Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. Objeto

Contratação de empresa especializada para execução de serviços técnicos contínuos de segurança da Informação referente a Testes de Intrusão (PENTEST) Externos e Internos aos Sistemas e Redes da PROCEMPA, com fornecimento de relatórios específicos de avaliação de vulnerabilidades expostas.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1 Razão da necessidade de contratação

Cada vez mais violações de segurança vem ocorrendo no Brasil e no mundo, e as organizações precisam se proteger e manter a integridade dos seus dados. Torna-se fundamental que as empresas invistam na qualidade da sua segurança, realizando testes contínuos e demonstrando aos seus parceiros de negócios que você leva a sério a segurança cibernética.

A tecnologia sempre surge com o objetivo de auxiliar nas atividades diárias do ser humano, criando assim uma dependência. Com a necessidade de permanecer em casa devido à pandemia de COVID-19, muitas atividades tiveram que ser adequadas para o home office.

Com o aumento de pessoas conectadas, aumentaram também os ataques digitais. Esses ataques a empresas e pessoas em todo o mundo podem ocorrer de diversas formas, uma delas é pela instalação de softwares maliciosos, como os ransomwares.

Algumas medidas podem ser tomadas com o intuito de prevenção. No entanto, é necessário se identificar onde e quais são as **fragilidades e vulnerabilidades da empresa**. Com a certeza do que essas informações trarão, se terá um processo de aprimoramento das defesas mais efetivo e certeiro para solucionar os problemas da empresa.

O **Pentest**, abreviação do termo em inglês **Penetration Test** (**Teste de Penetração**, em tradução literal), é também conhecido como o **Teste de Intrusão**, onde fará a detecção minuciosa com técnicas utilizadas pelos hackers éticos. Esses hackers são profissionais especialistas em **segurança da informação** que são contratados pela organização para realizar os testes, sem que exerçam atividades que prejudiquem a empresa ou tenham efeitos criminosos.

Ao se aplicar o **Pentest**, se poderá encontrar as potenciais vulnerabilidades em um sistema, servidor ou de uma estrutura de rede. Além disso, o **Pentest** usa ferramentas específicas para realizar a intrusão, que mostram quais as informações ou dados corporativos estão expostos e passíveis de serem roubados por meio desta ação. Assim, a Procempa poderá conhecer mais a fundo suas fraquezas e onde será necessário melhorar as defesas do sistema, rede ou servidor. Os esforços e investimentos em **segurança da informação** serão focados nos **pontos de fragilidade da organização**, fortalecendo a estrutura contra qualquer gargalo de segurança em potencial.

Existem algumas maneiras de se aplicar o **Pentest**, onde cada uma delas terá uma eficácia diferente e será selecionado a partir das necessidades da empresa. Entre esses diferentes métodos, podemos destacar a White Box, a Black Box e, por fim, a Grey Box.

White Box

Ao se aplicar o teste do método white box, ou caixa branca, se tem um **teste de intrusão** mais completo. Isto se dá por ter uma análise integral, que avaliará toda a infraestrutura da rede. Onde, ao iniciar o teste, o hacker ético já possui o conhecimento de todas as informações essenciais da empresa, como as senhas, IPs, logins e demais dados que dizem respeito à rede, servidores, estrutura, potenciais medidas de segurança e firewall. Será a partir dessas informações preliminares que o teste será direcionado de modo que seu ataque seja mais eficiente e seja possível descobrir o que tem maior necessidade de ser aprimorado e reorientado.

Black Box

O black box, caixa-preta, se trata de um teste às cegas, onde o hacker não tem grande informação disponível sobre a corporação. Mesmo que seja direcionada, já que atingirá a empresa contratante e descobrirá as suas vulnerabilidades, o **pentest** de caixa-preta será o mais próximo de um ataque externo real.

Por suas características, sem um grande mapeamento de informações, ele agirá de forma muito similar aos criminosos. Isso permite uma experiência muito importante para a empresa, pois a invasão, caso não tenha intenções maliciosas, servirá como um método de reconhecer as fragilidades na estrutura da rede.

Grey Box

Como o próprio nome indica, caixa cinza, esse método é uma mistura dos dois anteriores, assim o profissional já possuirá algumas informações específicas para a realização do **teste de intrusão**.

A quantidade de informações compartilhadas será baixa, e não se compara a quantidade de dados disponibilizados em um **pentest** de caixa branca.

Assim, esse teste investirá seu tempo e recurso em identificar as vulnerabilidades e possíveis ameaças, se baseando na quantidade de informações específicas que tem disponível.

O **Pentest** pode ser dividido em alguns tipos, de acordo com o serviço que será desempenhado. Esses tipos são:

Teste de serviço de rede: se dá pela realização de análises da infraestrutura de rede da corporação, em procura de **fragilidades** que podem ser solucionadas. Neste quesito, são avaliadas as configurações de firewall, testes de filtragem, entre outros.

Teste de aplicação web: é feita uma análise extremamente detalhada e as vulnerabilidades são facilmente descobertas por se basear na busca em aplicações web.

Teste de client side: nesse tipo a exploração dos softwares, programas de criação de conteúdo, entre outros, em computadores de usuários.

Teste de rede sem fio: neste é feito o exame de todas as redes sem fio utilizadas na corporação. Os testes são feitos em protocolos de rede sem fio, pontos de acesso e credenciais administrativas.

Teste de engenharia social: se utiliza de manipulação psicológica, como uma tentativa de induzir os colaboradores a repassarem itens e dados sigilosos.

Os principais benefícios são:

Auxiliar a empresa na verificação e testagem da capacidade de sua segurança digital;

Permite descobrir as **fragilidades no sistema de segurança** antes do criminoso descobrir;

Proporciona a possibilidade às empresas de adotarem novas posturas em relação à Segurança da Informação, assim como apresentar as justificativas que respaldam o investimento na área;

O **Pentest** protege a reputação da empresa, uma vez que mostra o comprometimento em assegurar a continuidade do negócio e manutenção da relação efetiva com a segurança corporativa.

> ***"A informação é um ativo muito importante para qualquer organização, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé podem comprometer significativamente, não apenas a imagem da organização perante terceiros, como também o andamento dos próprios processos organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações."***
>
> **(TCU – Manual de Boas Práticas em Segurança da Informação)**

2.2 A demanda da PROCEMPA tem como base as seguintes informações e histórico de necessidades:

Devido à complexidade e criticidade das informações administradas pela PROCEMPA, enquanto empresa pública de TIC, bem como para melhor gerenciar a Segurança da Informação nos seus aspectos de confidencialidade, integridade e disponibilidade, em conformidade com sua Política de Segurança da Informação

Para que haja maior transparência e autonomia na análise de eventuais vulnerabilidades encontradas na rede e nos Sistemas utilizados pela PROCEMPA, é necessária a contratação de empresa especializada para realizar, especificamente, os testes de intrusão, checando assim o nível de segurança da PROCEMPA e contribuindo na gestão de segurança.

3. Modalidade da Licitação - Pregão Eletrônico

3.1. Da Justificativa da Modalidade
O objeto caracterizado por este Termo de Referência tem padrões de qualidade e desempenho definidos objetivamente, além de se tratar de objeto plenamente disponível no mercado.

3.2 Das Restrições de competição previstas em Lei
A CONTRATADA, desde que com a prévia e expressa autorização do gestor do contrato da PROCEMPA, pode subcontratar parcela do objeto deste contrato, desde que não se refira a parcela sobre a qual a PROCEMPA exigiu atestado de capacidade técnica durante o processo licitatório. A subcontratação pode abranger aspectos acessórios e instrumentais de tais parcelas.

3.3 Condições de Participação:
Não será permitida a participação de empresas reunidas em consórcio ou cooperativa uma vez que os serviços prestados em cada um dos itens exigem elevada especialização técnica e controle uníssono para fiscalização do contrato.

4. Modo de Disputa

4.1 Critério de julgamento: Menor Preço

5. Da Especificação dos Itens

A contratação será de banco de horas a serem consumidas sob demanda, de forma planejada, em um período de 1 ano.

A quantidade de total do banco de horas, estimada em 600 horas (seiscentas horas) para teste de invasão em redes e 3.540 (três mil quinhentos e quarenta) horas para teste de invasão em sistemas, foi baseada no seguinte cenário:

Média de 17 (dezessete) horas por aplicação e 6 (quinze) horas por serviço/ativo de rede para testes de segurança

Estimaram-se cerca de 200 (duzentos) sistemas e 100 (cem) serviços/ativos de rede a serem escolhidos em momento oportuno.

Item	Objeto	Descrição	Quantidade	Unidade
1	Serviço de Teste de invasão em redes	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 (**Wireless**) e **Rede** de Área Local (**LAN**) do tipo Externos e/ou Internos.	600	Horas
2	Serviço de Teste de invasão em sistemas no padrão Red Team, Blackbox, GreyBox e WhiteBox.	Testes para identificar falhas de segurança em sistemas	3.540	Horas

Serviços para os itens 1 e 2

5.1.1 A atividade de Testes de Invasão poderá ser do tipo Externos e/ou Internos (in loco) e terá como objetivo principal análise geral do ambiente da PROCEMPA quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica da PROCEMPA, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.

5.1.2 A empresa contratada deverá entregar à equipe da DPO – Data Protection Officer todo detalhamento dos testes de invasão a serem realizados, desde os ativos que foram testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.

5.1.3 O teste de invasão de redes só poderá acontecer mediante autorização da DPO, com anuência da T-GT2 – Gerência de Infraestrutura.

5.1.4 O teste de invasão de sistemas só poderá acontecer mediante autorização da DPO, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.

5.1.5 Para toda vulnerabilidade encontrada, a Contratada deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo da PROCEMPA decidir pela liberação.

5.1.6 O tempo estimado para cada teste deve considerar as atividades entre: varreduras, mapeamentos, testes e análise. O tempo gasto pelos testes automatizados devem se limitar apenas a esforço gasto para manipulação da ferramenta, desconsiderando o tempo de varredura.

5.1.7 Todos os testes a serem realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações da PROCEMPA.

5.1.8 Estes testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações da PROCEMPA, e devem observar orientações e técnicas emanadas por padrões internacionais ou equivalente apresentados pela empresa CONTRATADA, caso possua, em seu portfólio, normativos que complementem os demonstrados abaixo:

5.1.9 OSSTMM 3 (*The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined)*;

5.1.10 ISSAF/PTF (Information Systems Security Asssessment Framework);

5.1.11 NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);

5.1.12 NIST Special Publication 800-42 (Guideline on Network Security Testing)

5.1.13 OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.

5.1.14 PCI DSS (Payment Card Industry Data Security Standard)

5.1.15 PCI SSC Information Supllement

5.1.16 PTES (Penetration Testinf Execution Standard)

5.1.17 A CONTRATADA deverá realizar, no mínimo, 01 (uma) vez a cada 06 (seis) meses, simulações de invasão, com o consentimento da PROCEMPA, a ativos e informações (Teste de Invasão) a serem executadas internamente (qualquer ponto da rede corporativa da PROCEMPA) ou externamente (através da Internet), com duração de até 15 (quinze) dias cada teste.

5.1.17.1 Caso necessário a PROCEMPA poderá solicitar teste sob demanda utilizando as horas contratadas conforme item 5.1.18.

5.1.18 Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério da PROCEMPA.

5.1.18.1 Cada fase deve ser feita durante o período que não comprometa processamento da PROCEMPA, sendo feita em no máximo 2 dias corridos no total.

5.1.20 Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverá ser reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

5.1.21 Transferência de conhecimento técnico com apresentações dos serviços.

5.1.22 Evolução do atual modelo de gestão de segurança da informação com aumento consequente do nível de maturidade.

5.1.23 Teste de Intrusão

5.1.23.1 O teste de invasão deverá obedecer às seguintes fases:

a. Planejamento;

b. Descoberta;

c. Ataque;

d. Relatório de Teste de Invasão;

e. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;

f. Reavaliação, novo teste após remediação;

g. Relatório final do Teste de Invasão.

5.1.23.2 Planejamento:

5.1.23.2.1 Todas as premissas, processos, atividades descritas, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento para os tipos de teste de penetração a seguir:

a. **PENTEST DE REDE interna e externa**: Este teste é focado em recursos de rede, onde o escopo é definido em termos de endereços IP e intervalos de rede. Os testes de rede externa também podem ter o escopo definido em termos de nomes de domínio (o avaliador precisa descobrir os endereços de rede associados a esses domínios como parte do teste).

b. **PENTEST DE APLICAÇÃO**: Este teste é focado em aplicação, geralmente aplicação web, mobile e cliente/servidor. Os avaliadores se concentrarão em encontrar e explorar vulnerabilidades somente nessa aplicação.

c. **PENTEST DE REDE SEM FIO:** Este teste é semelhante a um pentest de rede, mas o escopo é definido por redes sem fio, tanto faz se especificadas diretamente pelos identificadores de conjunto de serviços (SSIDs) e localização física ou apenas por localização (por exemplo, “qualquer rede sem fio da PMPA – Prefeitura Municipal de Porto Alegre”).

d. **PENTEST DE ACESSO REMOTO**: este teste é semelhante a pentest de rede, mas o escopo é definido em pontos específicos de acesso à rede corporativa (como VPN de acesso remoto de funcionários ou VPN B2B)

e. **PENTEST DE ENGENHARIA SOCIAL**: quando os testes incluem a tentativa de enganar as pessoas para fornecer dados confidenciais ou privilégios de acesso ao avaliador, os tipos de truques a serem executados (como golpes de telefone, tentativas de phishing ou acesso físico) e alvos autorizados (como pessoas que podem ser alvo do teste, incluindo executivos, agentes do call center ou qualquer pessoa no escritório principal) são parte da definição do escopo.

f. TESTE FÍSICO OU DE INSTALAÇÕES: estes testes abrangem controles de segurança física, como controle de acesso a instalações e recursos de TI. Um teste típico de segurança física pode incluir acesso a um centro de dados e acesso direto aos racks dos servidores. Também pode ser focado em ambientes de escritório, verificando a disponibilidade de informações confidenciais em papel ou acesso a desktops e laptops dos usuários.

5.1.23.2.2 Todos os testes bem-sucedidos devem ser gravados e/ou registrados em documentos restritos para compor as ações dos serviços realizados.

5.1.23.2.3 Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas, podendo ser utilizadas ambas, conforme definição do escopo:

5.1.23.2.4 Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista, pois a maioria das pessoas entende que os pentes implicam fornecer ao avaliador apenas as informações necessárias sobre o ambiente alvo para definir o escopo. Embora esta seja a abordagem mais comum, conhecida como “caixa-preta”, esta não é a única opção. Os testes de caixa-preta são adequados quando a organização está interessada em ver a quantidade de informação sobre seu ambiente e sistemas pode ser obtida pelo avaliador. Quando a intenção do teste é verificar o que um invasor externo poderia fazer, esta é a opção preferida. No entanto, a extensão do que será testado pode acabar limitada pela quantidade de informações sobre o meio ambiente que o avaliador pode obter. A falta de resultados neste caso não significa que não existam vulnerabilidades exploráveis, mas que o avaliador não conseguiu encontrar onde procurá-los).

5.1.23.2.5 Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste, visto que em testes de caixa branca, a organização compartilha todas as informações sobre o ambiente alvo. Em testes de rede, isso pode incluir os endereços IP e as funções dos servidores na rede, topologias de rede e espaços de endereço existentes, ou todos os nomes de domínio usados pela organização. Os testes de aplicativos que seguem a abordagem da caixa branca geralmente incluem credenciais para o aplicativo (para que o invasor possa se concentrar em privilégios de escalada e executar transações não autorizadas em vez de obter acesso) ou mesmo o código-fonte. Os testes de caixa branca têm maiores chances de encontrar vulnerabilidades e dar mais garantia de que todos os pontos

potencialmente vulneráveis são testados. Os testes de caixa branca podem ser uma opção mais realista para validar o que podem ser feitos pelos iniciados);

5.1.23.2.6 Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo, ou seja, o modelo de caixa cinza é uma abordagem “do meio da estrada” que tenta ganhar valor a partir de modelos preto e branco. Em um teste de caixa cinza, a organização compartilha apenas informações suficientes para garantir que o avaliador encontre e teste os pontos que espera ser testados. Quando as redes em escopo são muito grandes, também faz sentido compartilhar algumas informações sobre os pontos mais interessantes; Isso evitará situações em que o avaliador gaste muito tempo em recursos menos importantes. Nos testes de aplicativos, fornecer credenciais de acesso básicas também garante que o avaliador testará partes do aplicativo que só são acessadas por usuários autenticados. As aplicações tipicamente terão uma boa camada de autenticação, o suficiente para evitar que o assessor acesse a área autenticada, mas existem vulnerabilidades graves nessa área. Nesses casos, Um teste puro de caixa-preta pode dar à organização uma falsa percepção de segurança. É aqui que um modelo de caixa cinza pode fornecer o melhor equilíbrio entre um cenário realista e uma avaliação mais completa).

5.1.23.2.7 Técnicas de Operações Red Team: Consiste em um ataque realista e sem limites no ambiente geral da PROCEMPA onde será utilizada métodos não destrutivos necessários para atingir um conjunto de objetivos definidos de comum acordo entre as partes, simulando o comportamento de um atacante em todas as suas esferas. A atividade desta técnica imita bem os métodos de ataque aos ativos e furtivos de um atacante real com o uso de TTPs (Tactics, Techniques, and Procedures). Esta técnica objetiva externar ao PROCEMPA avaliar a capacidade da sua equipe de segurança de detectar e responder a um cenário de ataque ativo.

5.1.23.2.8 E outras técnicas novas que surgirem e não estão definidas aqui, mas acordadas com a PROCEMPA e definidas no Plano de Teste de Penetração.

5.1.23.3 Deverá ser elaborado o “PLANO DE TESTE DE PENETRAÇÃO”, para cada teste ou reavaliação, novo teste pós remediação do teste realizado anteriormente, contemplando as informações de PLANEJAMENTO do teste, tais como:

5.1.23.4 Objetivos, premissas e escopo do teste, datas e horas dos testes, realizações, metodologias, vulnerabilidades encontradas, categorização e

severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.

5.1.25 Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:

5.1.25.1 Detalhes da infraestrutura alvo dos testes de invasão;

5.1.25.2 Equipamentos e recursos demandados para este teste;

5.1.25.3 Tipos de ataque que serão realizados;

5.1.25.4 Prazos (janela de tempo para execução dos testes);

5.1.25.5 Contato da CONTRATADA (responsáveis para tratamento de questões não abordadas nos testes);

5.1.25.6 Tipos de testes a serem realizados pelos especialistas em segurança da informação

5.1.26 Os alvos dos “Testes de Invasão”, bem como as premissas e condições para realização dos mesmos serão definidos e aprovados pela PROCEMPA.

5.1.27 Planejamento das atividades: compreende a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e do cronograma de execução.

5.1.28 Análise de vulnerabilidades do ambiente de TI externo: avaliação da existência de vulnerabilidades para até 100 (cem) serviços/ativos definidos pela PROCEMPA;

5.1.29 A CONTRATADA não deverá alterar a integridade das informações, ou seja, não deve alterar informações dos servidores e sistemas que possam comprometer os serviços da CONTRATADA. Caso o teste cause alguma indisponibilidade de serviço, isso deve ser informado à PROCEMPA imediatamente.

5.1.30 Teste manual das vulnerabilidades do ambiente TI interno e/ou externo: avaliação da possibilidade de exploração, comprometimento e/ou vulnerabilidades do ambiente de TI, para até 100 (cem) serviços/ativos, definidos pela PROCEMPA. Para o tipo de teste interno, este deverá ocorrer dentro das dependências da CONTRATADA, pois para esse teste não será fornecido VPN para realização deste tipo de teste.

5.1.31 Testes de Invasão em Aplicações

5.1.31.1 Deverão ser realizados testes de invasão do tipo “Cross Site Scripting (XSS)”.

5.1.31.2 Deverão ser realizados testes de invasão do tipo “Injeção de Código;

5.1.31.3 Deverão ser realizados testes de invasão do tipo “Inclusão Remota de Arquivos (RFI)”;

5.1.31.4 Deverão ser realizados mapeamentos e sondagens, com o objetivo de identificar possíveis vetores de entradas de ataques;

5.1.31.5 Deverão ser realizados testes de invasão do tipo “Referência Direta a Objetos”.

5.1.31.6 Deverão ser realizados testes de invasão do tipo “Vazamento de informações”, onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda.

5.1.31.7 Deverá ser realizado testes de invasão baseado em “Gerenciamento de Sessões”.

5.1.31.8 Deverão ser analisadas, pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.

5.1.31.9 Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações;

5.2 Serviço de Auditoria de Segurança em Códigos Fonte de Aplicações

5.2.1 Para a efetiva correção de uma vulnerabilidade poderá ser necessário a avaliação/auditoria do código fonte de uma determinada aplicação.

5.2.2 As auditorias podem ser realizadas tanto remotamente ou presencialmente na sede da PROCEMPA.

5.2.3 Para a realização das auditorias, a PROCEMPA disponibilizará o código-fonte da aplicação a ser auditada, que deverá ser mantida sob sigilo.

5.2.4 O tempo estimado para cada auditoria deve considerar as atividades de reuniões, dentre planejamentos, varreduras, mapeamentos, testes, análise e elaboração e apresentação dos resultados.

5.2.5 A auditoria de códigos-fonte visa avaliar, dentre outros itens, os seguintes conceitos:

5.2.5.1 Avaliação do fluxo de informações indo desde a arquitetura física (ex:

fluxo de informações entre camadas web, camadas de aplicação e bancos de dados) até o fluxo de informações entre os módulos - variáveis e parâmetros.

5.2.5.2 Avaliação das lógicas de negócio requisitadas e implementadas. Detecção de possíveis fraudes internas ou vulnerabilidades na implementação das lógicas de negócio.

5.2.5.3 Avaliação da utilização das APIs e construtos da linguagem de programação apontamento dos locais no código onde é feito uso inseguro das bibliotecas do sistema, dos elementos da linguagem de programação e recomendações de correção classificadas por risco e custo.

5.2.5.4 Avaliação da exposição do código-fonte e das regras de negócio para entidades externas apontando os aspectos do código que estariam mais sujeitos a permitir o vazamento de segredos industriais.

5.2.6 Fica proibida a divulgação e utilização do código fonte pela contratante, sendo a PROCEMPA o único dono do código.

5.2.7 Teste manual de vulnerabilidades de aplicações web, avaliação da possibilidade de exploração, comprometimento e/ou vulnerabilidades de até 200 (duzentas) aplicações web definidos pela PROCEMPA.

5.2.8 Cada uma das aplicações web definidas será avaliada duas vezes, teste e re-teste, após a correção dos problemas descobertos.

5.2.9 As aplicações Web serão divididas em ciclos de testagem, conforme definição da PROCEMPA.

5.2.10 Prazos (janelas de tempo para execução dos testes)

5.2.10.1 A CONTRATADA deverá elaborar o “Plano de Teste de Invasão”, para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste, metodologia de análise de vulnerabilidades, equipe envolvida, prazos do teste, de acordo com as informações abaixo:

5.2.10.1.1 O planejamento abrange a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e o cronograma de execução. Deve ser realizado previamente, e em conjunto com a PROCEMPA, sendo obrigatória, a autorização formal da PROCEMPA antes da execução.

5.2.10.1.2 Deve apresentar todo o detalhamento das análises e testes a serem realizados, desde os ativos que serão testados, procedimentos adotados,

técnicas e ferramentas utilizadas, entre outras informações que possam ser relevantes ou solicitadas.

5.2.10.1.3 Deve ser demonstrado e explanado a finalidade de cada ferramenta a ser utilizada, para avaliação e autorização prévia da PROCEMPA.

5.2.10.1.4 Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, o que deve ser considerado na definição do cronograma. Caso a PROCEMPA entenda que haja algum risco neste sentido, solicitará modificação da metodologia e/ou do cronograma, inclusive podendo requerer a execução em finais de semana, feriados ou fora do horário comercial.

5.2.10.1.5 Os testes e avaliações poderão ser interrompidos por solicitação expressa da PROCEMPA a qualquer momento.

5.2.10.1.6 Durante a fase de planejamento, a PROCEMPA definirá qual o tipo de teste a ser aplicado a cada ativo, dentre as seguintes possibilidades: “caixa-preta”, “caixa-cinza” ou “caixa-branca”, segundo a definição “OWASP – Testing Guide”.

5.2.10.1.7 É possível paralelização de atividades, por exemplo: análise de vulnerabilidades internas/externas e teste de vulnerabilidades manuais, desde que atendidas todas as demais condições.

5.2.10.1.8 Deverão ocorrer no mínimo 03 (três) reuniões (presenciais ou remotas) de planejamento na PROCEMPA a cada semestre, sendo possível solicitar mais reuniões para alinhamento de informações adicionais, relativas a esta etapa de planejamento.

5.2.10.1.9 Todas as ferramentas e recursos utilizados para a prestação dos serviços são de responsabilidade da CONTRATADA.

5.2.11 Fornecer visualização da aplicação web através de relatório de ‘mapa do site’.

5.2.12 Fornecer análise detalhada de scripts e páginas estáticas descobertas em servidores web analisados que reflete as strings de conexão de banco de dados, endereços de e-mail, campos de formulário ocultos e outros itens potencialmente sensíveis.

5.2.13 Suportar autenticação para varredura de aplicações web protegidas por credenciais.

5.2.14 Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pela PROCEMPA.

5.2.15 Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pela PROCEMPA.

5.2.15.1 Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada a PROCEMPA, haja vista a necessidade de manter a disponibilidade dos seus ambientes, ativos e serviços.

5.2.16 Descoberta:

5.2.16.1 Deverá ser utilizado, pelo menos, 01 (uma) ferramenta de análise de vulnerabilidade, além de técnicas manuais de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e aprovação em sua utilização, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades.

5.2.17 Ataque

5.2.18 *Análise de vulnerabilidades do ambiente de TI*

5.2.18.1 O serviço deve contemplar a realização semestral de análise de vulnerabilidade em até 254 (duzentos e cinquenta e quatro) endereços IPs externos definidos pela PROCEMPA, visando identificar pontos de falha em suas configurações e versões que possam implicar não atendimento as melhores práticas de segurança estabelecidas pelo mercado, além de identificar possíveis vulnerabilidades presentes em ativos, servidores, aplicações, sistemas, serviços, versões e configurações em produtos atualmente em uso pela PROCEMPA;

5.2.18.2 Os endereços IPs externos a serem testados serão definidos pela PROCEMPA durante a etapa de planejamento. Estes endereços IPs podem não ser todos pertencentes diretamente a PROCEMPA e, não necessariamente farão parte do mesmo bloco de endereços;

5.2.18.3 Neste processo é aceito o uso de ferramentas automatizadas de escaneamento próprias e padrões de mercado.

5.2.18.4 A análise de vulnerabilidade deve considerar as principais vulnerabilidades informadas pelos principais meios de informações até a data de execução da análise, tais como fabricante de softwares, canais de divulgações de vulnerabilidades, além de recomendações aceitas como boas práticas pelo mercado.

5.2.18.5 O método de análise de vulnerabilidades deve contemplar, no mínimo, não se restringindo somente a estes, os seguintes itens:

5.2.18.5.1 Identificação de pontos de entrada;

5.2.18.5.2 Mapeamento todas as portas abertas e serviços;

5.2.18.5.3 Descoberta de ativos, servidores, aplicações, sistemas, serviços e configurações;

5.2.18.5.4 Identificação de versões utilizadas e informar se esta é a versão atualizada;

5.2.18.5.5 Testes de configuração**;**

5.2.18.5.6 Testes de vulnerabilidades;

5.2.18.5.7 Vetores de acesso;

5.2.18.5.8 Vetores de criação;

5.2.18.5.9 Vetores de alteração;

5.2.18.5.10 Vetores de exclusão;

5.2.18.5.11 Vetores de negação de serviço (comprometimento geral/parcial);

5.2.18.5.12 Análise de mensagens de erro;

5.2.18.5.13 Identificação da vulnerabilidade (de acordo com CVE-http://cve.mitre.org/), problema, bug, erro ou item em não conformidade com boas práticas de segurança.

5.2.18.6 O mapeamento deve ser pró-ativo, identificando as ameaças confirmadas e ameaças potenciais, mapeando o grau do risco e classificando conforme padrões de mercado.

5.2.18.7 Todos os endereços IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações foco da análise, devem ser previamente aprovados pela PROCEMPA, que pode eventualmente impedir alguns tipos de análises, bem como solicitar análises específicas, com foco de verificar a segurança de determinado ativo.

5.2.18.8 O resultado da análise deve seguir as seguintes etapas e conter os seguintes itens para análise de vulnerabilidades de infraestrutura:

5.2.18.8.1 Identificação e explicação do endereço IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações encontrados;

5.2.18.8.2 Identificação de vulnerabilidades;

5.2.18.8.3 Metodologia utilizada passo a passo (descrição do teste);

5.2.18.8.4 Resultados obtidos (descrição do resultado);

5.2.18.8.5 Evidência do teste;

5.2.18.8.6 Classificar e priorizar as vulnerabilidades por risco (seguindo o pradrão CVSS - http://www.first.org/cvss);

5.2.18.8.7 Controles mitigatórios aplicáveis;

5.2.18.8.8 Definição da recomendação técnica para solução.

5.2.19 *Teste manual das vulnerabilidades do ambiente de TI externo*

5.2.19.1 O escopo deste serviço prevê a realização semestral de testes manuais de vulnerabilidades de infraestrutura para até 70 (setenta) IPs externos definidos pela PROCEMPA, no intuito de aprofundar o mapeamento realizado na etapa anterior de análise de vulnerabilidades, tentando explorar as vulnerabilidades identificadas no ambiente.

5.2.19.2 Os endereços IPs externos serão os mesmos definidos na etapa anterior "5.2.18 - Análise de vulnerabilidades do ambiente de TI externo";

5.2.19.3 Os testes devem incluir pelo menos as seguintes atividades, não se restringindo somente a estas:

5.2.19.3.1 Leitura/Alteração/exclusão de configurações.

5.2.19.3.2 Fingerprint.

5.2.19.3.3 Descoberta da senha de acesso do ativo.

5.2.19.3.4 Escalonamento(salto) de acessos, até o ponto máximo possível.

5.2.19.4 Os testes devem ser feitos nas seguintes camadas:

5.2.19.4.1 Aplicação;

5.2.19.4.2 Apresentação;

5.2.19.4.3 Sessão;

5.2.19.4.4 Transporte;

5.2.19.4.5 Rede.

5.2.19.5 Os testes devem avaliar a possibilidade de exploração, comprometimento e/ou vulnerabilidades de:

5.2.19.5.1 Servidores (diversas plataformas);

5.2.19.5.2 Serviços (web, ftp, telnet, e-mail, dns, outros..);

5.2.19.5.3 Ativos de rede (Firewall, IPS, Switches, Roteadores, Soluções de Balanceamentos, outros..).

5.2.19.6 Nos testes deve ser utilizado a última metodologia disponível OSSTMM, item "Testes de Segurança em Rede de Dados (Capítulo 11 - Data Networks Security Testing)".

5.2.19.7 Deve ser imediatamente comunicado a PROCEMPA cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.

5.2.20 *Teste manual de vulnerabilidades de aplicações web*

5.2.20.1 O escopo deste serviço prevê a realização de testes manuais de vulnerabilidades de até 50 (cinquenta) aplicações web por ciclo, definidos pela PROCEMPA;

5.2.20.2 Cada uma das aplicações web definidas será avaliada apenas uma vez a cada ciclo, sendo que a distribuição das avaliações poderá ser semestral ou mensal, conforme critério da PROCEMPA. Caso não sejam analisadas as aplicações web previstas para o 1º (primeiro) ciclo, por solicitação da PROCEMPA, as análises das aplicações não realizadas neste ciclo poderão ser executadas durante o 2º (segundo) ciclo, desde que previamente acordado com a LICITANTE VENCEDORA;

5.2.20.3 Os testes devem englobar baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):

5.2.20.3.1 Aplicações acessadas via internet ou Intranet;

5.2.20.3.2 Portais web disponíveis;

5.2.20.3.3 Serviços web diversos detectados;

5.2.20.3.4 Webservices;

5.2.20.3.5 Sockets.

5.2.20.4 A critério da PROCEMPA, será definido qual escopo de usuários utilizado em cada teste, podendo ser definidos um ou mais destes critérios para uma mesma aplicação:

5.2.20.4.1 Sem credenciais;

5.2.20.4.2 Credenciais comuns;

5.2.20.4.3 Credenciais de administrador.

5.2.20.5 Os testes devem contemplar todas as páginas, telas e transações disponíveis na aplicação, incluindo páginas/telas disponíveis para usuários sem credencias, com credencias, páginas/telas de administração, bem como demais existentes.

5.2.20.6 Os testes manuais em aplicações devem contemplar as seguintes fases e itens em seu planejamento e execução, não se limitando somente a estes:

5.2.20.6.1 Coleta de Informações;

5.2.20.6.2 Teste de lógica de negócios;

5.2.20.6.3 Teste de autenticação;

5.2.20.6.4 Gerenciamento de Sessões;

5.2.20.6.5 Testes de validação de Dados;

5.2.20.6.6 Teste de Web Services;

5.2.20.6.7 Negação de Serviço.

5.2.20.7 Deve incluir os testes listados e descritos nas duas últimas versões do TOPTEN disponibilizadas pela OWASP;

5.2.20.8 E demais a ser informada na reunião prévia entre a CONTRATADA e a PROCEMPA.

5.2.20.9 Deve ser imediatamente comunicado a PROCEMPA cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.

5.2.20.11 Avaliação funcional de segurança com análise de código e segurança em software que consiste em avaliação automatizada seguida por inspeção manual por amostragem. Essa forma é a mais custo eficiente para identificação de problemas no código.

5.2.20.12 A Avaliação funcional de segurança com análise de código e segurança em software totalmente automatizada tende a apresentar grande número de falsos positivos e ainda pode deixar de identificar algumas vulnerabilidades.

5.2.20.13 A Avaliação funcional de segurança com análise de código e segurança em software totalmente manual implica um esforço e prazos muito longos que, tipicamente, não apontam nenhuma vulnerabilidade adicional ao processo misto. A inspeção de código é realizada em duas etapas.

5.2.20.14 Numa primeira verificação, o analista executará um sistema de inspeção automatizada de código fonte sobre este código. O sistema de Avaliação funcional de segurança com análise de código e segurança em software destacará trechos do código que considerar sensíveis. A atividade de inspeção de código tem por objetivo:

5.2.20.14.1 Indicar código malicioso inserido pelo desenvolvedor;

5.2.20.14.2 Apontar código inseguro e sugerir melhorias;

5.2.20.14.3 Identificar vulnerabilidades latentes;

5.2.20.14.4 Apontar uso de funções do sistema operacional com problemas conhecidos de segurança;

5.2.20.14.5 Indicar implementações de controles de segurança fora dos padrões e normas.

5.2.20.15 Deve-se notar que a Avaliação funcional de segurança com análise de código e segurança em software de código é muito mais eficiente para detectar os ataques de falha de configuração de segurança, falha de controle de acesso e, principalmente, falhas ou backdoors introduzidos propositalmente pelo desenvolvedor. Este último caso, particularmente, só é identificado com inspeção de código.

5.2.20.16 Cada ponto fraco identificado é apontado com o código correspondente, descrição do problema e forma de solução.

5.2.20.17 Deve ser feita uma análise detalhada e manual do código-fonte do aplicativo. Muitas das vulnerabilidades detectadas em uma análise de código-fonte são semelhantes às vulnerabilidades detectadas durante um Teste de penetração de aplicativo.

5.2.20.18 Ao contrário de um teste de penetração, uma análise de código permite uma maior amplitude de cobertura e um aumento no nível de confiança nos resultados da avaliação. Este é principalmente o resultado de ter uma

compreensão mais completa do design, da arquitetura de software e de seus componentes internos, o que permite que vulnerabilidades identificadas tenham sua exploração totalmente avaliada a partir de uma perspectiva de risco.

5.2.20.19 Algumas vulnerabilidades ou falhas de design também são mais fáceis de detectar em uma análise de código, tal como uma funcionalidade "oculta" em um aplicativo ou deficiências em controles de auditoria.

5.2.20.20 Deve-se personalizar o plano de teste para adequar a tecnologia usada pelo aplicativo.

5.2.21 *Relatório de Teste de Invasão*:

5.2.21.1 A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidades vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências apuradas; fontes de pesquisa, pontos positivos encontrados, referências e ferramentas utilizadas.

5.2.21.2 Os relatórios deverão ser validados junto a PROCEMPA, onde poderão ser solicitadas tantas alterações e correções quantas forem necessárias, até que se chegue a uma versão final aceita por ambas as partes.

5.2.21.3 Não serão aceitos relatórios obtidos diretamente por ferramentas automatizadas utilizadas para a realização dos testes, sem a devida transcrição e contextualização adequada, bem como atendimento de todos os requisitos do edital.

5.2.21.4 Os relatórios devem ser entregues na língua portuguesa com atendimento aos requisitos do edital.

5.2.21.5 Deve ser comunicado a PROCEMPA, e devidamente documentado, o andamento da análise/teste, especialmente se identificada uma situação crítica.

5.2.21.6 As entregas devem ser realizadas por meio físico e/ou digital a ser definido pela PROCEMPA. Se digital disponibilizar: 1 arquivo .doc não protegido contra gravação e 1 arquivo pdf assinado digitalmente com certificado digital ICP Brasil; e protegido por criptografia que deverá conter no mínimo código hash de cada documento, a fim de garantir integridade destas entregas. A versão digital dos documentos deverá ser assinada digitalmente com certificado digital ICP Brasil.

5.2.21.7 Ao final do projeto, deve ser realizada uma apresentação detalhada, nas dependências da PROCEMPA, com local a ser definido posteriormente, das documentações e conclusões.

5.2.21.8 Para auxiliar na solução para correção das vulnerabilidades identificadas, o relatório deve indicar a PROCEMPA mais de uma opção de correção para cada item de vulnerabilidade identificado. Estas opções devem ser validadas com a PROCEMPA durante a redação dos relatórios, de forma que considerem as peculiaridades do seu ambiente, até o aceite final do mesmo.

5.2.21.9 A CONTRATADA deve fornecer a PROCEMPA todas informações necessárias para correção da vulnerabilidade, clarificando eventuais dúvidas durante a vigência de todo o contrato.

5.2.22 Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste:

5.2.22.1 Deverão ser entregues 04 (quatro) tipos de relatórios:

5.2.22.1.1 Relatório Técnico de Análise de Vulnerabilidade: O relatório semestral deve ser entregue ao final de cada ciclo contendo uma visão completa de todas as vulnerabilidades encontradas nos 70 IP´s, com a explicação da vulnerabilidade, evidência e procedimento de teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades, conforme requisitos deste documento.

5.2.22.1.2 Relatório Técnico de Teste manual das vulnerabilidades do ambiente de TI (interno e externo): O relatório semestral deve ser entregue ao final de cada ciclo contendo todos os procedimentos efetuados e todos os resultados da etapa do teste de vulnerabilidades manual de infraestrutura nos 70 IP´s, com a identificação do problema de segurança, explicação do procedimento detalhado, evidência do teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas no processo de teste de vulnerabilidades manual. Este deve descrever o passo-a-passo de como a vulnerabilidade/falha pode ser explorada, para efeito de validação da solução aplicada por parte da PROCEMPA, e atender itens conforme requisitos deste documento.

5.2.22.1.3 Relatório Técnico de Teste manual de vulnerabilidades de aplicações web (se houver distinção): O relatório mensal ou semestral, conforme estipulado a critério da PROCEMPA na etapa de planejamento, deve ser entregue ao final de cada mês ou ao final de cada ciclo, contendo todos os procedimentos efetuados e todos os resultados da etapa do teste de vulnerabilidades manual de aplicações Web. Deve conter a identificação dos problemas de

segurança, explicação do procedimento detalhado, evidência do teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas no processo de teste de vulnerabilidades manual. Este deve descrever o passo-a-passo de como a vulnerabilidade ou falha pode ser explorada, para efeito de validação da solução aplicada por parte da PROCEMPA, e atender itens conforme requisitos deste documento.

5.2.22.1.4 Relatório Executivo Final, com considerações e recomendações: O relatório anual, a ser entregue ao final do segundo ciclo, deverá conter um histórico com a evolução da situação real do ambiente diante das análises e testes aplicados, bem como processo de mitigação e verificações feitas que elenquem as conclusões do trabalho, recomendações referentes às vulnerabilidades identificadas e exploradas resolvidas e não resolvidas, conforme requisitos deste documento.

5.2.23 Sugestão para perfis seguros de estações

5.2.24 Deverão constar como anexos as filmagens dos ataques bem-sucedidos (ex. com a utilização de softwares como o Camtasia)

5.2.25 Reavaliação, novo teste completo após remediação, verificando se não foram abertas novas vulnerabilidades com a remediação.

5.2.25.1 A contratada fará novos testes do mesmo tipo em até 60 dias após a correção das vulnerabilidades apontadas no respectivo relatório por parte da PROCEMPA.

5.2.25.2 A contratada não obterá nenhuma informação e acesso sobre serviços e Sistemas da PROCEMPA, devendo por seu próprio esforço obter informações necessárias para análises e testes, quando acordado com PROCEMPA no planejamento.

5.2.26 Os alvos dos testes a serem efetuados, assim como suas condições serão definidos em reunião prévia entre a CONTRATADA e a PROCEMPA.

5.2.27 As atividades utilizadas para a execução dos testes não se resumirão apenas ao uso de ferramentas, devendo incluir também procedimentos e técnicas com interação humana e não oferecidos por ferramentas conhecidas.

5.2.28 Decorridos 5 (cinco) dias do início efetivo dos testes, a contratada poderá solicitar informações e acessos necessários a PROCEMPA para obter acesso aos sistemas web como usuário básico com o objetivo de simular possibilidades de escalonamento de privilégios e acessos indevidos a outros níveis/sistemas.

5.2.29 Execução das análises de projeto, inspeções de código e testes de invasão com todas as características disponíveis.

5.2.30 Utilização de ferramenta como uma aplicação local (mantém todos os dados localmente no seu próprio computador).

5.2.31 Utilização de ferramenta Web, instalada na PROCEMPA, para rodar uma análise rápida, sem instalar o software.

5.2.32 Para a obtenção das informações poderão ser utilizadas técnicas de Engenharia Social e PhishingScam.

5.2.33 Restrições e Limites

5.2.33.1 As janelas de tempo para a execução dos testes serão acordadas entre CONTRATADA e PROCEMPA, priorizando sempre os períodos/horários de menor pico de forma a não impactar no negócio.

Restrição	Exemplo	Razão da Restrição
Tempo de restrição	Teste de intrusão só poderá ser feito durante final de semana ou dia não útil	Reduzir risco de causar impacto durante horas de trabalho normal para assegurar que as atividades do teste sejam controladas e monitoradas devidamente.
Tipo de teste	Não executar teste de engenharia social	Focar na análise dos resultados técnicos somente
	Não execute ataque de força bruta em sistema com autenticação	Evitar problemas de bloqueio de credenciais advindo do ataque de força bruta.

IPs e aplicações	Não executar teste em IP's não especificados no escopo Teste não deve envolver determinado componente de sistema X	Evitar ambiente compartilhado Evitar impacto no negócio com corrupção/interrupção de determinado sistema

5.2.33.2 Tipo de teste a ser feito

5.2.33.3 Redes e aplicações incluídas ou excluídas do escopo

5.2.33.4 Pessoas afetadas

5.2.33.5 Dado autorizado a ser acessado.

5.2.33.6 Escopo de teste autorizado pelo PROCEMPA para realização do teste acordado, assinado pelo gestor do contrato. Documento deve conter as tecnologias dos componentes e infraestrutura física, incluindo serviço na nuvem se for o caso.

5.2.33.7 Cada fase deve ser feita durante o período que não comprometa processamento da PROCEMPA e que as agências estejam fechadas sendo feita em no máximo 2 dias corridos no total.

6. Níveis Mínimos de Serviço/ Indicadores de Desempenho Esperados Para os Itens 1 e 2.

6.1 A ferramenta de análise de vulnerabilidade comercial deverá contemplar, ao menos, as seguintes características que serão comprovadas através de relatórios:

6.1.1 Prover identificação e correlação de ameaças, além de avaliar o potencial risco das vulnerabilidades encontradas;

6.1.2 Fornecer evidências de ativos "não vulneráveis" através de provas conclusivas como:

6.1.2.1.1 Resultados de varreduras esperados e obtidos;

6.1.2.1.2 Lista de ativos não analisados;

6.1.2.1.3 Falhas nas varreduras.

6.1.3 A solução de análise de vulnerabilidades não deve ser baseada na necessidade de instalação prévia de agentes no ambiente corporativo pela PROCEMPA.

6.1.4 Resultados de varredura enviados para o banco de dados através da rede corporativa devem ser criptografados.

6.1.5 Fornecer cobertura de conteúdo para executar verificações com autenticação e sem autenticação.

6.1.6 Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando as credenciais para se autenticar em sistemas Windows, UNIX ou qualquer ativo de infraestrutura, tais como dispositivos de rede, etc;

6.1.7 Permitir o acesso seguro ao back-end do banco de dados de modo a permitir a mineração de dados para possíveis relatórios personalizados que sejam solicitados;

6.1.8 Deve ter certificado pelo EAL Common Criteria e validar criptografia FIPS-140-2.

6.1.9 Suportar métricas de pontuação baseadas em risco;

6.1.10 O processo de varredura deve ter um impacto mínimo sobre a rede, não superior a 10 Mbps de tráfego (podendo ser revisto após discussão e aprovação da PROCEMPA);

6.1.11 Permitir o ajuste de desempenho para adequar a quantidade de banda consumida na rede durante a varredura de análise de vulnerabilidade, tanto para a realização de varreduras mais rápidas que consomem mais recursos;

6.1.12 A descrição de vulnerabilidade deve possuir no mínimo os seguintes detalhes:

6.1.12.1 Nome;

6.1.12.2 Nível de Risco;

6.1.12.3 Intrusiva (sim/não)

6.1.12.4 Descrição;

6.1.12.5 Observação;

6.1.12.6 Recomendação de remediação;

6.1.12.7 Link do patch ou da correção;

6.1.12.8 Número CVE;

6.1.12.9 SANS / FBI referência Top 20;

6.1.12.9.1 IAVA(Information Assurance Vulnerability Alert) Referência

6.1.12.10 Realizar análise de vulnerabilidades Segundo as seguintes tecnologias:

6.1.12.10.1 XCCDF

6.1.12.10.2 OVAL

6.1.12.10.3 CVSS

6.1.12.10.4 CVE

6.1.12.10.5 CPE

6.1.12.10.6 CCE

6.1.13. Em caso de problemas durante a execução dos testes de penetração/ vulnerabilidade a PROCEMPA acionará a Contratada para manutenções corretivas. Ao acionar a CONTRATADA, a PROCEMPA classificará o problema em um dos níveis de criticidade da tabela a seguir. A PROCEMPA dará efetivo apoio e envolvimento de seus técnicos para a solução dos problemas. Cada nível de severidade possui diferentes níveis mínimos de serviço, conforme descrito também nas tabelas a seguir:

CLASSIFICAÇÃO DE EVENTOS	
(A) EMERGENCIAL	São consideradas como “Emergência” todas as falhas cujas consequências tenham impactos sobre o serviço, rede, tráfego de dados e sincronismo e/ou recursos de manutenção que exigem ação corretiva imediata (independente da hora do dia ou do dia da semana).
(B) ALTA PRIORIDADE	Situações que podem configurar uma severidade emergencial. São situações potenciais e exigem atenção imediata. São situações potenciais que precedem, em sua maioria, uma situação que pode ser classificada num segundo momento como severidade emergencial.
(C) MÉDIA PRIORIDADE	Problemas que não prejudicam significativamente o funcionamento dos sistemas / serviços. São problemas graves ou perturbações que afetam uma área específica de determinada funcionalidade. Exemplos: degradação de desempenho, perda de funcionalidades.

(D) BAIXA PRIORIDADE E CONSULTA	Consulta geral e problemas secundários que têm um efeito pequeno na funcionalidade do produto. Ex.: Falhas de documentação, falhas no projeto e questionamentos operacionais.

NÍVEL	SEVERIDADE	TEMPO PARA RESTABELECIMENTO DO SISTEMA APÓS ABERTURA DO CHAMADO	TEMPO PARA SOLUÇÃO DEFINITIVA DO PROBLEMA
A	EMERGENCIAL	até 1 hora	até 4 dias corridos
B	ALTA PRIORIDADE	até 2 horas	até 7 dias corridos
C	MEDIA PRIORIDADE	até 4 horas	até 10 dias corridos
D	BAIXA PRIORIDADE E CONSULTA	Até 24horas	até 15 dias corridos

7 Das Definições do Acordo de Nível de Serviços (SLA).

7.1 A CONTRATADA deverá cumprir rigorosamente os prazos estabelecidos pela PROCEMPA, referente à prestação dos serviços conforme Item 6.1.13, no caso de extrapolação dos prazos definidos será aplicado um redutor sobre o valor da fatura mensal do contrato, referente a cada nível de severidade, conforme tabela abaixo:

7.2 O redutor será aplicado por hora corrida extrapolada em relação ao Tempo para Restabelecimento do Sistema Após Abertura do Chamado.

NÍVEL DE SEVERIDADE	REDUTOR	REFERÊNCIA
A	0,5%	Fatura Global
B	0,4%	Fatura Global
C	0,2%	Fatura Global
D	0,1%	Fatura Global

7.3 O Total de descontos não poderá extrapolar 20% da fatura global.

7.4 A CONTRATADA deverá cumprir os níveis de serviço que estão expostos na seção de sanções.

7.5 Os descontos serão efetuados quando da emissão da fatura do respectivo pedido.

7.6 A PROCEMPA comunicará formalmente a CONTRATADA, via email, o percentual de SLA a ser aplicado.

7.7 Os atrasos de qualquer natureza deverão ser justificados formalmente a PROCEMPA.

7.8 Os Acordos de Níveis de Serviços – SLA poderão ser aplicados cumulativamente.

8 Dos Requisitos de Habilitação

8.1.1 A empresa licitante deverá apresentar pelo menos dois atestados de capacidade técnico-operacional (ANEXO I.II) emitido por pessoa jurídica de direito público ou privado, onde são ou foram prestados pelo menos os seguintes serviços: Testes de Invasão poderá ser do tipo Externos e/ou Internos nos sistemas (web e legados), processos e ativos de infraestrutura tecnológica (rede cabeada e wifi) nos 24 meses anteriores a licitação deste edital com comprovação. Estas obrigações dar-se-ão devido à sensibilidade das informações da instituição que serão expostas nos testes, sendo assim é necessário termos empresas qualificadas para a execução do objeto deste Termo de Referência.

8.1.2 O(s) atestado(s)/certidão(ões)/declaração(ões) deverá(ão) ser apresentado(s) em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato e deve(m) indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

8.1.3 Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da CONTRATADA.

8.1.4 O atestado de capacidade técnica apresentado poderá ser objeto de diligência a critério da PROCEMPA, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela CONTRATADA e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a LICITANTE, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

8.1.5 Certidão Negativa de Licitante Inidôneo do Tribunal de Contas do Estado do Rio Grande do Sul e do Tribunal de Contas da União.

8.2 PERFIS PROFISSIOGRÁFICOS PARA OS ITENS 1 E 2

8.2.1 A seguir estão relacionadas exigências de perfis dos profissionais que executarão os serviços dos itens 1 e 2 do objeto dessa contratação. A comprovação se dará através da apresentação tempestiva de currículos detalhados, diplomas, e documentação das certificações (dentro do período de validade), exigidas na data da assinatura do contrato.

8.2.2 A PROCEMPA se reserva o direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

8.2.3 A CONTRATADA deve retirar dos serviços qualquer empregado que, a critério da PROCEMPA, seja julgado inconveniente ao bom andamento dos trabalhos;

8.2.4 Comprovação de possuir no seu quadro permanente, no ato da contratação, no mínimo, em conjunto de profissionais com os certificados abaixo:

8.2.6 Responsável Técnico e sua Equipe

ITEM	DESCRIÇÃO
PERFIL E EXPERIÊNCIA PROFISSIONAL	
Análise de Vulnerabilidades	Deverá ter experiência de, no mínimo, 03 (três) anos em execução de teste de intrusão, devido a rápida evolução tecnológica em relação as execuções de testes.

8.2.7 No momento da assinatura do contrato a CONTRATADA deverá apresentar a lista de profissionais, com suas devidas certificações, que poderão atuar nos testes.

8.2.8 A prestação do Serviço de Teste de Invasão em Redes e Sistemas deverá ser realizada por equipe de profissionais que possua, pelo menos 3 (três) das seguintes certificações, pois para o objeto é necessário que o profissional possua certificações para executar com a melhor técnica os testes de intrusão devido a rápida evolução tecnológica:

Especificação Técnica

TR Teste de Intrusão PENTEST

Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

Item	Certificação
1	EC-COUNCIL - CNDA
2	CPTE - CERTIFIED Penetration Testing Engineer - Mile2
3	Certified Information Systems Security Professional (CISSP)
4	EC-Council Certified Ethical Hacker (CEH)
5	EC-Council Licensed Penetration Tester (LPT) Master
6	CompTIA Cybersecurity Analyst (CySA+)
7	CompTIA Security+
8	CompTIA Security Analytics Professional (CSAP)
10	IACRB Certified Penetration Tester (CPT)
11	CompTIA Security+ (SYO-401)
14	Certified Expert Penetration Tester (CEPT)
15	Certified Mobile and Web Application Penetration Tester (CMWAPT)
17	Certified Red Team Operations Professional (CRTOP)
18	CompTIA PenTest +
19	Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
20	Global Information Assurance Certification (GIAC) Web Application Penetration Tester (GWAPT)
21	Global Information Assurance Certification (GIAC) Certified Intrusion Analyst (GCIA)
22	Global Information Assurance Certification (GIAC) Exploit Researcher and Advanced Penetration Tester (GXPN)
23	Offensice Security Certified Professional (OSCP)
24	EC Council Security Analyst (ECSA)

25	Certified Mobile and Web Application Penetration Tester (CMWAPT)
26	Certified Secure Software Lifecycle Professional (CSSLP)

8.2.9 A CONTRATADA deverá apresentar também, na assinatura do contrato, a lista dos profissionais com seus currículos e a comprovação da exigência de certificação acima, suas responsabilidades em cada etapa (testes externos, testes internos, análise de aplicações web), quais atuarão on site (na PROCEMPA) e quais atuarão remotamente e, por fim, a comprovação de seu vínculo empregatício com a CONTRATADA.

8.3 Dos Documentos Comprobatórios aos Critérios de Sustentabilidade

8.3.1 A contratada se compromete, sob pena de infração e rescisão contratual, a:

8.3.2 Não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

8.3.3. Não empregar menores de 18 anos para trabalho noturno, perigoso ou insalubre, e menores de dezesseis anos para qualquer trabalho, com exceção a categoria de Menor Aprendiz;

8.3.4 Não permitir a prática ou a manutenção de discriminação limitativa ao acesso na relação de emprego, ou negativa com relação a sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar ou estado gravídico, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

8.3.5 Respeitar o direito de formar ou se associar a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias;

8.3.6 Buscar a incorporação em sua gestão dos Princípios do Pacto Global, disponível em http:http://www.pactoglobal.org.br/artigo/56/Os-10-principios, bem como o alinhamento com as diretrizes da Política de Responsabilidade Socioambiental da PROCEMPA

8.3.7 Proteger e preservar o meio ambiente, bem como buscar prevenir e erradicar práticas que lhe sejam danosas, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos às áreas de meio ambiente, emanadas das esferas federal, estaduais e municipais e implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

8.3.8. Desenvolver suas atividades respeitando a legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como os demais dispositivos legais relacionados proteção dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se:
"Condições ultrajantes": condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo;
"Condições sub-humanas": tudo que está abaixo da condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano. Situação abaixo da linha da pobreza;
"Condições degradantes de trabalho": condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão.

8.3.9 A PROCEMPA poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o Contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia defesa, caso se comprove que a CONTRATADA, subcontratados ou fornecedores utilizem-se de trabalho em desconformidade com as condições referidas nas cláusulas supracitadas.

8.3.10 Plano de Gerenciamento de Resíduos Sólidos ou Declaração de Sustentabilidade Ambiental;

8.3.11 Certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências do edital.

8.5 Da Visita Técnica

Não haverá necessidade de Visita Técnica visto o objeto deste Termo de Referência.

9 Da Adjudicação do Objeto

Menor preço global

10 Das Condições de Contratação para o item 1 e 2

10.1 A empresa licitante deverá demonstrar qualificação técnica necessária à prestação dos serviços apresentando material que comprove a posse de portfólio de serviços de segurança da informação sendo uma condição de contratação.

10.2 A empresa deve apresentar currículo assinado pelo próprio profissional de, pelo menos, um dos profissionais que participarão dos testes de intrusão, que contemple experiência com ao menos duas das seguintes metodologias/frameworks/boas práticas:

10.2.1 OSSTMM 3 (The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined);

10.2.2 ISSAF/PTF (Information Systems Security Asssessment Framework);

10.2.3 NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);

10.2.4 NIST Special Publication 800-42 (Guideline on Network Security Testing)

10.2.5 OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.

10.2.6 PCI DSS (Payment Card Industry Data Security Standard)

10.2.7 PCI SSC Information Supllement

10.2.8 PTES (Penetration Testinf Execution Standard)

10.2.9 As experiências apresentadas no item anterior garantem que a empresa vencedora executará com excelência o objeto do certame, uma vez que são certificações voltadas para os Testes de Intrusão, reconhecidas nacional e internacionalmente.

12 Características e Condições da Execução do Contrato

12.2.1 O prazo de vigência do contrato será de 12 (doze) meses, contados da assinatura do mesmo, podendo ser prorrogado a critério da PROCEMPA, conforme legislação vigente.

12.3 Da Entrega

12.3.1 A empresa contratada deverá entregar à equipe da DPO – Data Protection Officer todo detalhamento dos testes de invasão a serem realizados, desde os ativos que foram testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.

12.3.4 Os serviços serão solicitados sob demanda por meio de ordem de serviço a ser emitida pela PROCEMPA;

12.3.5 Os serviços deverão ser prestados de forma local ou remota;

12.3.6 A PROCEMPA solicitará o serviço a ser executado, sempre que achar necessário, mediante a validação de escopo entre as partes;

12.3.7 O escopo dos serviços deverá ser acordado entre a PROCEMPA e a CONTRATADA por meio de reuniões para definição do escopo, de estimativa de esforço, cronograma e prazo para o início da execução da ordem de serviço

12.3.8 A execução será sempre precedida de emissão de Ordem de Serviço (OS), contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados, técnicos que atuarão no projeto;

12.3.8.1 Não serão aceitos técnicos que não tenham as certificações exigidas neste edital;

12.3.8.2 Uma Ordem de Serviço (OS) somente será autorizada após conferência e ateste do Gestor do Contrato;

12.3.8.3 Toda OS deverá ser assinada pelo Preposto da Empresa Contratada perante a PROCEMPA, declarando a concordância da Contratada em executar as atividades descritas na OS de acordo com as especificações estabelecidas;

12.3.8.4 Os serviços deverão estar sempre de acordo com as especificações constantes nas OS;

12.3.8.5 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução - quando a OS é emitida, durante a execução - com o acompanhamento e supervisão de responsáveis da PROCEMPA, e ao término da execução - com o fornecimento dos respectivos relatórios pela CONTRATADA e atesto dos mesmos pelos respectivos responsáveis;

12.3.8.6 Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues a PROCEMPA em forma digital complementarmente aos relatórios dos serviços;

12.3.9 Uma vez definido escopo, prazo e cronograma, o início da execução dos serviços deverá ocorrer na data e prazo previstos.

12.3.10 Caso o trabalho ultrapasse a quantidade de horas estimadas, a PROCEMPA deverá ser informado imediatamente que deliberará sob a nova quantidade estimada.

12.3.11 O aceite e o posterior pagamento dos serviços não eximem a Licitante vencedora das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades causadas por estes.

12.3.12 Será designado representante para acompanhar e fiscalizar a realização dos serviços, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

12.3.13 As decisões e providências que ultrapassarem a competência do representante deverão ser solicitadas ao seu gestor, em tempo hábil para adoção das medidas convenientes.

12.3.14 O representante da PROCEMPA anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

12.3.15 A PROCEMPA, poderá rejeitar, no todo ou em parte, se em desacordo com o Termo de Referência.

12.3.16 Quaisquer exigências da Fiscalização, inerentes ao Objeto da presente contratação, deverão ser prontamente atendidas pela CONTRATADA.

12.4 Do Recebimento do Objeto

12.4.1 Concluída a realização dos serviços solicitados através da OS, a CONTRATADA deverá comunicar este fato formalmente a PROCEMPA. A PROCEMPA emitirá o documento de aceite da Ordem de Serviços que deverá conter as informações relacionadas a execução e ser assinado por responsáveis da CONTRATADA e pelo Gestor Técnico da PROCEMPA.

12.5 Obrigações da Contratada

12.5.1 Adicionalmente às responsabilidades estabelecidas nos demais tópicos constantes deste documento, incumbe à contratada observar os seguintes requisitos:

12.5.2 Cumprir os prazos e obrigações estabelecidas no Edital.

12.5.3 Prestar os serviços no prazo, quantidade e especificações solicitadas conforme as características descritas na sua proposta e no edital.

12.5.4 Observar as normas e procedimentos internos da PROCEMPA no que se refere à segurança (Política de Segurança da Informação e seus Manuais de Normas e Procedimentos) e sigilo dos dados manuseados, bem como no que é pertinente à documentação (Termo de Confidencialidade, Acordo de Confidencialidade da Informação e Responsabilidade – ANEXO I.IV e Acordo de Proteção de Dados Pessoais – ANEXO I.VIII, sobre os quais se obriga a dar ciência a seus funcionários, que tiverem acesso às dependências da PROCEMPA, e aos que possuírem acesso remoto);

12.5.5 Alocar profissionais necessários à realização dos serviços, de acordo com a experiência profissional e qualificação técnica exigida, apresentando a documentação que comprove a qualificação.

12.5.6 Dar conhecimento a todos os profissionais que venham a prestar serviços relacionados ao objeto contratado, os processos de trabalho, políticas e normas internas da PROCEMPA, bem como zelar pela observância de tais instrumentos.

12.5.7 Informar imediatamente a PROCEMPA a ocorrência de transferência, remanejamento, promoção ou demissão de profissional sob sua responsabilidade, para providências de revisão, modificação ou revogação de privilégios de acesso a sistemas, informações e recursos da PROCEMPA.

12.5.8 Prestar os serviços no prazo, quantidade e especificações solicitadas conforme as características descritas na sua proposta e no edital;

12.5.9 Colocar, nos prazos contratados, os profissionais à disposição da PROCEMPA para execução dos serviços;

12.5.10 Responsabilizar–se pelos encargos fiscais e comerciais resultantes desta contratação e ainda pelos encargos trabalhistas, previdenciários, securitários, tributos e contribuições sociais em vigor, obrigando-se a saldá-los nas épocas próprias, haja vista que os empregados da CONTRATADA não manterão qualquer vínculo empregatício com a PROCEMPA;

12.5.11 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

12.5.12 Responsabilizar-se pelos danos causados direta ou indiretamente ao PROCEMPA ou a terceiros, decorrentes de sua culpa ou dolo quando do fornecimento dos produtos contratados, não excluindo ou reduzindo essa responsabilidade em caso de fiscalização e/ou acompanhamento pela PROCEMPA;

12.5.13. Manter garantia contra defeitos de hardware e software, inclusive atualização de versões dos programas utilizados para objeto deste Edital;

12.6 Obrigações da PROCEMPA

12.6.1 Fiscalizar o fornecimento do objeto deste Edital, podendo sustar, recusar, mandar fazer ou desfazer qualquer fornecimento dos produtos/serviços que não estejam de acordo com as normas, especificações e técnicas usuais;

12.6.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA sobre os produtos objeto desta licitação;

12.6.3 Acompanhar e atestar nas Notas-Fiscais/Faturas a efetiva entrega do produto/serviço do objeto deste Edital;

12.6.4 Aplicar à CONTRATADA as penalidades regulamentares e contratuais, previstas em lei e neste Edital;

12.6.5 Comunicar à CONTRATADA, quaisquer irregularidades observadas no objeto deste Edital.

12.6.6 Verificar a regularidade da situação fiscal da CONTRATADA, antes de efetuar o pagamento devido.

12.6.7 Proceder às advertências, descontos e demais cominações legais pelo descumprimento das obrigações assumidas pela CONTRATADA.

12.6.8 Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado, pelas demais empresas fornecedoras, de forma a garantir que continuem a serem os mais vantajosos para a Administração.

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.I
MODELO DE PROPOSTA
CARTA DE APRESENTAÇÃO DE PROPOSTA

À PROCEMPA

Ref: Edital de Licitação nº ...../.....
Objeto:.....
Prezados senhores,

A ....., inscrita no CNPJ sob o nº ....., sediada .....(endereço completo)....., com o telefone para contato nº (.....).....-..... e e-mail ....., por intermédio do seu representante legal o(a) Sr.(a) ....., ...(cargo)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº ....., residente e domiciliado(a) no .....(endereço completo)....., tendo examinado as condições do edital e dos anexos que o integram, apresenta a proposta comercial relativa à licitação em epígrafe, assumindo inteira responsabilidade por quaisquer erros ou omissões que tiverem sido cometidos quando da preparação da mesma:

Propõe-se o Valor Total para o Lote de R$ .....(.....), conforme quadro abaixo:

	ITEM	DESCRIÇÃO	QTD	UND	VALOR UNITÁRIO	VALOR TOTAL
LOTE ÚNICO	1	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 (**Wireless**) e **Rede** de Área Local (**LAN**) do tipo Externos e/ou Internos.	600	Hora		
	2	Serviço de Teste de invasão em sistemas no padrão Red Team, Blackbox, GreyBox e WhiteBox.	3.540	Hora		
	VALOR TOTAL DO LOTE (R$)					

No valor total proposto estão englobados todos os custos e despesas previstos no edital nº ...../....., tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucros e outros necessários ao cumprimento integral do objeto.

Junta-se detalhamento da proposta acima.

Que, em relação às prerrogativas da Lei Complementar nº 123/2016, o proponente:
( ) Enquadra-se como microempresa, empresa de pequeno porte ou equivalente legal, nos termos previsto no Decreto nº 8.538/2015, conforme certidão expedida pela Junta Comercial ou Cartório de Registro em anexo. Ainda, que:
( ) É optante do Simples Nacional, submetendo-se à alíquota de .....%, apurada com base no faturamento acumulado dos últimos 12 (doze) meses.
( ) Não é optante do Simples Nacional.

Essa proposta é válida por 120 (cento e vinte) dias, contados da data prevista para abertura da sessão.

Até que o contrato seja assinado ou recebida a Nota de Empenho conforme o caso, esta proposta constituirá um compromisso da ....., observadas as condições do edital. Caso esta proposta não venha a ser aceita para contratação, a PROCEMPA fica desobrigado de qualquer responsabilidade referente a presente proposta.

Os pagamentos serão efetuados em conformidade com as condições estabelecidas no Termo de Referência e Nota de Empenho.
Devem ser utilizados, para quaisquer pagamentos, os dados bancários a seguir:

BANCO: .....
AGÊNCIA: .....
CONTA CORRENTE: .....
PRAÇA DE PAGAMENTO: .....

Por fim, declara conhecer e aceitar as condições constantes do edital nº ...../..... e de seus anexos.

.....
(Local e Data)
(Representante legal)

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I. II
ATESTADO DE CAPACIDADE TÉCNICA

(Modelo)

Atestamos para os devidos fins que a empresa **[Razão Social da Empresa licitante]**, inscrita no CNPJ sob o Nº. **[da Empresa Licitante]**, estabelecida na **[endereço da Empresa Licitante]**, prestou ou presta serviços para esta empresa/Entidade **[Razão Social da Empresa Emitente do atestado]**, inscrita no CNPJ sob o Nº. **[CNPJ da Empresa Emitente do atestado]**, situada no **[endereço da Empresa Emitente do atestado]**, conforme descriminado abaixo:, no período de (__/__/__ a __/__/__):

SERVIÇO PRESTADO:

VALOR GLOBAL (R$):.....

Declaramos ainda que os compromissos assumidos foram executados satisfatoriamente, não constando em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

_____
Local e Data

_____ [Nome do Representante da Empresa Emitente] Cargo / Telefone/Email/ Contatos:

OBSERVAÇÃO: EMITIR EM PAPEL TIMBRADO DA EMPRESA/ ENTIDADE OU IDENTIFICÁ-LA LOGO ABAIXO OU ACIMA DO TEXTO, COM NOME, CNPJ, ENDEREÇO, TELEFONES, FAX E E-MAIL.

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.III

DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E A ADMINISTRAÇÃO PÚBLICA

Declaro que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida em _____, possui os seguintes contratos firmados com a iniciativa privada e a administração pública:

Nome do Órgão/Empresa contrato	Vigência do Contrato	Valor total do
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
Valor total dos Contratos		R$_____

Local e data

Assinatura e carimbo do emissor

Observação:
Além dos nomes dos órgãos/empresas, o licitante deverá informar também o endereço completo dos órgãos/empresas, com os quais têm contratos vigentes.

ANEXO I.IV

ACORDO DE CONFIDENCIALIDADE

Este **ACORDO DE CONFIDENCIALIDADE** ("Contrato") é celebrado entre as partes abaixo qualificadas:

[º], pessoa jurídica de direito privado, devidamente inscrita no CNPJ/MF sob o número [º], com sede na Rua [º], nº [º], Estado [º], CEP [º], neste ato representada na forma de seu [º], doravante denominada, simplesmente, **[º]**;

e,

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICIPIO DE PORTO ALEGRE - PROCEMPA, sociedade de economia mista, inscrita no CNPJ/MF nº 89.398.473/0001-00, com sede na Av. Ipiranga 1200, CEP 90160-091, neste ato representada na forma de seu Estatuto Social, doravante denominada, simplesmente, **PROCEMPA;**

[º] e **PROCEMPA** serão referidas coletivamente como "Partes" ou individualmente como "Parte".

CONSIDERANDO que as Partes desejam ajustar as condições de revelação de informações confidenciais, bem como definir as regras relativas ao seu uso e proteção;

CONSIDERANDO o contrato de prestação de serviços celebrado nos autos do processo SEI n° _____;

RESOLVEM as Partes celebrar o presente acordo de confidencialidade, o qual se regerá, de comum acordo entre as Partes, pelas considerações acima, bem como pelas cláusulas e condições a seguir:

Em conexão com a contratação, as Partes entendem a necessidade da divulgação de certas informações consideradas confidenciais. Tais informações podem incluir (mas

não estão limitadas) a dados cadastrais de clientes, segredos industriais, descobertas, ideias, conceitos, know-how, técnicas, designs, especificações, desenhos, diagramas, dados, programas de computador, atividades e operações comerciais, relatórios, estudos e outras informações técnicas e não técnicas, comerciais, patentes, direitos autorais, informações financeiras e contábeis, balanço patrimonial, detalhes e especificações, esquemas, informações de engenharia, fórmulas, estratégias de desenvolvimento e comercialização, planos, cálculos, prognósticos, orçamentos, estratégias de fixação de preços, requisitos de aquisições, políticas internas, listas de clientes e fornecedores, listas de locadores e imóveis alugados, listas de topos de condomínios alugados, técnicas, modelos, processos, equipamentos, algoritmos, "software", contratos e estratégias de negociação, sejam referidas informações escritas, gráficas, verbais ou inseridas em meios eletrônicos ou de qualquer outra forma armazenadas (aqui referidas como **"Informações Confidenciais**").

As Informações Confidenciais também incluirão todas as análises, compilações, estudos, resumos, extratos, cópias ou quaisquer outros documentos que contenham ou reflitam tais Informações Confidenciais, sejam eles preparados pela Parte Divulgadora ou pela Parte Receptora.

1. Proteção da Informação Confidencial. As Partes reconhecem que a Parte Reveladora considera suas Informações Confidenciais bens especiais, valiosos e únicos. Assim, a Parte que receber tais informações ("Parte Receptora") e seus executivos, diretores, administradores, agentes, empregados, afiliados, consultores e assessores, concordam que devem:

(a) Manter em segredo e tomar as medidas apropriadas para proteger o sigilo das Informações Confidenciais que receberem.

(b) Restringir a divulgação da Informação Confidencial a um mínimo necessário de pessoas (tais como empregados, diretores, executivos, advogados, contadores e consultores, os quais também devem ser pessoalmente comprometidos a manter a informação sob sigilo); e

(c) Utilizar a Informação Confidencial apenas em relação ao cumprimento do contrato de prestação de serviços.

Cada Parte será responsável pelo descumprimento por parte de seus Representantes e concorda em envidar esforços comercialmente razoáveis, exclusivamente a suas expensas (incluindo sem limitação a instauração de ações judiciais), com a finalidade de evitar que seus Representantes utilizem ou divulguem as Informações Confidenciais de algum modo proibido ou não autorizado.

Para fins deste Contrato, todas as referências à PROCEMPA ou à [º] incluirão qualquer entidade que de maneira direta ou indireta controle, seja controlada ou se encontre sob o controle comum da PROCEMPA ou da [º], respectivamente, sempre e quando tais entidades recebam Informações Confidenciais da outra Parte de acordo com este Contrato. As Partes assegurarão que estas entidades cumpram com o disposto no presente Contrato.

2. Identificação da Informação Confidencial. Salvo se disposto expressamente em contrário, todas as informações trocadas pelas Partes devem ser consideradas como Informação Confidencial.

3. Limitações nas Informações Confidenciais. Não se incluem nas Informações Confidenciais as informações que sejam:

(a) Livres de obrigação de sigilo, conforme demonstrado por documento escrito ou determinado pela lei aplicável;

(b) Publicamente disponíveis por meio de divulgação lícita, por outro meio que não pela divulgação da referida Informação Confidencial pela Parte Receptora ou pelos seus Representantes;

(c) Desenvolvidas de forma independente pela parte Receptora e sem referência alguma à Informação Confidencial;

(d) Licitamente obtida pela Parte Receptora de um terceiro, observado que, depois da devida investigação, a Parte Receptora tenha determinado razoavelmente que a fonte mencionada não esteja sujeita a contrato de confidencialidade nem a outra obrigação de confidencialidade com relação à referida informação; ou

(e) Já se encontre na posse da Parte Receptora no momento da divulgação, conforme devidamente comprovado pela Parte Receptora por escrito.

As limitações acima mencionadas devem ser aplicadas apenas à porção da Informação Confidencial sujeita a tais exceções. O restante das Informações Confidenciais mantém-se sujeito às restrições deste Contrato.

4. Revelação Obrigatória. Se a Parte Receptora receber uma ordem judicial para divulgar Informações Confidenciais (por meio de solicitações verbais, interrogatórios, solicitações de informações ou documentos, citações, inquérito civil de investigação ou um processo similar), ela não poderá sofrer qualquer penalização em decorrência do cumprimento da medida.

Porém, assim que possível, ela deve notificar a Parte Reveladora acerca do recebimento da ordem judicial, para permitir que esta atue da forma que entender adequada.

Na ausência de uma proteção judicial ou do recebimento da dispensa da obrigação de confidencialidade, a tal Parte ficará, não obstante a opinião do seu assessor jurídico, obrigada a divulgar a Informação Confidencial; ou ainda, caso esteja sujeita a ser processada por desacato ou a sofrer algum outro modo de censura ou penalização, tal Parte poderá divulgar aquela parte da Informação Confidencial que lhe for legalmente exigida sem penalização em virtude deste Contrato.

5. Retorno da Informação Confidencial. Todas as informações fornecidas sob este Contrato devem continuar de propriedade da Parte Reveladora e mediante solicitação

por escrito da outra Parte devem ser devolvidas a ela ou destruídas tão logo lhe seja solicitado (conjuntamente com todas as respectivas cópias, extratos, planos, esquemas ou outras reproduções totais ou parciais); observado, entretanto, mas sem prejuízo do anteriormente mencionado, que cada Parte poderá manter uma cópia das referidas Informações Confidenciais se assim for exigido por lei ou pela política de retenção de documentos adotada pela empresa, ou caso tal cópia se encontre em servidores de backup, dos quais não seja possível apagar as Informações Confidenciais.

6. Ausência de Licença. Nenhuma licença de qualquer direito de propriedade intelectual, incluindo, de forma declaratória, mas não se limitando, a licença de uso com relação às Informações Confidenciais é concedida, de forma explícita ou implícita, pela simples transmissão de Informações Confidenciais (ou outras informações) para a Parte Receptora, nem deve essa transmissão constituir qualquer declaração ou garantia da Parte Reveladora em relação à infringência de direitos de propriedade intelectual de terceiros.

Neste sentido, ambas as Partes reconhecem expressamente que a única detentora (incluindo de forma declaratória, mas não taxativa ou limitante, direitos autorais, marcas, nomes comerciais) das Informações Confidenciais divulgadas pela Parte Divulgadora, obrigando-se a Parte Receptora a não exercer, sem autorização expressa e por escrito da Parte Divulgadora, ação alguma concernente ao uso, propriedade ou divulgação das mencionadas Informações Confidenciais.

7. Ausência de Garantia. A Parte Reveladora não declara ou garante a precisão ou completude das Informações Confidenciais. As Partes, ainda, não serão responsáveis por omissões ou erros que possam existir na Informação Confidencial.

8. Ausência de Compromisso. O presente instrumento não é um compromisso das Partes de celebrar qualquer acordo comercial, nem de tomar quaisquer outras providências que não tenham sido expressamente acordadas neste instrumento ou

outro documento celebrado depois pelas Partes. Se as Partes desejarem perseguir oportunidades de negócios, elas devem celebrar em separado um acordo escrito para reger tais relações.

A Parte Divulgadora entende que a Parte Receptora poderá, no presente ou no futuro, desenvolver informações internamente ou receber informação de outras partes que podem ser similares à Informação Confidencial da Parte Divulgadora.

As Partes acordam que tal informação não estará compreendida dentro da definição de Informações Confidenciais segundo este Contrato e nada estipulado neste Contrato será interpretado como uma declaração ou inferência de que a Parte Receptora (i) não desenvolverá produtos, sistemas ou serviços, nem mandará desenvolver produtos, sistemas e serviços que concorram com os produtos, sistemas ou serviços contemplados nas Informações Confidenciais, ou (ii) não prestará serviços a entidades que concorram com a outra Parte.

9. Notificações. Todas as notificações sob este Contrato devem ser consideradas devidamente entregues mediante apresentação do aviso de recebimento, para os seguintes endereços ou para outro endereço validamente notificado por escrito pela respectiva Parte:

Notificações para a PROCEMPA:

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICIPIO DE PORTO ALEGRE – PROCEMPA.

Aos cuidados de: [º]

Av. Ipiranga, n. 1200

Azenha – CEP 90160-091

Porto Alegre – RS

Notificações para a [º]:

Aos cuidados de: [º]

Rua [º]

CEP [º]

10. Perdas e Danos e Multa*.* Cada uma das Partes acorda que os danos e prejuízos monetários não servirão de recurso no caso de qualquer descumprimento do presente Contrato e que a Parte inocente terá direito ao recurso cabível, incluindo ordem judicial, no caso de qualquer descumprimento deste Contrato, além de quaisquer outros remédios jurídicos aplicáveis.

Fica entendido e acordado que nenhuma omissão ou atraso de qualquer das Partes no exercício de qualquer direito, faculdade ou prerrogativas estabelecidas neste Contrato serão considerados como renúncia a tal direito, nem o exercício único ou parcial dos mesmos impedirá qualquer outro ou futuro exercício de qualquer direito, faculdade ou prerrogativa.

A Parte vencedora em qualquer ação interposta com a finalidade de exigir o cumprimento do presente Contrato terá direito ao reembolso de quaisquer honorários de advogados, despesas e custos incorridos pela outra Parte com tal ação.

11. Início e Fim da Vigência**.** Este Contrato inicia sua vigência na data em que a última assinatura for nele firmada e aplica-se às discussões ocorridas no prazo de vigência contratual. Não obstante, as Partes acordam que as obrigações de confidencialidades relativas ao uso das Informações Confidenciais compartilhada durante tal prazo sobreviverão ao referido prazo.

12. Independência das Disposições**.** Se alguma disposição deste Contrato for declarada inválida, nula ou inexequível, o remanescente continuará em vigor.

13. Ausência de Renúncia**.** A inércia de qualquer das Partes de exigir o cumprimento de qualquer disposição deste Contrato não deve afetar de forma alguma o direito de requerer tal execução posteriormente.

14. Acordo Completo, Aditivos**.** Este Contrato incorpora o entendimento integral das Partes e sobrepõe-se a todas as negociações prévias pertinentes a seu escopo. Este Contrato não deve ser modificado exceto por um aditivo escrito devidamente assinado por representante legal de ambas as Partes.

15. Transferência, Efeito de Compromisso**.** Uma Parte não pode ceder ou transferir os direitos e obrigações decorrentes este Contrato sem o prévio consentimento da outra, e qualquer transferência em violação a este Contrato será nulo. Este Contrato

deve beneficiar e vincular as Partes e seus respectivos sucessores e cessionários permitidos. Com exceção de sucessores e cessionários permitidos, nada do expressado ou envolvido neste Contrato tem a intenção de conferir ou outorgar a qualquer terceiro direito ou recurso algum.

16. Foro. As partes elegem o Foro Central da Cidade de Porto Alegre, Estado do Rio Grande do Sul, com expressa renúncia a qualquer outro, por mais privilegiado que seja ou se torne, para dirimir qualquer questão proveniente do presente Contrato. O presente Contrato será regido e interpretado de acordo com as leis da República Federativa do Brasil.

E, por estarem justas e convencionadas as Partes assinam o presente Contrato em duas vias idênticas, cada uma sendo tratada como um original, as quais conjuntamente constituirão um único documento original e que poderão ser transmitidas por fac-símile ou por correio eletrônico, juntamente com as testemunhas abaixo arroladas.

Porto Alegre, [º] de [º] de 2022.

_____

[º]

_____

[º]

PROCEMPA

PROCEMPA

TESTEMUNHAS:

_____

Nome:

CPF:

_____

Nome:

CPF:

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.V

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão Dezembro 2020

Apresentação

A Revolução Digital consolidada nas últimas décadas tornou possível um enorme avanço: a coleta, contabilização e processamento de quantidades significativas de dados do turbilhão de eventos que ocorrem todos os dias na sociedade. Hoje podemos extrair mais facilmente desses dados muitas informações que servem como farol orientador importantíssimo para tomada de decisões e identificação de oportunidades.
Considerando que os dados podem ser usados na tomada de decisões importantes, seu valor é reconhecido e deve ser preservado. O grande valor atrai grandes ameaças. Não devem cair nas mãos erradas. Adulterações e indisponibilidade podem levar a decisões erradas ou falta de ação.
Estas são as bases e justificativas para a Segurança da Informação, que visa a manutenção da Confidencialidade, Integridade e Disponibilidade das informações. E o instrumento importante para isso é a Política de Segurança da Informação, um conjunto de diretrizes, normas, procedimentos e padrões a serem observados e seguidos por todas as pessoas que utilizarem a infraestrutura da Companhia.

Diretrizes

Estes são os princípios básicos que regem a Política de Segurança da Procempa, estabelecidos de acordo com as necessidades da instituição.
1. À Procempa é atribuída a guarda de informações de seus clientes diretos e indiretos, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é essencial para a continuidade de negócio da Companhia.
2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, integridade e disponibilidade e ser tratada de acordo com a sua classificação, independente da sua forma de armazenamento, digital ou não.
3. Dados Pessoais e informações relacionadas a pessoa natural identificada ou identificável, devem obrigatoriamente ser protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) e tratados como confidenciais quando não houver justificativa legitima em contrário. Cuidados redobrados devem ser tomados em relação aos Dados Pessoais
Sensíveis, aqueles que podem revelar origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde, vida sexual ou orientação sexual.
4. As informações devem ter o ciclo de vida programado. Informações consideradas confidenciais, quando não mais necessárias, devem ser destruídas através de

mecanismos apropriados. O descarte ou reutilização de mídias contendo essas informações deve ser feito de forma a inviabilizar a recuperação das mesmas.
5. Todo o indivíduo que tenha acesso as dependências da Procempa deverá ser identificado.
O acesso de terceiros em áreas onde exista o processamento físico ou digital de informações deverá ser fundamentado pela estrita necessidade e deverá ocorrer sempre com o acompanhamento de empregado da Companhia, responsável pelas informações naquele setor.
6. Todos os equipamentos na Companhia deverão estar inventariados e identificados de forma individual.
7. Credenciais de acesso as instalações e sistemas são pessoais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas mediante autenticação com sua credencial, por isso deve zelar por sua proteção e sigilo, e realizar as ações de manutenção apropriadas para cada tipo de credencial, como a troca periódica de senhas.
8. Alterações no ambiente de produção devem ser previamente estudadas, formalizadas por processo padronizado, comunicadas, autorizadas e, sempre que possível, testadas em ambiente apropriado e isolado, anteriormente à efetiva colocação dos recursos em produção, para verificação e avaliação dos impactos causados no processo produtivo, com o objetivo de garantir a estabilidade do ambiente..
9. Os empregados, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações ou de mídias, equipamentos, componentes ou acessórios que as contém, como por exemplo: e-mails corporativos, planilhas, arquivos de dados ou vídeos.
10. A responsabilidade de manter a segurança é compartilhada por todos os funcionários. A Procempa deverá ministrar treinamentos para promover a conscientização e preparo.

Normas

Violações das normas abaixo relacionadas, incidentes ou falhas de segurança devem ser notificadas imediatamente à equipe de Segurança da Informação da Procempa. Se houver mera possibilidade de vazamento de Dados Pessoais, deve ser notificado também imediatamente o Encarregado de Processamento de Dados (DPO).

Segurança Física

1. Todo o indivíduo ao ingressar nas instalações da Procempa deverá usar crachá de identificação.
2. Pessoas externas à Companhia deverão ser identificadas na recepção e o seu ingresso nas instalações da Procempa será realizado mediante autorização e acompanhamento do empregado da Companhia.
3. Todo o equipamento que ingressar ou sair da Procempa, deverá estar acompanhado da respectiva nota fiscal e autorização do setor de Patrimônio.

4. Os prestadores de serviços da Procempa são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio da Procempa, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.
5. Documentos ou papeis contendo informações confidenciais, quando não mais necessários, devem ser triturados ou destruídos de forma a impossibilitar leitura.
6. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.
7. Mídias regraváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.
8. A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe e mediante prévia assinatura de termo de confidencialidade.
9. Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.

Credenciais

1. Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
2. Cada funcionário deve trocar periodicamente suas senhas e é de sua responsabilidade escolher senhas robustas, complexas e longas.
3. As senhas devem ser únicas, não devem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sites ou serviços não gerenciados pela Procempa, sejam de natureza pessoal ou não.

Uso da Rede

1. O acesso a Internet é fornecido para atividades e finalidades da Companhia. Acessos com fins particulares lícitos podem ser feitos ocasionalmente, preferencialmente fora do horário de expediente, desde que não violem as demais normas.
2. É proibido usar a rede para acessar ou enviar conteúdo pornográfico, ofensivo ou difamatório, bem como para constranger terceiros, sejam eles funcionários ou não.
3. O uso para fins particulares de redes sociais como Facebook ou Twitter e sítios de vídeos como YouTube, Vimeo e Netflix durante o horário de expediente é considerado inadequado e pode estar bloqueado a qualquer horário a critério da Companhia.
4. Qualquer sítio conhecido de conteúdo vedado ou inadequado pode estar em listas de bloqueio automático. Eventuais erros na classificação de determinado sítio podem ser comunicados à equipe responsável pelos proxys para retificação.
5. Os acessos à Internet podem ser monitorados e registrados pela Companhia. Os registros ficam a disposição da Companhia pelo tempo que esta julgar adequado.

6. O compartilhamento de recursos nas estações de trabalho deve ser limitado a atividades de interesse da Companhia, com liberação somente para leitura por conjunto restrito de usuários.
7. Não é permitido instalar, usar ou configurar equipamentos (hardware ou software) que deem acesso à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, hub, switch, vpn, roteador ou software de acesso remoto para fins pessoais.
8. Não é permitido copiar arquivos ou realizar acessos com fins particulares que onerem excessivamente a utilização da rede.
9. Todas as mensagens enviadas por correio eletrônico com o endereço profissional são de propriedade da Companhia, portanto devem ser usadas para assuntos de interesse da Procempa e não se deve manter qualquer expectativa de privacidade de seus conteúdos.
10. É vedado o envio ou participação em correntes, mesmo de solidariedade, premiações ou informações.
11. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.
12. Não é permitido distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo “corrente” e mensagens em massa, comerciais, de propaganda política ou o envio de correio eletrônico não solicitado, SPAM.
13. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede da Companhia sem autorização. Tais equipamentos podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela Companhia.

Proteção de Estações

1. Em todas as estações de trabalho, notebooks e laptops deve estar instalado, ativo e atualizado o antivírus corporativo indicado pela equipe de administração do antivírus para o seu sistema operacional.
2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe de administração do antivírus.
3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar aos responsáveis pela administração do antivírus que tomarão as providencias cabíveis.

Utilização de Programas

1. As estações de trabalho são disponibilizadas com os programas - sistema operacional e aplicativos - mínimos necessários para o desempenho de sua função básica.
2. São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras da Companhia e a legislação.

Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos e não abusivos.
3. Não é permitida a instalação nos equipamentos da Companhia de qualquer software, gratuito ou não, sem as devidas licenças para uso comercial da Companhia.
4. O uso ou instalação de software sem licença de uso ou em nome de outros sem autorização caracteriza crime de pirataria, ficando o usuário e o instalador sujeitos às sanções administrativas, legais e penais da legislação.
5. Ocasionalmente serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

Cópias de Segurança ou Backup

1. Cada usuário é responsável pela manutenção de cópias de segurança de seus arquivos de dados.
2. Arquivos gerados nas estações de trabalho que necessitem cópia de segurança deverão ser armazenados em servidor de arquivos apropriado da Companhia, desde que autorizado pelo supervisor. É responsabilidade do funcionário confirmar com a equipe de Backups que as pastas estão incluídas nas rotinas de cópias de segurança.
3. Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela Companhia ou cliente.
4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.
5. O responsável pelo servidor deverá ativar processo de backup das informações críticas, incluindo serviços como correio eletrônico, banco de dados e aplicações.
6. Todo o backup deve periodicamente passar por teste de restauração.
7. Meios de armazenamento devem ser guardados em local seguro, armário, cofre ou sala com chave ou controle de acesso e devem ser respeitados os tempos de vida útil sugeridos pelo fabricante.
8. Alguns backups têm tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

Sistemas e Aplicações

1. Não é permitida a transferência de dados para processamento ou armazenamento em serviços externos, de terceiros não autorizados expressamente pela Companhia ou cliente.
2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Companhia.
3. Os sistemas deverão gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim funções do Sistema de Segurança em uso, recursos do sistema operacional, recursos de banco de dados e/ou recursos da aplicação. Os registros deverão conter ao menos as seguintes informações: identificação da aplicação e função, momento da ocorrência (timestamp), informações que identifiquem a máquina ou local da ocorrência e os dados relevantes manipulados pela aplicação.

O Sistema de Segurança poderá se encarregar do registro de algumas dessas informações.
Informações confidenciais não devem ser registradas em log sem estarem criptografadas.
4. No desenvolvimento e manutenção de sistemas é obrigatório o uso de software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela Companhia.
5. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo utilizar preferencialmente áreas de trabalho em servidores designados. Caso estejam residentes em sua máquina, o desenvolvedor deve providenciar cópia de segurança (backup) dos mesmos, quando necessária.
6. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.
2. Após sua instalação o responsável deverá encaminhar à Equipe de Segurança solicitação para verificação complementar do servidor.
3. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas;
4. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia, tais como TELNET, FTP e VNCSERVER;
5. Os equipamentos utilizados devem possuir sistema operacional atualizado e com recursos de segurança.
7. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pela Equipe de Segurança), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego.
8. Não é permitida a instalação de serviços de rede não autorizados pela Equipe de Segurança.
9. Todo o tráfego de informações confidenciais por meio compartilhado será protegido através de criptografia.
10. Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvo dos serviços o acesso aos mesmos mediante solicitação para a equipe de Segurança.
11. A equipe de Segurança da Informação pode indicar e usar ferramentas de detecção e prevenção de intrusos, para emitir alertas e registrar possíveis tentativas de invasão.

Registros e Auditoria

1. Os administradores devem habilitar registros de segurança (logs), de forma a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditorias;
2. Os registros de segurança deverão ser analisados periodicamente (manual ou automaticamente).

Documentação Exigida

1. É fortemente recomendado que sistemas críticos tenham documentado Plano de Continuidade de Negócio ou Recuperação de Desastre.
2. Todas as instalações e atualizações deverão ser documentadas pelo responsável, administrador ou desenvolvedor, inclusive:

- Procedimentos para instalação;
- Correções instaladas (service packs, hot fixes, patches);
- Softwares instalados/atualizados;
- Configurações a serem realizadas;
- Permissões de acesso;
- Contatos para suporte;
- Informações Complementares.

Segurança Física de Servidores

1. O acesso físico aos servidores e equipamentos de infraestrutura deve ser restrito aos empregados e terceiros autorizados.
2. Os servidores e equipamentos de infraestrutura devem operar em ambiente adequado, sob condições (temperatura, nível de poeira, umidade, etc) indicadas pelo fabricante.

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.VI

MODELO DO TERMO DE ACEITE PARA PAGAMENTO

CONTRATADA:
CONTRATO:
OBJETO:

ATESTAMOS, para os devidos fins, que a empresa <nome da empresa> , procedeu com <apontar o serviço executado>, discriminados na Nota Fiscal/Fatura n.º <número da nota fiscal>, emitida em __ / __ / 20____, referente a OS Nº <inserir o número da OS>, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

Porto Alegre, ____ de _____ de 20__.

NOME DO GERENTE / GESTOR
Cargo e nome da área – SIGLA SIGLA

NOME DO RESP. PELA EMISSÃO
Cargo e nome da área –

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.VII

MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO – Nº

PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE SEGURANÇA

CONTRATO Nº

A presente ordem de serviço é celebrada em conformidade com o procedimento para PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE SEGURANÇA, previstos no Contrato Nº....., firmado entre o PROCEMPA e a CONTRATADA, em vigor desde ___ de _____ de _____, sendo incorporada ao mesmo por referência.

Quantidade de Horas	Período de Atividade da OS		Valor Total
	Início	Fim	
		TOTAL GERAL	

Descrição das atividades:

Planejamento

Descoberta;

Ataque (exploração);

Relatório Teste de Invasão;

Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste

Reavaliação, novo teste pós-remediação

Relatório final do teste de invasão

Para efeito do cumprimento desta ORDEM DE SERVIÇO a PROCEMPA e CONTRATADA indicam os seguintes responsáveis:

Especificação Técnica

TR Teste de Intrusão PENTEST

Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

CONTATOS DA CONTRATANTE		
Nome:		
Gerência:	Unidade:	Matrícula:
Telefones de Contato:		

CONTATOS DA CONTRATADA		
Nome:		
Gerência:	Unidade:	Matrícula:
Telefones de Contato:		

Porto Alegre, _____ de _____ de 20__

CONTRATANTE CONTRATADA

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.VIII

ACORDO DE PROTEÇÃO DE DADOS PESSOAIS

TERMO ADITIVO A CONTRATO DE PRESTAÇÃO DE SERVIÇOS

Processo SEI nº [º]

CONTRATANTE: COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE - PROCEMPA, sociedade de economia mista, inscrita no CNPJ sob o nº 89.398.473/0001-00, com sede na Avenida Ipiranga, 1200, Bairro Azenha, Porto Alegre, Estado do Rio Grande do Sul, neste ato representada por seu diretor-presidente, [º], e seu diretor técnico, [º], abaixo assinados.

CONTRATADA: [º]

As partes acima identificadas vêm aditar o contrato de prestação de serviços firmado nos autos do processo administrativo eletrônico nº [º], nos termos da Lei nº 13.303/2016, tão somente quanto ao que segue:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente termo aditivo tem por objeto estabelecer as obrigações da CONTRATADA relativas ao tratamento de dados pessoais em decorrência da execução do contrato firmado com a PROCEMPA, nos termos do instrumento contratual ora aditado.

CLÁUSULA SEGUNDA - DA PROTEÇÃO DE DADOS PESSOAIS:

2.1. A CONTRATADA obriga-se a guardar o mais completo sigilo por si, por seus empregados ou prepostos, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venha(m) tomar conhecimento ou ter acesso, em razão desse CONTRATO, ficando na forma da lei responsável pelas consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei ou desse CONTRATO.

2.2. Em relação a informações eventualmente protegidas por lei em especial deve ser observado o que segue:

(i) é vedada à CONTRATADA a utilização de referidas informações para quaisquer finalidades, que não previstas neste CONTRATO, ainda que estejam codificadas/criptografadas;

(ii) a CONTRATADA obriga-se a zelar pelo sigilo e guarda de tais informações como se suas fossem, observado o disposto na cláusula de sigilo/confidencialidade das informações e demais termos deste CONTRATO;

(iii) a CONTRATADA obriga-se a supervisionar e a fiscalizar toda a sua operação, no escopo desta contratação, com a finalidade de assegurar que o uso esteja aderente ao previsto neste instrumento.

2.3. Após o uso, todas as informações a que a CONTRATADA teve acesso deverão ser devolvidas, descartadas / excluídas do ambiente da CONTRATADA de forma irrecuperável, a critério da PROCEMPA.

2.4. Entende-se por “Dado Pessoal”, por força deste CONTRATO, todos e quaisquer dados ou informações que, individualmente ou em conjunto com outros dados ou nomes, identifiquem ou permitam que um determinado empregado/usuário seja identificado, incluindo: (i) dados que forem definidos explicitamente como uma categoria de dados pessoais, nos termos da Lei 13.709/2018 ("LGPD"); (ii) dados pessoais não públicos, tais como o número de identidade (RG), número de passaporte, número de seguro social (ou número equivalente), número de licença do motorista, CPF, endereço, telefone, e-mail, contato em redes sociais, nome dos pais de uma pessoa, data de nascimento, número do título de eleitor, entre outros; e/ou (iii) informações financeiras, como por exemplo, número de conta bancária, entre outras relacionadas.

2.5. A CONTRATADA, na qualidade de operadora dos Dados Pessoais, deverá trata-los única e exclusivamente para as finalidades estabelecidas no contrato ora aditado, ou conforme orientação por escrito fornecida pela PROCEMPA. Em caso de descumprimento da LGPD, em decorrência deste CONTRATO ou das orientações fornecidas pela PROCEMPA, a CONTRATADA será solidariamente responsável por eventuais prejuízos sofridos pela PROCEMPA.

2.6. A CONTRATADA, ao realizar o tratamento de Dados Pessoais, compromete-se a envidar os melhores esforços para cumprir as obrigações estabelecidas na LGPD.

2.7. A CONTRATADA manterá os Dados Pessoais e Informações Confidenciais sob programas de segurança (incluindo a adoção e a aplicação de políticas e procedimentos internos) elaborados para (a) identificar riscos prováveis e razoáveis para segurança e acessos não autorizados à sua rede; e (b) minimizar riscos de segurança, incluindo avaliação de riscos e testes regulares.

2.8. Uma Parte (“Parte Notificante”) deverá notificar a outra (“Parte Notificada”): (i) se tiver conhecimento ou suspeitar de qualquer comprometimento, divulgação a pessoas não autorizadas ou uso de Dados Pessoais e/ou Informações Confidenciais da Parte Notificante de maneira não autorizada; (ii) se tiverem sido apresentadas quaisquer reclamações sobre as práticas de tratamento pela Parte Notificante; ou (iii) se tiver ocorrido qualquer descumprimento significativo ou substancial dos requisitos contidos neste CONTRATO (cada, um “Incidente de Segurança”).

2.9. Salvo se legalmente exigido por lei ou compelida por uma intimação, ordem judicial ou outro documento legal similar emitido judicialmente ou por uma autoridade fiscalizadora, a Parte Notificante concorda em não divulgar o Incidente de Segurança a qualquer terceiro sem primeiramente obter o consentimento prévio e por escrito da Parte Notificada.

2.10. As obrigações e responsabilidades aqui assumidas pelas Partes permanecerão definitivamente em vigor, mesmo após o rompimento ou término, deste CONTRATO.

CLÁUSULA TERCEIRA - DA SEGURANÇA DA INFORMAÇÃO

3.1. A CONTRATADA, na forma aqui representada, declara ciência quanto às disposições da Política de Segurança da Informação da PROCEMPA, além de documentos correlatos, conforme aplicável, disponibilizada (os) através do link https://prefeitura.poa.br/procempa/politicas-e-lgpd comprometendo-se em cumpri-la(os) e fazê-la(os) cumprir por seus empregados e prepostos.

3.2. A PROCEMPA poderá a qualquer tempo, por si, ou por empresa interposta, auditar os sistemas e ambiente(s), físicos e virtuais, da CONTRATADA, relacionados

ao objeto da presente contratação, para verificar sua conformidade aos termos desse CONTRATO e aos normativos pertinentes à segurança da informação aplicáveis.

3.3. A CONTRATADA compromete-se a assegurar:

(a) o cumprimento da legislação e da regulamentação em vigor, em especial, mas não se limitando a LGPD;

(b) o mais pleno acesso da PROCEMPA aos dados e às informações a serem tratadas, processadas e/ou armazenadas, conforme o caso, nos termos desse CONTRATO;

(c) o acesso da PROCEMPA as informações fornecidas pela CONTRATADA, visando verificar o cumprimento do disposto nessa Cláusula Terceira - Da Segurança da Informação;

(d) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos dados disponibilizados pela PROCEMPA;

(h) que todos os dados e informações disponibilizadas no contexto do CONTRATO serão utilizadas exclusivamente nos termos e finalidades previstas nesse instrumento, estando vedada qualquer utilização não prevista, exceto se expressamente e inequivocamente aprovado pela PROCEMPA;

3.4. No caso de rompimento do CONTRATO, por qualquer motivo, a CONTRATADA se obriga a:

(a) transferir os dados e/ou informações contempladas nesse CONTRATO a novo prestador de serviços / fornecedor, conforme indicação da PROCEMPA, ou à própria PROCEMPA, observando as suas instruções;

(b) garantir a integridade e disponibilidade dos dados recebidos pela PROCEMPA e transferidos nos termos da alínea anterior; e

(c) excluir os referidos dados e/ou informações, de forma irrecuperável, após a transferência dos dados prevista na alínea "a" e/ou conforme solicitação da PROCEMPA, conforme o caso, emitindo em seguida declaração de que o fez, devidamente firmada pelos representantes da CONTRATADA.

3.5. A CONTRATADA obriga-se a comunicar imediatamente a PROCEMPA quando da ocorrência de qualquer incidente envolvendo os serviços contratados, execução do CONTRATO e os dados e/ou informações disponibilizados pela PROCEMPA (e/ou suas próprias informações), tomando de imediato todas as medidas que possam minimizar eventuais perdas e danos causados em razão do incidente, além de envidar os melhores esforços para cessar o incidente com a maior brevidade possível.

3.6. Eventuais perdas e danos causados em razão de incidentes envolvendo os dados e/ou informações que compõem o objeto desse CONTRATO em razão de ação e/ou omissão da CONTRATADA e/ou de terceiros a ela relacionados, deverão ser arcados pela CONTRATADA, ainda que a CONTRATADA não tenha agido com dolo e/ou culpa e ainda que ela tenha tomado medidas mitigadoras, cumprido o disposto neste CONTRATO e/ou comunicado à PROCEMPA tão logo tenha tomado ciência do incidente.

CLÁUSULA QUARTA – DAS DEMAIS CLÁUSULAS E CONDIÇÕES

4.1. As partes ratificam as demais cláusulas e condições não alteradas pelo presente termo aditivo.

Finalmente, por estarem assim, justas e acertadas, as partes assinam este instrumento de forma eletrônica, para que surta seus jurídicos e legais efeitos.

Porto Alegre, ... de de 2020.

CONTRATANTE:

CONTRATADA:

Especificação Técnica

TR Teste de Intrusão PENTEST
Elaborada para PROCEMPA em 26/05/2022 com validade até 26/05/2023

ANEXO I.IX

MODELO DE DECLARAÇÃO – CONFORMIDADE AO ART.38 DA LEI Nº 13.303/2016

À PROCEMPA
Ref: Edital de Licitação nº ...../.....
Objeto:.....

Prezados senhores,

A ....., inscrita no CNPJ sob o nº ....., sediada .....(endereço completo)....., com o telefone para contato nº (.....).....-..... e email ....., por intermédio do seu representante legal o(a) Sr.(a) ....., ...(cargo)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº ....., residente e domiciliado(a) no .....(endereço completo)....., DECLARA, para os devidos fins legais, que a empresa não incorre em nenhum dos impedimentos para participar de licitações e ser contratada, prescritos no art. 38 da Lei nº 13.303/2016, quais sejam:

- cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;
- suspensa pela empresa pública ou sociedade de economia mista;
- declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;
- constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;
- cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;
- constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
- cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
- que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

Aplica-se a vedação também:

- à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

- a quem tenha relação de parentesco, até o terceiro grau civil, com:
- dirigente de empresa pública ou sociedade de economia mista;
- empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;
- autoridade do ente público a que a empresa pública ou sociedade de economia mista esteja vinculada.
- cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a respectiva empresa pública ou sociedade de economia mista promotora da licitação ou contratante há menos de 06 (seis) meses.

.....
(Local e Data)

.....
(representante legal)