alertas e dashboards

2.11.10. Procedimentos de manutenção, backup e atualização

2.12. Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD) - 40 h/a

2.12.1. Principais diferenças da IN 04/2014 e a IN 01/2019;

2.12.2. Ministério da Economia- Nova organização;

2.12.3. Secretaria de Governo Digital;

2.12.4. SISP;

2.12.5. Plano Anual de Contratações Corporativas- PAC;

2.12.6. Programação Estratégica de Contratações;

2.12.7. Contratações;

2.12.8. PDTI;

2.12.9. Restrições de contratações;

2.12.10. Vedações;

2.12.12. Critérios;

2.12.13. Planejamento da Contratação;

2.12.14. Seleção de Fornecedores;

2.12.15. Gestão do Contrato;

2.12.16. Gestão de Riscos;

2.12.17. Diretrizes Específicas;

2.12.18. Base legal e legislação vigente.

2.13. Planejamento e Gestão Estratégica de TI (EaD) - 24 h/a

2.13.1. Relações entre a gestão, as estratégias de negócio e as estratégias de TI;

2.13.2. Mudança organizacional e diagnóstico de maturidade do planejamento;

2.13.3. Conceitos relacionados à ferramenta Balanced ScoreCard (BSC);

2.13.4. Habilidades e conhecimentos específicos de profissionais da área de TI na organização para a realização de metas estratégicas da área de TI;

2.13.5. Alinhamento da área de TI com as metas estratégicas de longo prazo das organizações e seu controle através da criação de indicadores;

2.13.6. Análise da relação entre PEE, PETI, PDTI.

2.14. Fundamentos do COBIT 2019 (EaD) - 24 h/a

2.14.1. Estrutura do COBIT;

2.14.2. Objetivos de controle;

2.14.3. Práticas de controle;

2.14.4. Diretrizes de gerenciamento;

2.14.5. Diretrizes de auditoria;

2.14.6. Visão sistêmica das áreas e processos do COBIT;

2.14.7. Componentes do framework do COBIT

2.15. Gerenciamento Ágil de Projetos de TI (EaD) - 24 h/a

2.15.1. Gerenciamento de Projetos de TI com base nas boas práticas do PMBOK, Manifesto Ágil e Guia do Scrum e em outros guias de referência;

2.15.2. Definição de Projeto;

2.15.3. As áreas de conhecimento do Gerenciamento de Projetos;

2.15.4. Processos de Gerenciamento de Projetos;

2.15.5. Fases e ciclo de vida do Gerenciamento de Projetos;

2.15.6. Técnicas Ágeis;

2.15.7. Melhoria de processos organizacionais em TI.

2.16. Elaboração de PDTI (EaD) - 24 h/a

2.16.1. Plano Diretor de Tecnologia da Informação;

2.16.2. Fase de Preparação;

2.16.3. Fase de Diagnóstico: Conhecendo a Realidade da TI;

2.16.4. Fase de Diagnóstico: Avaliando os Recusos de TI;

2.16.5. Fase de Planejamento: Definindo Metas e Ações;

2.16.6. Fase de Planejamento: Terminando o PDTI.

2.17. Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) - 24 h/a

2.17.1. Introdução ao Gerenciamento de Serviços e ao ITIL;

2.17.2. Gerenciamento de Serviços no mundo moderno;

2.17.3. Sobre o ITIL 4; A estrutura e os benefícios do ITIL 4;

2.17.4. O Programa de certificação ITIL;

2.17.5. Conceitos chaves para o Gerenciamento de Serviços;

2.17.6. Valor e co-criação de valor;

2.17.7. Organização, Provedores de Serviço e Consumo de Serviço;

2.17.9. Produtos e Serviços; Relacionamento de Serviços;

2.17.10. Valor: Entradas, custos e riscos;

2.17.11. As quatro Dimensões do Gerenciamento de Serviços;

2.17.12. Organizações e Pessoas;

2.17.13. Informação e Tecnologia;

2.17.14. Parceiros e Fornecedores;

2.17.15. Fluxos de valor e Processos;

2.17.16. Fatores externos;

2.17.17. O Sistema de Valor do ITIL;

2.17.18. Overview no sistema de valor;

2.17.19. Governança;

2.17.20. Cadeia de valor de serviço;

2.17.21. Melhoria contínua; Práticas;

2.17.22. Práticas de Gestão do ITIL;

2.17.23. Práticas gerais de Gestão;

2.17.24. Práticas de gerenciamento de serviços;

2.17.25. Práticas de gerenciamento técnico.

2.18. Sistema de Gestão da Integridade – Compliance & Antissuborn - 24 h/a

2.18.1. Programa do curso Gênesis;

2.18.2. O que é corrupção? Uma breve história da corrupção;

2.18.3. O contexto organizacional;

2.18.4. O que é uma organização? O contexto interno da organização. O contexto externo da organização;

2.18.5. As partes interessadas, quem são e o que querem?;

2.18.6. Conflito de interesse e Conflito de agenda;

2.18.7. Gerenciamento de riscos;

2.18.8. O que é risco? Identificação de riscos. Análise Qualitativa dos riscos;

2.18.9. Análise Quantitativa dos riscos. Tratamento dos riscos;

2.18.10. O papel da liderança;

2.18.11. O que é a política de gestão?;

2.18.12. Escopo do sistema de gestão;

2.18.13. Atribuições e responsabilidades;

2.18.14. Objetivos do Sistema de gestão;

2.18.15. O que é uma métrica?;

2.18.16. Indicadores – BSC, KPI e KRO;

2.18.17. Desempenho do sistema de gestão;

2.18.18. Planejamento dos processos;

2.18.19. O que é um processo? Mapeamento de um processo. Medição do processo;

2.18.20. Conscientização;

2.18.21. O que é competência?;

2.18.22. A importância da comunicação;

2.18.23. Treinamento, formas de realização;

2.18.24. Parceiro de negócio;

2.18.25. O que é um parceiro de negócio?;

2.18.26. Cadeia de suprimento;

2.18.27. Critérios para escolha e manutenção de seu parceiro;

2.18.28. Monitoramento e controle;

2.18.29. O que é um canal de preocupação?;

2.18.30. Due diligence – escopo, profundidade e limitação;

2.18.31. Auditorias de primeira parte, segunda parte e terceira parte;

2.18.32. Gestão da informação documentada; Em busca da excelência;

2.18.33. O que é benchmarking?;

2.18.34. Ação corretiva;

- 2.18.35.** Melhoria contínua;
- 2.18.36.** Normas e Certificação;
- 2.18.37.** O que certificação?;
- 2.18.38.** ISO 19600;
- 2.18.39.** ISO 37001;
- 2.18.40.** Compliance e Antissuborno;
- 2.18.41.** Como implantar um sistema de gestão;
- 2.18.42.** O que é um sistema de gestão?;
- 2.18.43.** O método PDCA;
- 2.18.44.** Um mapa para sua jornada.

CLÁUSULA TERCEIRA – DA METODOLOGIA E CARGA HORÁRIA

3.1. A capacitação terá caráter teórico-prático com material de apoio, exercícios e/ou dinâmicas, bem como análise de casos, considerando o contexto de atuação dos servidores em suas respectivas lotações.

3.2. A metodologia será baseada em vivências, simulações e exercícios práticos, a fim de possibilitar ao cursista aplicar os conceitos desenvolvidos.

3.3. O material de apoio de todos os treinamentos serão disponibilizados em ambiente virtual, e inclui: conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeos.

3.4. Duração dos cursos

3.4.1. Os cursos Segurança de Redes e Sistemas (EaD), Tratamento de Incidentes de Segurança (EaD), Teste de Invasão de Aplicações Web (EaD), Hardening em Linux (EaD), PenTest + EaD (parceria oficial CompTIA), CySA+ EaD (parceria oficial CompTIA), Security+ EaD (parceria Oficial CompTIA), CASP+ (CAS-003) EaD (parceria Oficial CompTIA, Cibersegurança EaD (parceria oficial Ascend), Planejamento de Contratações de TI no Judiciário (EaD), Correlacionamento de eventos com Graylog e Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD), são divididos em 10 sessões de aprendizagem, totalizando 40 horas e os cursos Planejamento e Gestão Estratégica de TI (EaD), Fundamentos do COBIT 2019 (EaD), Gerenciamento Ágil de Projetos de TI (EaD), Elaboração de PDTI (EaD), Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) e Sistema de Gestão da Integridade – Compliance & Antissuborn (ED, são dividido em 6 sessões de aprendizagem, totalizando 24 horas.

3.4.2. Os cursos serão ministrados na modalidade EAD, para os servidores da STIC do Tribunal de Justiça do Piauí, com temas, quantidades de vagas, e carga horária de acordo com tabela a seguir:

ITEM	TEMA	DURAÇÃO	VAGAS
2.1.	Segurança de Redes e Sistemas (EaD)	40 h/a	4
2.2.	Tratamento de Incidentes de Segurança (EaD)	40 h/a	4
2.3.	Teste de Invasão de Aplicações Web (EaD)	40 h/a	4
2.4.	Hardening em Linux (EaD)	40 h/a	4
2.5.	PenTest + EaD (parceria oficial CompTIA)	40 h/a	5
2.6.	CySA + EaD (parceria oficial CompTIA)	40 h/a	4
2.7.	Security + EaD (parceria Oficial CompTIA)	40 h/a	4
2.8.	CASP + (CAS-003) EaD (parceria Oficial CompTIA)	40 h/a	4

ITEM	TEMA	DURAÇÃO	VAGAS
2.9.	Cibersegurança EaD (parceria oficial Ascend)	40 h/a	5
2.10.	Planejamento de Contratações de TI no Judiciário (EaD)	40 h/a	6
2.11.	Correlacionamento de eventos com Graylog	40 h/a	4
2.12.	Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD)	40 h/a	6
2.13.	Planejamento e Gestão Estratégica de TI (EaD)	24 h/a	8
2.15.	Gerenciamento Ágil de Projetos de TI (EaD)	24 h/a	19
2.16.	Elaboração de PDTI (EaD)	24 h/a	8
2.17.	Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD)	24 h/a	10
2.18.	Sistema de Gestão da Integridade – Compliance & Antissuborn	24 h/a	6
	TOTAL		113

3.4.3. A carga horária dos cursos serão distribuídas em 50% de aulas EaD síncrona e 50% de auto estudo, conforme ementas.

CLÁUSULA QUARTA – DO VALOR

4.1. O CONTRATANTE pagará pelo pela prestação dos serviços objeto do presente contrato o valor total de **R\$ 171.470,00 (cento e setenta e um mil quatrocentos e setenta reais)** referente ao 2º grau de jurisdição.

4.2. O valor acima mencionado inclui todas as despesas incidentes sobre a prestação do serviço contratado, tais como as definidas em leis sociais, trabalhistas, comerciais, tributárias e previdenciárias, impostos e todos os custos, insumos e demais obrigações legais, inclusive todas as despesas que onerem, direta ou indiretamente, não cabendo, pois, quaisquer reivindicações da CONTRATADA, a título de revisão de preço ou reembolso.

CLÁUSULA QUINTA – LOCAL E PERÍODO DE EXECUÇÃO

5.1. A capacitação será desenvolvida na modalidade EAD com apoio da Escola Judiciária do Tribunal de Justiça do Piauí, com datas e horários a serem definidos pela EJUD/TJPI, juntamente com a STIC e a empresa.

CLÁUSULA SEXTA – DO RESPONSÁVEL PELO ACOMPANHAMENTO DA EXECUÇÃO

6.1. O responsável pelo acompanhamento da execução do curso, objeto deste instrumento, será o servidor Levi de Sousa Soares Ciríaco, Analista Judiciário / Área Especializada - Analista de Sistemas/Desenvolvimento, Matrícula N° 3654, lotado na Secretaria de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Piauí.

CLÁUSULA SÉTIMA – DA VIGÊNCIA

7.1. O prazo de vigência do Contrato ora ajustado é de 12 (doze) meses, a contar da data da publicação do extrato deste instrumento no Diário da Justiça do TJ/PI.

CLÁUSULA OITAVA – DOS RECURSOS ORÇAMENTÁRIOS E FINANCEIROS

8.1. Os recursos para atender as despesas decorrentes deste Contrato serão oriundos da EJUD, conforme tabela a seguir:

Unidade Orçamentária: FONTE:	040106 - EJUD 118- Recursos de Fundos Especiais
Ação Orçamentária: Classificação Funcional Programática: Natureza da Despesa: Valor Reservado:	2871 - TREINAMENTO E CAPACITAÇÃO - 2º GRAU 02.061.0015.2871 339040 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica R\$ 171.470,00 (2021NR00149)

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

Além das obrigações resultantes da observância da Lei nº 8.666/93, a CONTRATADA deverá:

- 9.1. Executar o serviço conforme especificações e demais condições contidas no Termo de Referência e na proposta apresentada;
- 9.2. Manter, durante a execução do contrato, todas as condições da habilitação e da proposta;
- 9.3. Responder por todas as despesas de natureza tributária, trabalhista e previdenciária que incidam ou venham a incidir sobre a prestação dos serviços bem como as despesas com passagens aéreas, deslocamentos, hospedagem e alimentação do instrutor;
- 9.4. Fornecer os materiais didáticos, de apoio e certificado de conclusão do curso para os participantes que obtiverem presença mínima de 75% (setenta e cinco por cento);
- 9.5. Corrigir, às suas expensas, quaisquer falhas ou irregularidades detectadas ou notificadas pela Administração;
- 9.6. Fornecer certificado de conclusão do curso para os participantes que obtiverem presença mínima de 75% (setenta e cinco por cento), que deverão conter, além de outros dados, a “logo” da EJUD/TJPI, espaço para assinatura, com nome do Diretor Geral da EJUD/TJ-PI, Desembargador FERNANDO LOPES E SILVA NETO, bem como conteúdo programático;
- 9.7. Solicitar o pagamento relativo à prestação do serviço, por meio de Requerimento dirigido ao Diretor Geral da EJUD/TJPI, por intermédio do endereço eletrônico da Ejud: ejud@tjpi.jus.br; oportunidade em que também deverá apresentar RECIBO do respectivo pagamento;
- 9.8. Apresentar Nota Fiscal relativa ao serviço prestado, indicando como tomadora do serviço a Escola Judiciária do Tribunal de Justiça do Estado do Piauí, “Des. Lucrécio Dantas Avelino”.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE

Além das obrigações resultantes da observância da Lei 8.666/93, o CONTRATANTE deverá:

- 10.1. Fornecer à Contratada todas as informações, esclarecimentos, documentos e demais condições necessárias à execução da capacitação conforme as especificações estabelecidas no Termo de Referência;
- 10.2. Providenciar os equipamentos solicitados;
- 10.3. Acompanhar a frequência dos cursistas e encaminhar para a empresa contratada, via e-mail, para fins de confecção de Certificados;
- 10.4. Acompanhar e fiscalizar a execução dos serviços, bem como atestar na nota fiscal a sua efetiva prestação;
- 10.5. Recusar, com a devida justificativa, qualquer serviço prestado fora das especificações constantes no Termo de Referência;
- 10.6. Efetuar o pagamento correspondente à Nota de Empenho e respectiva Nota Fiscal;

10.7. Notificar a Contratada, por escrito, sobre quaisquer irregularidades constatadas, solicitando a sua regularização.

CLÁUSULA DÉCIMA PRIMEIRA – DO PAGAMENTO

11.1. A liquidação da despesa e respectivo pagamento observarão as disposições IN TCE/PI nº 02/2017 c/c o disposto na Lei Nº 8.666/93.

11.2. O pagamento será realizado por curso concluído, após atesto do Responsável pelo Acompanhamento da Execução, indicado no item 9.

11.3. O pagamento será efetuado por meio de Ordem Bancária para crédito na Conta Corrente indicada na proposta da Contratada;

11.4. A Nota Fiscal deverá ser emitida pela Contratada, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e da proposta, não se admitindo Notas Fiscais emitidas com outros CNPJ, mesmo aquelas de filiais ou da matriz. As Notas Fiscais deverão conter discriminação idêntica à contida na respectiva Nota de Empenho;

11.5. A empresa optante pelo Simples Nacional deverá apresentar declaração em conformidade com o art. 6º da Instrução Normativa SRF nº 1.234/2012;

11.6. No caso de não ser apresentada a declaração, serão retidos os tributos e contribuições no pagamento a ser efetuado;

11.7. Se a Nota Fiscal for apresentada em desacordo com este contrato ou com irregularidades, o prazo para pagamento ficará suspenso até que a Contratada providencie as medidas saneadoras necessárias à sua regularização formal, não implicando quaisquer ônus para esta Escola Judiciária;

11.8. Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência;

11.9. Na hipótese de eventual atraso de pagamento, por causa atribuída exclusivamente à Administração, incidirão correção monetária e juros moratórios. Fica convencionado que a correção monetária e os encargos moratórios devidos pelo CONTRATANTE entre a data de seu vencimento e a do efetivo pagamento da nota fiscal/fatura será calculada por meio da aplicação da seguinte fórmula:

$EM = N \times VP \times I$, sendo:

EM= Encargos moratórios;

N= Número de dias entre a data prevista para o pagamento e a do efetivo pagamento:

VP = valor da parcela em atraso

I = índice de compensação financeira = 0,00016438, assim apurado:

$I = i/365$ $I = 0,06/365$ $I = 0,00016438$ e,

I = taxa percentual no valor de 6%.

11.10. Não haverá, sob hipótese alguma, pagamento antecipado;

11.11. Não haverá reajuste considerando-se que o prazo de vigência da contratação não ultrapassa 01 (um) ano.

CLÁUSULA DÉCIMA SEGUNDA – DAS ALTERAÇÕES

12.1. Este Contrato poderá ser alterado na ocorrência de quaisquer dos fatos estipulados no artigo 65 da Lei 8.666/93.

CLÁUSULA DÉCIMA TERCEIRA – DAS SANÇÕES

13.1. As sanções por descumprimento são aquelas constantes da Lei 8.666/1993 e suas alterações posteriores.

CLÁUSULA DÉCIMA QUARTA – DA INEXECUÇÃO E RESCISÃO CONTRATUAL

As hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei 8666/93.

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão submetidos ao parecer da Secretaria de Assuntos Jurídicos, e resolvidos de conformidade com o preceituado na Lei nº 8.666/93, suas alterações posteriores e demais legislações aplicáveis, depois de submetidos à anuência da maior autoridade administrativa do TJ/PI.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICIDADE

16.1. O extrato deste Contrato será publicado no Diário de Justiça, conforme dispõe o artigo 61, parágrafo único, da Lei n.º 8.666/1993.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES FINAIS

17.1. As partes elegem o foro da Comarca de Teresina, Capital do Estado do Piauí, para dirimir as dúvidas oriundas deste Contrato, excluído qualquer outro, por mais privilegiado que seja.

E por estarem as partes, justas e acordadas, firmam o presente instrumento, assinando-o eletronicamente, conforme art. 1º, III, "b", da Lei 11.419/2006 e Resolução 22/2016/TJPI, para que produza seus efeitos jurídicos legais.

Teresina (PI), 29 de novembro de 2021.

Desembargador **SEBASTIÃO RIBEIRO MARTINS**
Diretor-Geral da Escola Judiciária do Tribunal de Justiça do Piauí

CONTRATANTE

LEANDRO MARCOS DE OLIVEIRA GUIMARÃES

Representante Legal

CONTRATADA

Documento assinado eletronicamente por **Sebastião Ribeiro Martins, Diretor Geral da EJUD,**



em 26/11/2021, às 16:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Leandro Marcos de Oliveira Guimarães, Usuário Externo**, em 29/11/2021, às 16:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <http://sei.tjpi.jus.br/verificar.php> informando o código verificador **2879925** e o código CRC **0500BB8D**.
