Processo: Processo de Contratação - Solução de TI - Teste de Penetração (Pentest) (Proc. N° 274552)

Estudo Técnico Preliminar de TI - Análise de Viabilidade (ID 7457892)

Especificação dos Requisitos da Demanda (ID 7457893)

Requisitos de Negócio - Integrante Demandante:

1) Garantir a adequação, modernização e segurança da infraestrutura, sistemas, ativos e serviços de TIC.

2) Assegurar o controle, a conformidade, a rastreabilidade e eficiência sobre os ativos de Tecnologia da Informação e Comunicação - Política Nº 5 de 2017 - Gestão de Ativos de Tecnologia da Informação.

3) Realizar varreduras em busca de vulnerabilidades - Portaria CNJ 162/2021 - ANEXO IV - Proteção de Infraestruturas Críticas de TIC - Controles de Gerenciamento Contínuo de Vulnerabilidades.

Requisitos de Capacitação - Integrante Demandante e Técnico:

A contratação do serviço não envolverá treinamento ou capacitação para membros do CONTRATANTE.

Requisitos Legais - Integrante Demandante:

1) Lei de Licitações e Contratos Administrativos - Lei nº 14.133/2021.

2) Resolução CNJ 182/2013 que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação.

Requisitos de Manutenção - Integrante Demandante:

1) A CONTRATADA deverá prestar suporte ao CONTRATANTE durante o período de vigência do contrato, através de telefone e correio eletrônico.

2) Durante a vigência contratual, a CONTRATADA deverá atender número ilimitado de incidentes de suporte, desde que relacionados aos serviços a serem executados.

3) O suporte técnico deverá ocorrer, pelo menos, em regime “8x5" (8 horas por dia, 5 dias por semana).

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Requisitos Temporais - Integrante Demandante:

1) A CONTRATADA deverá participar de reunião com equipe técnica da CONTRATANTE, a ser realizada em até 5 (cinco) dias úteis da assinatura do contrato.

2) O CONTRATANTE deverá aprovar os documentos apresentados pela CONTRATADA em até 5 (cinco) dias úteis da realização da reunião.

3) A CONTRATADA deverá concluir a execução dos testes de intrusão em até 30 (trinta) dias úteis da aprovação pelo CONTRATANTE dos documentos apresentados na reunião de planejamento.

4) A CONTRATADA deverá entregar ao CONTRATANTE relatório de execução dos testes de intrusão (pentest) em até 10 (dez) dias úteis da conclusão do pentest.

5) O CONTRATANTE deverá avaliar e aprovar o relatório em até 5 (cinco) dias úteis da entrega pela CONTRATADA.

6) A CONTRATADA deverá realizar apresentação do resultado dos testes em até 5 (cinco dias úteis) após a aprovação dos relatórios de execução dos testes de intrusão.

7) O contrato terá vigência de 120 (cento e vinte) dias, sendo que todas as atividades requisitadas contidas no contrato deverão ser executadas durante esse período.

Requisitos de Segurança da Informação - Integrante Demandante e Técnico.:

1) A CONTRATADA deverá seguir todas as Normas, Políticas e Procedimentos de Segurança, aplicáveis, estabelecidos pelo CONTRANTE para execução do Contrato.

1.1) Observar, principalmente, a Política de Segurança da Informação (PSI) formalizada pela Resolução Administrativa (RA) 85/2018 - Política Nº 28 – Institui A Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI): https://www.trt9.jus.br/portal/arquivos/6774415

1.2) Demais políticas podem ser acessadas pelo seguinte link: https://www.trt9.jus.br/transparencia/transparenciaPoliticasTIC.xhtml

2) A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o CONTRATANTE.

2.2) Todos os profissionais da CONTRATADA envolvidos na execução dos serviços, desde o início ou alocados posteriormente, deverão assinar o **TERMO DE COMPROMISSO E SIGILO,** comprometendo-se a manter sigilo de todas as informações que tenham acesso durante a execução dos serviços.

3) A CONTRATADA deverá zelar para que todos os eventuais privilégios de acesso a sistemas concedidos, informação e qualquer outro recurso do CONTRATANTE sejam utilizados exclusivamente na execução dos serviços e pelo tempo estritamente essencial à realização deles.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Requisitos Sociais, Ambientais e Culturais - Integrante Demandante:

1) Estar habilitada juridicamente e em regularidade fiscal, social e trabalhista, conforme Lei de Licitações e Contratos Administrativos - Lei nº 14.133/2021.

2) Cumprir o disposto no Inc. XXXIII, Art. 7º da Constituição Federal de 1988, quanto ao emprego de menores.

Requisitos de Arquitetura Tecnológica - Integrante Técnico:

CARACTERÍSTICAS DOS SERVIÇOS

Reunião inicial de planejamento o teste de intrusão (pentest).

1. A CONTRATADA deverá participar de reunião com equipe técnica do CONTRATANTE, a ser realizada em até 5 (cinco) dias úteis da assinatura do contrato;
2. A reunião poderá ser realizada remotamente, por videoconferência, em data a ser aprovada pelo CONTRATANTE;
3. A CONTRATADA deverá apresentar ao CONTRATANTE proposta de cronograma, detalhando as atividades a serem executadas;
4. A CONTRATADA deverá apresentar ao CONTRATANTE detalhes sobre a metodologia utilizada na execução dos serviços;
5. A CONTRATADA deverá informar a equipe responsável pela execução dos serviços, bem como o papel de cada membro;

6. Os documentos apresentados pela CONTRATADA na reunião deverão ser entregues ao CONTRATANTE em formato PDF, assim como em formato editável (DOC/DOCX);
7. O CONTRATANTE deverá aprovar os documentos apresentados pela CONTRATADA em até 5 (cinco) dias úteis da realização da reunião;
8. Todos os profissionais da CONTRATADA envolvidos na execução dos serviços, desde o início ou alocados posteriormente, deverão assinar TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO se comprometendo a manter sigilo de todas as informações que tenham acesso durante a execução dos serviços.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Execução dos testes de intrusão (pentest).

1. A CONTRATADA deverá concluir a execução dos testes de intrusão em até 30 (trinta) dias úteis da aprovação pelo CONTRATANTE dos documentos apresentados na reunião de planejamento;
2. Os testes serão do tipo externo, ou seja, com origem a partir da Internet, e terão como objetivo principal identificar, mapear e explorar vulnerabilidades nos sistemas e serviços acessíveis pela Internet em eventuais ativos de infraestrutura tecnológica expostos do CONTRATANTE, através de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações da instituição;
3. As atividades do teste de intrusão (pentest) deverão ser realizadas seguindo um caminho de menor resistência, onde deverá ser explorado o ambiente (aplicações e infraestrutura) ao máximo, buscando alcançar a camada mais interna possível.
4. As atividades realizadas durante os testes de intrusão não devem, em qualquer hipótese, se resumir ao uso de ferramentas automatizadas, sendo obrigatória a atuação de equipe especializada na realização de análises dessa natureza, devendo esta realizar análise qualitativa que extrapolem os possíveis relatórios gerados por ferramentas;
5. Todas as atividades realizadas durante o teste de intrusão (pentest) bem como seus resultados devem ser registrados em meio apropriado (logs, gravações de telas, relatórios de ferramentas automatizadas etc) independente do sucesso dos mesmos. Tais registros/evidências devem ser entregues junto com o relatório do teste de intrusão (pentest);
6. A execução dos testes não deverá comprometer ou prejudicar os sistemas e ativos de infraestrutura tecnológica do CONTRATANTE, exceto quando expressamente autorizado;
7. Deverá ser realizado ataque de negação de serviço que deverá durar no máximo 5 (cinco) minutos, após ser expressamente autorizado e agendado pelo CONTRATANTE;
8. A execução dos testes não deverá modificar ou excluir informações e dados nos sistemas e ativos do CONTRATANTE;

9. Todas as fases dos testes de intrusão poderão ser acompanhadas e/ou supervisionadas, a critério do CONTRATANTE, por membro destacado do corpo técnico interno da organização;
10. Qualquer software ou hardware necessário para a execução dos serviços será de responsabilidade do CONTRATADA;
11. A execução dos testes incluirá, no mínimo, as seguintes atividades:

    11.1) Verificação de segurança de ativos tecnológicos relacionados ao escopo;
    11.2) Simulação de ataques com o intuito de testar a segurança das informações da instituição;
    11.3) Medição do nível de exposição das informações para ameaças oriundas do ambiente externo da organização, testando a confidencialidade das informações envolvidas;
    11.4) Identificação e classificação dos riscos das vulnerabilidades encontradas de acordo com o impacto potencial.

12. Os testes poderão explorar elementos relacionados ao escopo, como:

    12.1) Aplicações web;
    12.2) Portais webs;
    12.3) Webservices;
    12.4) Sockets;
    12.5) Serviços web diversos detectados;
    12.5) Componentes de infraestrutura (firewalls, roteadores, bancos de dados, serviços de resolução de nomes, serviços de diretório, storages, máquinas virtuais, sistemas operacionais, dentre outros);

13. Os testes devem incluir minimamente as vulnerabilidades listadas em “2021 CWE Top 25 Most Dangerous Software Weaknesses “ e "OWASP Top 10 - 2017”, não se limitando a estas;

    13.1 Tanto o Testing Guide Versão 4 da OWASP como o CWE – Common Weakness Enumerations, do MITRE, poderão ser utilizados como referenciais de testes que deverão ser executados.

14. Os testes de intrusão (pentest) devem cobrir, o mínimo, as fases descritas abaixo e seus respectivos testes:

Fase de teste	Teste	Descrição
	Observação direta do alvo	Consiste em navegar pela aplicação obtendo acesso a todos os recursos disponíveis publicamente.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Reconhecimento ***(Obter o máximo de informações sobre os ativos contemplados)***	Reconhecimento através de Sites de Busca	Utilizar sites de busca, como Google, para descobrir informações disponíveis (ou vazadas) de aplicações da CONTRATANTE. Buscar através de "***search engines***" especializados como o ***Shodan*** assinaturas de serviços e indícios de má configuração.
	Identificação de pontos de entrada	Realizar varreduras na superfície da aplicação buscando os pontos de entrada explícitos e implícitos mapeando os ataques de injeção modelados.
	Identificação de versões (***fingerprinting***)	Identificar versões de ativos envolvidos (servidor web, servidor de aplicação, sistema operacional, banco de dados e CMS) para correlação com as vulnerabilidades conhecidas e documentadas.
	Descoberta de Aplicações	Enumerar as aplicações hospedadas no mesmo servidor que possam servir de porta de entrada.
	Análise de Mensagens de Erro	Analisar o conteúdo das mensagens geradas em situações inesperadas pela aplicação.
	Descoberta de portais obsoletos e desprotegidos	Procurar por serviços desatualizados, sem patches, vulneráveis, desprotegidos, obsoletos, com configuração inadequada e com a existência de backdoors.
	Verificação de Suporte a SSL / TLS	Avaliar o suporte ao uso de tais protocolos e da maneira como estão implementados.
	Teste de Acesso direto ao Banco de Dados (DB Listener)	Testar a configuração da comunicação entre a aplicação e o banco de dados, avaliando o comportamento do Banco de Dados mediante requisições diretas simulando serem originadas na aplicação.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Teste de configuração ***(Avaliar as configurações dos ativos envolvidos)***	Análise das Configurações da Infraestrutura	Verificar a aderência com boas práticas de segurança por parte da configuração descobertas dos ativos envolvidos (servidor web, servidor de aplicação, sistema operacional, banco de dados, CMS e etc) para correlação com vulnerabilidades conhecidas e documentadas.
	Teste de Manuseio de extensões de arquivos	Buscar por informações sobre as tecnologias utilizadas através da identificação das extensões dos arquivos presentes na aplicação. Realizar uma avaliação de como a aplicação manipula arquivos referenciados diretamente com extensões inesperadas.
	Análise de Arquivos não referenciados, obsoletos e backups	Identificar os arquivos presentes (e acessíveis) na aplicação em questão mesmo que não sejam diretamente referenciados. Arquivos de rascunho, cópias de segurança e arquivos obsoletos podendo expor informações sensíveis caso tenham suas permissões de acesso negligenciadas e que estejam acessíveis via Internet.
	Identificação de Interfaces administrativas	Identificar as interfaces administrativas através de caminhos comuns e referências diretas. As interfaces identificadas podem ser submetidas a ataques de força bruta.
	Verificação de Métodos suportados pelo servidor	Verificar os métodos HTTP suportados pelo Servidor. Identificar os métodos potencialmente perigosos e de vulnerabilidade de ***Cross Site Tracing*** (XST).
	Verificação de configurações de servidores e redes	Verificar a existência de bugs /vulnerabilidades/erro de configuração que permita ações do tipo buffer overruns e race conditions, manipulação de DNS (dns spoofing), acessos privilegiados a servidores (Active Directory, Web Servers, E-mail etc), anomalias de roteamento, componentes que possam ser utilizados como vetor de ataque,

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

		vulnerabilidades associadas a¿ personificação de máquinas confiadas (trusted hosts).
Testes de Autenticação ***(Avaliar os esquemas e controles de autenticação)***	Teste sobre canais de transporte de credenciais	Verificar os dados que os usuários inserem em formulários web a fim de se autenticar na aplicação que são transmitidos usando protocolos seguros que os protejam de ataques de captura de dados.
	Teste de enumeração de usuários	Verificar a possibilidade de coleta de nomes de usuários válidos através da interação com o mecanismo de autenticação da aplicação.
	Teste de descoberta de usuários comuns / padrão	Identificar as contas de usuário padrão ou combinações usuário/senha fáceis de adivinhar.
	Teste de força bruta	Identificar combinações usuário/senha utilizando métodos de busca exaustiva.
	Teste visando contornar do esquema de autenticação	Identificar os recursos da aplicação que não estejam adequadamente protegidos pelo esquema de autenticação.
	Teste sobre funções de armazenamento /redefinição de senhas	Avaliar os métodos de redefinição /recuperação de "senhas esquecidas" e se a aplicação permite que o usuário armazene senhas no navegador (função "lembrar senha").
	Teste de gerenciamento de logout e cache do navegador	Verificar se as funções de ***logout*** e de uso de ***cache*** pelo navegador estão adequadamente implementadas.
		Identificar os vetores de ataque sobre implementações de CAPTCHA ("***Completely***

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

	Teste sobre o CAPTCHA	***Automated Public Turing test to tell Computers and Humans Apart***").
	Teste sobre autenticação em múltiplas etapas	Analisar a presença/configuração de cenários do tipo: Geradores de senha descartável (***One-time password***), Dispositivos de identificação por criptografia, Verificar as informações pessoais que somente o usuário legítimo deveria saber e etc.
	Teste sobre condições de corrida	Identificar as condições que produzem resultados inesperados quando o momento em que uma ação ocorre, influencia outras ações.
Testes de Autorização ***(Avaliar os esquemas e controles de autorização)***	Teste de adulteração de caminhos de diretórios	Verificar a possibilidade de executar ataques de adulteração de caminhos de diretórios (***path traversa attack***) e acessar informações protegidas.
	Teste de contorno do esquema de autorização	Verificar o esquema de autorização a fim de confirmar se cada perfil/privilégio tem acesso apenas a funções/recursos esperados.
	Teste de escalada de privilégios	Verificar a possibilidade de um usuário modificar seus privilégios/perfil na aplicação através da manipulação de requisições.
	Cross Site Scripting Refletido / Armazenado / baseado em DOM	Manipular as entradas passando instruções maliciosas através de ***scripts*** destinados ao navegador da vítima.
	Injeção de instruções SQL / LDAP / ORM / XML / SSI / XPath	Manipular as entradas passando instruções maliciosas para serviços internos.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Testes de Validação de Dados	Injeção de código e comandos de sistema operacional e serviços	Manipular as entradas passando comandos para serviços que se comunicam com a aplicação ou diretamente para o sistema operacional.
	Estouro de buffer (buffer overflow)	Verificar a presença de vulnerabilidades que permitam a execução de ataques de estouro de buffer (***buffer overflow***) sobre o servidor web.
	Manipulação de Validação Interna	Avaliação do processo de validação da aplicação sobre entradas geradas por ela mesma.
	HTTP Splitting /Smuggling	Manipular os dados contidos em cabeçalhos de requisições HTTP, avaliando o processo de validação da aplicação sobre entradas geradas por ela mesma
Testes de Negação de Serviço ***(Identificar vulnerabilidades dentro da aplicação web que possa***	Verificação de consultas com SQL Wildcard	Verificar a inclusão de entradas contendo SQL ***Wildcards*** a fim de forçar o banco de dados da aplicação a fazer consultas SQL extremamente custosas à CPU.
	Teste de trancamento de contas de usuários	Verificar se é possível trancar contas de usuários válidos através de sucessivas tentativas mal sucedidas de autenticação.
	Teste de estouro de buffer ou alocação de memória	Verificar a presença de vulnerabilidades que permitam alocar objetos na memória massivamente a ponto de esgotar os recursos do servidor web.
	Teste de injeção de condições de laço (loop)	Avaliar se é possível um usuário injetar código contendo laços que provoquem queda de desempenho da aplicação.
		Avaliar se é possível um usuário injetar dados ou gerar logs que o servidor web

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

permitir a um usuário malicioso tornar determinada funcionalidade ou até¿ o website inteiro indisponível)	Teste de escrita de dados no disco	armazena em disco a ponto de esgotar o espaço de disco comprometendo a disponibilidade da aplicação.
	Teste de armazenamento de dados de sessão e liberação de recursos	Avaliar se é possível alocar grandes massas de dados em objetos de sessão de usuário a fim de esgotar os recursos de memória do servidor web e verificação quanto ao tratamento da liberação de recursos pela aplicação, que podem provocar condições de esgotamento de recursos.
	Testes de negação de serviço	Os testes de invasão que possam levar a negações de serviço (***Denial of Service*** – DoS - - e DDoS – ***Distributed Denial of Service***) deverão ser realizados após autorização explícita da CONTRATANTE, que definirá os dias, horários e tempo máximo de indisponibilidade do serviço durante a execução dos testes.
Testes de Web Services	Teste de coleta de informações do web service	Coletar as informações sobre os pontos de entrada e meios de comunicação do ***web service.***
	Teste do WSDL	Verificar as informações contidas no WSDL em busca de pontos de entrada e tentativa de realizar operações não previstas como requisições SOAP padrão a fim de obter informações confidenciais.
	Teste estrutural de XML	Avaliar se é possível enviar uma mensagem XML muito grande ou mal formada a fim de provocar uma condição de negação de serviço devido a queda de desempenho do servidor causada pelo alto processamento do ***parser*** XML ou esgotamento de memória.
		Verificar se é possível a execução de ataques como injeção de SQL, de ***XPath***, de comando do sistema operacional, ataques

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

	Teste ao nível de conteúdo do XML	de estouro de ***buffer***, entre outros, sobre o servidor que hospeda o ***web service*** e as aplicações que o utilizam.
	Teste de parâmetros HTTP /REST	Verificar se é possível a execução de ataques como injeção de SQL, de ***XPath***, de comando do sistema operacional, ataques de estouro de ***buffer***, entre outros, utilizando uma requisição GET do HTTP.
	Teste de envio de arquivos maliciosos ao web services SOAP	Avaliar se é possível enviar arquivos maliciosos à ***web services*** que recebem arquivos.
	Teste de ataque de replay	Verificar se é possível reenviar requisições válidas ao ***web service***, visando assumir a identidade de um usuário válido
Testes sobre APEX ***(Identificar vulnerabilidades específicas de APEX (Oracle Application Express)***	Teste sobre vulnerabilidades do APEX	Verificar as vulnerabilidades relacionadas à exposição de funções internas da aplicação (***client-side functions***), URLs inseguras etc.
	Teste sobre APEX	Verificar a execução de ataques sobre aplicações web tradicionais sobre as que utilizam ***APEX***.
	Análise de Esquema de Gerenciamento de Sessão	Identificação dos atributos usados para gerenciamento de sessão. Enumeração de credenciais e mecanismos de controle utilizado.
	Análise de Atributos utilizados em Cookies	Análise da configuração dos atributos de controle utilizados nos cookies presentes nas transações com a aplicação.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Teste de gerenciamento de sessões	Teste de fixação de sessão	Avaliação do comportamento da aplicação no que diz respeito a renovação e reutilização de atributos de controle.
	Identificação de variáveis de sessão expostas	Avaliação da exposição de atributos de controle e possibilidade de manipulação dos mesmos.
	Teste de CSRF	Avaliação da possibilidade de forçar um usuário desconhecido a executar ações indesejadas na aplicação, ataque este conhecido como Cross Site Request Forgery (CSRF)

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

15. Caso algum teste solicitado não possa ser realizado, devido a escolha em comum acordo da modalidade de pentest (Black, Gray ou White Box), o fato deve ser informado pela CONTRATADA imediatamente após a reunião inicial.

Requisitos do Projeto de Implantação - Integrante Técnico:

1) Deverá haver a prestação de serviço especializado em teste externo de intrusão (pentest) em aplicações e endereços de internet do Tribunal Regional do Trabalho da 9a Região, visando identificar, mapear e explorar possíveis vulnerabilidades nos sistemas e serviços acessíveis pela Internet, e em eventuais ativos de infraestrutura tecnológica expostos;

1.1) O formato de aplicação do Teste de Intrusão, a modalidade do Pentest - Black Box, Gray Box ou White Box - deverá ser definido na reunião inicial do projeto, em comum acordo entre as partes.

2) Estão incluídos neste objeto o planejamento dos testes, a execução dos testes utilizando ferramentas e conhecimentos especializados, clarificação de dúvidas durante todo o processo, confecção de relatórios, apresentações para demonstração de resultados, bem como todas as atividades necessárias à execução do objeto durante a vigência contratual;

3) O escopo dos serviços executados será limitado a:

3.1) Um domínio (perímetro externo);

3.2) Uma faixa de endereços válidos na Internet (máscara de 24 bits).

4) Os serviços executados pela CONTRATADA deverão observar as orientações e técnicas de padrões internacionais tais como:

4.1) OSSTMM 3 (The Open Source Security Testing Methodology Manual);

4.2) NIST-SP 800-115 (Technical Guide to Information Security Testing and Assessment);

4.3) OWASP TESTING GUIDE 4 (The Open Web Application Security Project);

4.4) ISO/IEC 27002:2013 (Código de prática para controles de segurança da informação).

ROBSON CLEITON NOVAK 25/04/2022 SGSI

PAULO ROBERTO NUNES 25/04/2022 DSIR

PAULO CELSO GERVA 26/04/2022 SLC

Requisitos de Garantia e Manutenção - Integrante Técnico:

1) A CONTRATADA deverá prestar suporte ao CONTRATANTE durante o período de vigência do contrato, através de telefone e correio eletrônico.

2) Durante a vigência contratual, a CONTRATADA deverá atender número ilimitado de incidentes de suporte, desde que relacionados aos serviços a serem executados.

3) O suporte técnico deverá ocorrer, pelo menos, em regime “8x5" (8 horas por dia, 5 dias por semana).

Requisitos de experiência/formação da equipe que projetará, implantará e manterá - Integrante Técnico:

A equipe técnica da CONTRATADA designada para a execução das atividades de pentest deverá ser composta por profissionais que possuam, **no mínimo, DUAS** das certificações listadas abaixo:

a) CPTE - CERTIFIED Penetration Testing Engineer - Mile2;
b) CISSP - Certified Information Systems Security Professional;
c) CPT - IACRB Certified Penetration Tester;
d) CEPT - Certified Expert Penetration Tester;
e) CMWAPT - Certified Mobile and Web Application Penetration Tester;
f) CRTOP - Certified Red Team Operations Professional;
g) EC-Council Certified Ethical Hacker (CEH);
h) EC-Council Licensed Penetration Tester Master (LPT);
i) EC Council Security Analyst (ECSA);
j) EC-Council – Certified Network Defence Architect (CNDA)
k) CompTIA Cybersecurity Analyst (CySA+);
l) CompTIA Security+ (SY0-501 ou SY0-601));
m) CompTIA Security Analytics Professional (CSAP);

n) CompTIA PenTest+;
o) Global Information Assurance Certification (GIAC) Penetration Tester (GPEN);
p) Global Information Assurance Certification (GIAC) Web Application Penetration Tester (GWAPT);
q) Global Information Assurance Certification (GIAC) Certified Intrusion Analyst (GCIA);
r) Global Information Assurance Certification (GIAC) Exploit Researcher and Advanced Penetration Tester (GXPN);
s) OSCP - Offensive Security Certified Professional;
t) Penetration Tester Desec Security.

As certificações que comprovam a qualificação técnica da equipe da CONTRATADA deverão ser apresentadas ao CONTRATANTE para conferência previamente à assinatura do contrato.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Requisitos de Metodologia de Trabalho - Integrante Técnico:

A execução dos serviços pela CONTRATADA será composta, em linhas gerais, pelas seguintes atividades:

1) Reunião inicial de planejamento do teste de intrusão (pentest);

2) Execução dos testes de intrusão (pentest);

3) Confecção e entrega de relatórios tanto em nível técnico como gerencial, além da disponibilização das evidências geradas;

4) Apresentação dos resultados e relatórios ao CONTRATANTE;

5) Entrega dos vídeos/conteúdo das apresentações ao CONTRATANTE;

6) Exclusão de quaisquer dados sensíveis/sigilosos do CONTRATANTE da base de dados da CONTRATADA.

Requisitos de Segurança, sob o ponto de vista técnico - Integrante Técnico:

Os testes de invasão que possam levar a negações de serviço (Denial of Service – DoS e DDoS – Distributed Denial of Service) deverão ser realizados após autorização explícita do CONTRATANTE, que definirá os dias, horários e tempo máximo de indisponibilidade do serviço durante a execução dos testes.

Análise do Mercado de TI (ID 7457907)

Portal do Software Público Brasileiro:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede.

Modelo Nacional de Interoperabilidade - MNI:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede.

Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede.

Modelo de Requisitos Moreq-Jus:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede.

Adequação do Ambiente do Órgão (ID 7457912)

Necessidade de Adequação - Infraestrutura tecnológica:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede. Não há necessidade de adequação de nossa infraestrutura para realização do teste.

Necessidade de Adequação - Infraestrutura elétrica:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede. Não há necessidade de adequação de nossa infraestrutura para realização do teste.

Necessidade de Adequação - Logística de implantação:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede. Não há necessidade de adequação de nossa infraestrutura para realização do teste.

Necessidade de Adequação - Espaço físico:

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede. Não há necessidade de adequação de nossa infraestrutura para realização do teste.

Necessidade de Adequação - Mobiliário:

ROBSON CLEITON NOVAK 25/04/2022 SGSI

PAULO ROBERTO NUNES 25/04/2022 DSIR

PAULO CELSO GERVA 26/04/2022 SLC

Não aplicável ao serviço contratado. Trata-se de contratação de serviço de teste de penetração em rede. Não há necessidade de adequação de nossa infraestrutura para realização do teste.

ROBSON CLEITON NOVAK 25 /04/2022 SGSI

PAULO ROBERTO NUNES 25 /04/2022 DSIR

PAULO CELSO GERVA 26 /04/2022 SLC

Transferência de Conhecimento:

A CONTRATADA deverá entregar ao Tribunal toda e qualquer documentação gerada em meio físico ou digital em função da prestação de serviços, incluindo gravação das reuniões de apresentação dos relatórios.

Direitos de Propriedade Intelectual:

A CONTRATADA deverá ceder os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos técnicos e produtos gerados ao longo da execução do contrato.