CONSELHO REGIONAL DE MEDICINA DO ESTADO DO CEARÁ

Comunicação Interna N°. SEI-9/2023/CREMEC/PRES/DIR/DIREX/DETIN

Fortaleza, 22 de fevereiro de 2023

DE: Raimundo Miranda Ribeiro da Silva

PARA: Diretoria executiva

Assunto: Contratação de empresa de segurança para testar o sistema do CREMEC.

Senhor Diretor,

Informamos que a senha do firewall do CREMEC foi alterada durante o feriado de carnaval no que acreditamos ter sido um ataque virtual.

Durante o mês de janeiro/2023 o CREMEC foi alvo de 2 ataques ao seu sistema de informática. Na ocasião, restauramos o sistema e trocamos as senhas de acesso.

Dia 16/01/2023 – A senha de administrador do servidor de arquivos foi alterada e o restante dos usuários teve a conta desabilitada durante a noite, deixando o CREMEC sem acesso aos arquivos e ao SEI por algumas horas.

Dia 19/01/2023 – O computador que funciona como firewall e servidor de VPN teve sua configuração alterada durante a noite, fazendo com que a rede de computadores ficasse inativa por algumas horas. Esse ataque ficou registrado no log do sistema. (anexo)

Tais ataques trazem grande prejuízo ao setor de TI pois, além de já ter alta demanda pelos problemas causados por falhas de hardware e software, tem também que solucionar problemas causados por ataques intencionais.

Em vista do exposto, solicitamos a **contratação de empresa especializada em SEGURANÇA DE TI** para que sejam analisadas possíveis brechas de segurança que estão possibilitando os ataques externos e formas de combatê-los. Além de propor melhorias que aumentem a confiabilidade e segurança do sistema em geral.

Atenciosamente,

RAIMUNDO MIRANDA RIBEIRO DA SILVA

Técnico de Informático

Documento assinado eletronicamente por **Raimundo Miranda Ribeiro da Silva**, **Técnico de Informático**, em 22/02/2023, às 16:31, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0090424** e o código CRC **A2BB9436**.

CREMEC
CONSELHO REGIONAL DE MEDICINA DO ESTADO DO CEARÁ

Av. Antônio Sales, 485 - Bairro Joaquim Távora |
CEP 60135-101 | Fortaleza/CE - https://cremec.org.br/

Referência: Processo SEI nº 23.6.000001768-3 | data de inclusão: 22/02/2023

○	○	1/19/23 23:26:54	22.2	213 KiB	admin@10.10.20.5 (Local Database): Widget configuration has been changed.	
○	○	1/19/23 23:26:40	22.2	213 KiB	admin@10.10.20.5 (Local Database): Widget configuration has been changed.	
○	○	1/19/23 23:24:36	22.2	213 KiB	pfsense@10.10.20.5 (Local Database): Widget configuration has been changed.	
○	○	1/19/23 14:06:12	22.2	213 KiB	admin@192.168.0.26 (Local Database): Successfully edited user Miranda	
○	○	1/19/23 13:59:23	22.2	213 KiB	admin@192.168.0.26 (Local Database): Reverted to config-1674095608.xml.	
○	○	1/19/23 12:00:00	22.2	214 KiB	(system): Scheduled backup	
○	○	1/19/23 11:08:20	22.2	214 KiB	admin@192.168.0.26 (Local Database): Successfully edited user pfsense	
○	○	1/19/23 11:04:56	22.2	214 KiB	admin@192.168.0.26 (Local Database): Successfully edited user admin	
○	○	1/19/23 10:41:10	22.2	214 KiB	pfsense@10.10.20.5 (Local Database): Widget configuration has been changed.	
○	○	1/19/23 09:55:15	22.2	214 KiB	admin@192.168.0.64 (Local Database): DHCP Server - Settings changed for interface LAN	
○	○	1/19/23 09:53:33	22.2	214 KiB	admin@192.168.0.64 (Local Database): DHCP Server - Settings changed for interface LAN	
○	○	1/19/23 08:44:04	22.2	214 KiB	pfsense@10.10.20.4 (Local Database): Widget configuration has been changed.	
○	○	1/19/23 08:41:50	22.2	214 KiB	pfsense@10.10.20.4 (Local Database): Widget configuration has been changed.	
○	○	1/18/23 23:43:30	22.2	214 KiB	(system): Installed Netgate Firmware Upgrade package.	
○	○	1/18/23 23:43:16	22.2	213 KiB	pfsense@10.10.20.7 (Local Database): Creating restore point before package installation.	
○	○	1/18/23 23:35:06	22.2	213 KiB	admin@10.10.20.7 (Local Database): Widget configuration has been changed.	
○	○	1/18/23 23:34:29	22.2	213 KiB	admin@10.10.20.7 (Local Database): DHCP Server - Settings changed for interface LAN	
○	○	1/18/23 23:34:17	22.2	213 KiB	admin@10.10.20.7 (Local Database): DHCP Server - Settings changed for interface LAN	
○	○	1/18/23 23:33:28	22.2	213 KiB	admin@10.10.20.7 (Local Database): Firewall: Rules - saved/edited a firewall rule.	
○	○	1/18/23 23:27:34	22.2	213 KiB	admin@10.10.20.7 (Local Database): Successfully created user pfsense	
○	○	1/18/23 12:00:00	22.2	212 KiB	(system): Scheduled backup **Alteração às 23:34 do dia 18/01/2023**	
○	○	1/17/23 12:00:00	22.2	212 KiB	(system): Scheduled backup	
○	○	1/16/23 12:00:00	22.2	212 KiB	(system): Scheduled backup	
○		1/15/23 12:00:00	22.2	212 KiB	(system): Scheduled backup	

Diff

ANEXO I
TERMO DE REFERÊNCIA

1 – OBJETO DA CONTRATAÇÃO

1.1 Constitui objeto deste Termo de Referência o registro de preços para contratação de empresa especializada na prestação de serviço técnico de segurança da informação, de testes de intrusão (Pentest) em infraestrutura de rede e sistemas, na forma de consumo de UST, pelo período de 24 (vinte e quatro) meses, a ser executado sob demanda.

1.2 A contratação se dará mediante o consumo de USTs, sendo utilizadas sob demanda, de forma planejada, com escopo previamente definido e combinado com a CONTRATANTE.

1.3 O quantitativo sob demanda de UST representa uma mera expectativa em favor da(s) empresa(s) licitante(s) vencedora(s), posto que depende da necessidade da Instituição, não estando obrigada a realizá-la em sua totalidade e não cabendo à(s) empresa(s) contratada(s) pleitear(em) qualquer tipo de reparação.

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Qtd.	Métrica ou Unidade
1	Contratação de empresa especializada na prestação de serviço técnico de segurança da informação de testes de intrusão (Pentest) em infraestrutura de rede e sistemas, na forma de consumo de UST, pelo período de 24 (vinte e quatro) meses, a ser consumido sob demanda.	26077	960	UST

2.2 O quantitativo sob demanda de UST representa uma mera expectativa em favor da(s) empresa(s) licitante(s) vencedora(s), posto que depende da necessidade

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

da Instituição, não estando obrigada a realizá-la em sua totalidade e não cabendo à(s) empresa(s) contratada(s) pleitear(em) qualquer tipo de reparação.

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1 Contextualização e Justificativa da Contratação

- ✓ Devido à diversidade de sistemas operacionais, hardware, software e fabricantes que hoje compõem o ambiente computacional do Conselho Federal de Medicina, tem-se como boa prática prevista na ISO/IEC 27002:2013 e na Política de Segurança do CFM, realizar de forma sistemática a avaliação da segurança da infraestrutura.
- ✓ Os serviços de testes de intrusão (*pentest*) em infraestrutura de redes e sistemas visam identificar antecipadamente e de modo contínuo as vulnerabilidades na infraestrutura de TI do Conselho Federal de Medicina, que poderiam ser usadas para a obtenção de acesso não autorizado à rede corporativa, e dar margem a atos de roubo de informações, ataque à rede, violação de bancos de dados e sistemas entre outros ilícitos, colocando em risco a integridade da imagem do CFM.
- ✓ O teste de intrusão vem ao encontro dessa necessidade, sendo capaz de prover uma visão pormenorizada, considerando, inclusive, as mais recentes metodologias e técnicas utilizadas por atacantes, expondo internamente as possíveis fraquezas eventualmente existentes na infraestrutura de tecnologia do CFM. Desta maneira, será possível atuar de forma proativa nas correções e implantação de controles necessário à mitigação dos riscos, reduzindo consideravelmente a probabilidade de ataques e outras ações de atores maliciosos.

3.1 Motivação

Os seguintes fatores motivaram essa contratação:

- A terceirização de serviços de TI tem sido utilizada por grande parte dos órgãos da Administração Pública Federal para atender adequadamente à crescente demanda por sistemas e soluções originadas pelas áreas meio e fim;
- As atividades de todas as áreas do CFM dependem diretamente do uso das facilidades proporcionadas pelos recursos tecnológicos cada vez mais essenciais ao desenvolvimento de suas atividades;
- O CFM ainda não possui em seu quadro, pessoal qualificado em quantitativo suficiente para a prestação desses serviços;
- Necessidade de uma auditoria externa para avaliar de forma independente as vulnerabilidades existentes no ambiente do CFM.

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

3.2 Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
N1	Incentivar a eficiência tecnológica e adequar instalações físicas e recursos humanos

3.3 Estimativa da demanda

3.3.1 Para a realização testes de intrusão (*Pentest*) em infraestrutura de rede e sistemas para o Conselho Federal de Medicina foi estimado 960 UST, que corresponde a uma hora de serviço técnico especializado:

Id.	Descrição do Bem ou Serviço	Qtd.	Métrica ou Unidade
1	Contratação de empresa especializada na prestação de serviço técnico de segurança da informação de testes de intrusão (Pentest) em infraestrutura de rede e sistemas, na forma de consumo de UST, pelo período de 24 (vinte e quatro) meses, a ser consumido sob demanda.	960	UST

3.3.2 Com base nos entregáveis previstos nesse Termo de Referência, foi **estimado** uma quantidade de USTs para execução de cada entrega. Essa quantidade de UST por entregáveis poderá ter uma variação maior ou menor que será avaliado de forma planejada, com escopo previamente definido com a CONTRATANTE e aprovado pela CONTRATADA.

3.3.3 A divisão de estimativa de UST por sistema e por serviço é meramente explicativa e como colocado, trata-se de levantamento preliminar, que poderá apresentar variações de acordo com a complexidade e urgência do serviço ou sistema a ser testado, devendo o quantitativo exato de USTs, ser acordado entre CONTRATANTE e CONTRATADA em reunião oportuna para definição de escopo e testes a serem executados.

Item	Entregáveis	Estimativa de UST
1	Fase de Planejamento	**5**

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

1.1	Reunião Inicial	**2**
1.2	Entendimento da Solicitação	**3**
2	Fase de Descoberta e Exploração	**59**
2.1	Execução da descoberta e exploração	**40**
2.2	Relatório técnico Parcial dos resultados	**16**
2.3	Realização da apresentação Técnica	**3**
3	Reteste	**24**
4	Relatório final	**8**
4.1	Relatório técnico Final dos resultados	**7**
4.2	Seminário de Apresentação e Entrega do Relatório Final do Pentest	**1**
	Total	**96 USTs**

Observação: UST corresponde a uma hora de serviço técnico especializado

3.3.4 Para essa estimativa estamos tomando-se como premissa a realização de aproximadamente 10 testes de intrusão (Pentest) em infraestrutura de rede e sistema, sendo divido em:

- 02 testes para rede externa (ativos expostos à rede pública que sejam integrantes de esquemas de proteção (firewalls, roteadores, IPS, filtros, proxies, autenticadores e etc);
- 02 testes para rede interna: (vunerabilidades na rede sem fio (Wi-Fi), serviços como Web Servers, FTP Servers, DNS servers, SSH Servers e etc);
- 06 testes de para sistemas WEB que o CFM utiliza: Portal CFM, Intranet, SICOM, Prescrição Eletrônica, Fiscalização e Processo Administrativo Eletrônico.

3.4 Resultados e Benefícios a Serem Alcançados

Entre os benefícios diretos e indiretos esperados são:

- Análise geral do ambiente atual de TI do CFM em relação à segurança das informações;
- Listagem e classificação das vulnerabilidades encontradas no ambiente de TI do CFM;
- Priorização de ações de minimização de vulnerabilidades;
- Relatórios de testes de invasão;
- Prevenção de futuras invasões por vulnerabilidades já conhecidas;

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

- Mudança em processos internos com vista à minimização de vulnerabilidades;
- Subsídio para processo de educação e conscientização dos usuários do CFM em relação à segurança das informações;
- Subsídio para justificativa de aquisição de soluções e contratação de serviços especializados;
- Transferência de conhecimento técnico com apresentações dos serviços;
- Evolução do atual modelo de gestão de segurança da informação e o consequente aumento do nível de maturidade.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1 Requisitos Legais

Esta contratação encontra-se amparada no Art. 10, parágrafo 7º, do Decreto-Lei 200/67, pois as atividades que se pretende contratar, são extremamente especializadas, podendo ser realizadas mediante prestação de serviços terceirizados, em conformidade com a legislação pátria.

> Art. 10. A execução das atividades da Administração Federal deverá ser amplamente descentralizada. [...] § 7º Para melhor desincumbir-se das tarefas de planejamento, coordenação, supervisão e controle e com o objetivo de impedir o crescimento desmesurado da máquina administrativa, a Administração procurará desobrigar-se da realização material de tarefas executivas, recorrendo, sempre que possível, à execução indireta, mediante contrato, desde que exista, na área, iniciativa privada suficientemente desenvolvida e capacitada a desempenhar os encargos de execução. (Decreto-lei 200/1967).

Seguindo a mesma linha, o Decreto 9.507/2018 (Art. 3º, §1º) estabelece que as atividades materiais acessórias da Administração Pública Federal, inclusive as de informática, poderão ser de preferência, objeto de execução indireta. Constituíram ainda o referencial normativo da presente contratação os seguintes dispositivos legais:

I. Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;
II. Lei 10.520/2002: Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;
III. Decreto nº 5.450/2005: Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
IV. Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;

V. Nota Técnica nº 02/2008 – SEFTI/TCU – Estabelece o uso do pregão para aquisição de bens e serviços de tecnologia da informação;
VI. Instrução Normativa SLTI nº 04/2010: Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional; e
VII. Resolução nº CF-RES-2012/00187: Dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal – MCTI-JF no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

4.1 Requisitos para as licitantes

4.1.1 As empresas interessadas em participar desta licitação deverão verificar todas as especificações constantes no edital e em seus anexos, bem como as especificações definidas nos Encartes Técnicos referentes aos serviços a serem prestados.
4.1.2 A licitante deverá comprometer-se com o atendimento, nas condições técnicas e de preço oferecidas para o objeto do edital, respeitados os limites legais e técnicos, bem como, os prazos estipulados nos acordos de níveis mínimos de serviço.
4.1.3 Não há garantia de consumo mínimo para os serviços licitado.
4.1.4 Essa contratação obedecerá aos critérios de sustentabilidade ambiental para a contratação dos serviços, conforme estabelecido por meio da Instrução Normativa - IN nº 01/2010.

4.2 Requisitos de Projeto e de Implementação

4.2.1 Trata-se de contratação de serviços de teste de invasão em redes e sistemas de forma a mitigar ou eliminar o sucesso em possíveis ataques aos sistemas e serviços disponibilizados pela COINF (Coordenação de Informática) do Conselho Federal de Medicina (CFM) a ser executado sob demanda em um período de 24(vinte e quatro) meses.
4.2.2 A contratação será de UST a serem consumidas sob demanda, de forma planejada, com escopo previamente definido e combinado com a CONTRATANTE.
4.2.3 A divisão de estimativa de UST por sistema e por serviço é meramente explicativa e como colocado, trata-se de levantamento preliminar, que poderá apresentar variações de acordo com a complexidade do serviço ou sistema a ser testado, devendo o quantitativo exato de USTs, ser acordado entre CONTRATANTE e CONTRATADA em reunião oportuna para definição de escopo e testes a serem executados.
4.2.4 A execução dos Testes de Invasão poderá ser realizada presencialmente na sede da CONTRATANTE, em Brasília, ou

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

remotamente, em forma previamente combinada com e autorizada pela CONTRATANTE.

4.2.5 Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável do CFM.

4.2.6 Os Testes de Invasão serão executados sob demanda e com escopo previamente definido e combinado com a CONTRATANTE em reunião específica com a CONTRATADA, onde também será combinada a quantidade de USTs para a realização de cada Teste de Invasão.

4.2.7 Devem ser fornecidos pela CONTRATADA, na forma de serviços, sem ônus, quaisquer softwares ou hardwares necessários à execução dessa atividade.

4.2.8 A CONTRATADA deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante qualquer das fases de realização do *Pentest*.

4.2.9 A CONTRATADA é responsável pelo licenciamento, manutenção preventiva e corretiva das soluções de hardware e software integrantes dos serviços.

4.2.10 As atividades aqui descritas não devem, em qualquer hipótese, se resumir ao uso de ferramentas automatizadas, devendo prever obrigatoriamente a atuação de equipe especializada na realização de análises dessa natureza, devendo esta realizar análise qualitativa que extrapolem os possíveis relatórios gerados por ferramentas.

4.2.11 Inicialmente, deverão ser efetuadas operações automáticas e manuais de varredura, de forma a coletar informações que forneçam subsídios para uma eventual exploração das vulnerabilidades encontradas. Se encontradas vulnerabilidades exploráveis, deverão ser efetuadas tentativas sistemáticas de intrusões em profundidade, de forma a avaliar a extensão prática de um ataque bem-sucedido. Todas as evidências devem ser documentadas.

4.2.12 Para os casos de testes reativos, aqueles realizados após a ocorrência de um incidente de segurança, deve ser realizado uma análise forense, para identificar as ações externas que comprometeram os ativos de tecnologias, sistemas e aplicações.

4.2.13 Para toda vulnerabilidade encontrada, a Contratada deverá descrevê-la de forma detalhada assim como as ações para sua correção. Caso seja necessário ter acesso às configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo do CFM decidir pela liberação.

4.2.14 A CONTRATADA deverá estabelecer plano de comunicação entre envolvidos e conhecedores do(s) teste(s). O plano deve especificar, pelo menos, como e quando a comunicação ocorrerá, caso a equipe de teste comprometa o aplicativo, se alguma falha de segurança for descoberta ou se a realização do teste causar problemas não esperados para a instituição.

4.2.15 A CONTRATADA deverá propor padrão para registrar os resultados dos testes de segurança e detalhar as evidências no relatório emitido a cada pentest, no intuito de servir como referência técnica, durante processo de auditoria interna e externa.

4.2.16 A CONTRATADA deverá remover ao final dos testes os códigos de teste e arquivos desnecessários, contendo ou não informações sigilosas, incluindo as contas criadas para realizar os serviços.

4.2.17 O tempo estimado para cada teste, e consequentemente as USTs previstas, 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.

4.2.18 A Contratada deve apresentar um cronograma com todas as etapas e atividades e seus respectivos tempos para execução.

4.2.19 A Contratada deverá apresentar os resultados presencialmente ou de forma remota para o CFM, em data e hora oportunos, a serem definidos em comum acordo entre a Contratada e a equipe técnica do CFM.

4.2.20 Ao término de cada teste de invasão, deverão ser produzidos, no mínimo, os seguintes relatórios:

4.2.20.1 Relatório Executivo: com o resumo gerencial do teste e seu resultado. Este deve também fornecer informações resumidas, de forma gerencial, caso alguma falha tenha sido explorada;

4.2.20.2 Relatório Técnico: com o detalhamento completo do teste. Através deste deverá ser possível a reprodução da exploração.

4.2.21 Os testes não são exaustivos. Outros testes não citados poderão e deverão ser realizados caso entendimento da equipe técnica da Contratada da importância destes para correta identificação da segurança do objeto a ser testado.

4.2.22 Todos os testes a serem realizados deverão ser precedidos de caderno de testes gerado na fase de planejamento dos Testes, contendo todo o detalhamento das ações a serem executadas, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações do CFM.

4.2.23 A aprovação do caderno de testes, condição essencial para início das

atividades, deverá ser feito pelo responsável da Infraestrutura e/ou pelo responsável pelos sistemas, com anuência do Coordenador da Tecnologia da Informação.

4.2.24 O prazo para conclusão de um Teste de Invasão dependerá diretamente do escopo e do que será combinado em reunião oportuna entre a CONTRATANTE e a CONTRATADA.

4.2.25 As modalidades de *pentest* serão classificadas da seguinte maneira:

4.2.25.1 *Black-box*: Quando o executor do teste não possui informações acerca do ambiente tecnológico e arquitetura do alvo;

4.2.25.2 *Gray-box*: Quando o executor do teste tem conhecimento limitado ou algumas informações acerca do ambiente tecnológico e arquitetura do alvo;

4.2.25.3 *White-box*: Quando o executor tem pleno conhecimento e vasta informação acerca do ambiente tecnológico e arquitetura do alvo.

4.2.26 As ferramentas utilizadas nos testes de intrusão são de responsabilidade da CONTRATADA, não devendo ser instaladas no ambiente tecnológico do Órgão.

4.2.27 A utilização de ferramentas não deve resumir à atuação do analista quando da realização do *pente*st, sendo apenas auxiliares no processo de identificação, análise e posterior exploração de vulnerabilidades.

4.3 Requisitos dos testes de Invasão em Redes

TESTES EXTERNO

4.3.1 A contratada deverá avaliar a proteção do domínio da contratante sob o ponto de vista externo (a partir da Internet).

4.3.2 Deverão ser avaliados serviços críticos de comunicação, servidores, firewalls e outros elementos integrantes de esquemas de proteção, aplicações Web (portais), além da infraestrutura de roteamento.

4.3.3 Os serviços deverão ser executados fora das dependências do CONTRATANTE simulando, desta forma, ataques oriundos e qualquer parte da Internet.

4.3.4 As análises e testes deverão ser executados em no escopo de até 128 (cento e vinte e oito) endereços IP’s válidos, distribuídos em dois links, da contratante que possuem serviços associados.

4.3.5 Deverão ser incluídos no relatório todos os endereços IPs analisados e os respectivos serviços encontrados com seus fingerprints (se identificados, caso contrário informar que não conseguiu identificar).

4.3.6 Primeiramente, deverão ser efetuadas operações automáticas e manuais de varredura e probing, de forma a coletar informação que forneçam subsídios para uma eventual exploração das

vulnerabilidades encontradas. Se encontradas vulnerabilidades exploráveis, deverão ser efetuadas tentativas sistemáticas de intrusões em profundidade, de forma a avaliar a extensão prática de um ataque bem-sucedido.

4.3.7 Deverão ser alvos desta etapa:

4.3.7.1 Eventuais elementos ativos expostos à rede pública que sejam integrantes de esquemas de proteção (firewalls, roteadores, IPS, filtros, proxies e autenticadores);

4.3.7.2 Devem ser identificadas ameaças e vulnerabilidades através de simulações de testes de invasão nos ativos de tecnologia, como roteadores, servidores Windows, servidores Linux, switches, firewall, balanceadores e demais elementos da infraestrutura do CFM;

4.3.7.3 Deverão ser realizados mapeamentos e sondagens da infraestrutura, com o objetivo de realizar a varredura por hosts, regras de firewall e detecção de serviços em execução;

4.3.7.4 Deverão ser realizados, sob autorização do Gerente de Infraestrutura, com anuência do Coordenador de Tecnologia da Informação, testes remotos de quebra de senhas via dicionário, força bruta ou man-in-the-middle.

4.3.7.5 Deverão ser realizadas, análises do tráfego da rede, com o intuito de obter informações sensíveis;

4.3.7.6 Deverão ser realizados o lançamento de códigos maliciosos com o objetivo de explorar as vulnerabilidades encontradas. Essa ação deve ter a autorização do Gerente de Infraestrutura e com anuência do Coordenador de Tecnologia da Informação;

4.3.7.7 Os testes de segurança que possam levar a negações de serviço (Denial of Service – DoS – e DDoS – Distributed Denial of Service) deverão ser realizados após autorização do CONTRATANTE, que definirá os dias (fins de semana) e horários de execução dos testes;

4.3.7.8 Ao ser detectado sucesso na realização de DoS e DDoS, a contratada deverá cessar, imediatamente este ataque de forma que o ambiente possa responder normalmente aos seus usuários;

4.3.7.9 Resistência a spoofers;

4.3.7.10 Implantação de coletores de pacotes (packet sniffers), controles remotos e outras ferramentas de monitoração, quando e onde couber;

4.3.7.11 Testes remotos de quebra de senhas via dicionário, força bruta ou man-in-the-middle;

4.3.7.12 Busca por vulnerabilidades quanto à personificação de máquinas

confiadas (trusted hosts) e eventuais anomalias de roteamento;

4.3.7.13 Vulnerabilidades quanto à adulteração do DNS (DNS spoofing);

4.3.7.14 Deverão ser analisadas vulnerabilidades associadas a diversos serviços como Web servers, Application Servers, FTP Servers, Mail Servers, DNS Server, SSH, dentre outros;

4.3.7.15 Vulnerabilidades associadas ao elemento humano, utilizando-se, inclusive, engenharia social (phishing scam, telefonemas, etc.).

4.3.8 Os serviços executados nesta etapa não devem se resumir ao uso de ferramentas, devendo incluir procedimentos e técnicas não oferecidas por nenhuma ferramenta conhecida.

4.3.9 A contratada não deverá alterar a integridade das informações, ou seja, não deve alterar as informações de servidores e sistemas que possam comprometer os serviços prestados pelo CONTRATANTE.

4.3.10 O teste de invasão só poderá acontecer mediante autorização do Gerente de Infraestrutura e com anuência do Coordenador de Tecnologia da Informação.

4.3.11 Deverá ser comunicado ao Coordenador da COINF o andamento da análise, inclusive, se durante o teste de invasão encontrar alguma questão crítica.

4.3.12 Toda e qualquer modificação/alteração da configuração de um ativo no andamento do teste deve ser documentada e comunicada imediatamente, para aprovação da equipe de Infraestrutura do CFM.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

TESTES INTERNOS

4.3.13 A contratada deverá avaliar a proteção do domínio da contratante sob o ponto de vista interno (a partir das dependências da contratante e sua respectiva rede local – LAN/WLAN).

4.3.14 Deverão ser avaliados a topologia, arquitetura, serviços críticos de comunicação, e outros elementos integrantes de esquemas de proteção, aplicações Web (portais), além da infraestrutura de roteamento.

4.3.15 Para fins de dimensionamento da proposta, a licitante deverá utilizar os parâmetros elencados abaixo e tirar todas as dúvidas necessárias durante a vistoria técnica, pois dados foram omitidos por questões de segurança:

4.3.15.1 Aproximadamente 400 estações de trabalho (mini dekstop, notebooks);

4.3.15.2 Após a varredura de vulnerabilidades no ambiente, a contratada deverá elencar, no mínimo, 10% dos desktops para efetuar as análises detalhadas;

4.3.15.3 Aproximadamente 10 (dez) switches gerenciáveis;

4.3.15.4 Aproximadamente 80 servidores Linux incluindo produção, homologação e desenvolvimento.

4.3.16 Poderá haver horários distintos do item anterior para que sejam avaliados os controles de acesso do CFM.

4.3.17 Primeiramente, deverão ser efetuadas operações automáticas e manuais de varredura e probing, de forma a coletar informação que forneçam subsídios para uma eventual exploração das vulnerabilidades encontradas. Se encontradas vulnerabilidades exploráveis, deverão ser efetuadas tentativas sistemáticas de intrusões em profundidade, de forma a avaliar a extensão prática de um ataque bem-sucedido.

4.3.18 Deverão ser alvos desta etapa:

4.3.18.1 Elementos ativos que ofereçam serviços à rede pública e intranet, desde que possam representar ameaças aos serviços ou à rede interna e zonas desmilitarizadas, em caso de efetivo comprometimento, a exemplo de firewalls, proxies, switches, roteadores, desktops de usuários, servidores dedicados (appliances) e de propósito geral;

4.3.18.2 Os testes deverão incluir as seguintes categorias:

4.3.18.2.1 Procura de serviços privilegiados desprotegidos e existência de back doors;

4.3.18.2.2 Exploração de bugs conhecidos tais como buffer overflow, race conditions, XSS, SQL Injection, command injection, cookie/session poisoning, etc., para negação de serviço ou obtenção de acesso privilegiado;

4.3.18.2.3 Os testes de segurança que possam levar a negações de

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

serviço (Denial of Service – DoS – e Distributed Denial of Service - DDoS) deverão ser realizados após autorização do CONTRATANTE, que definirá os dias (fins de semana) e horários de execução dos testes;

4.3.18.2.4 Ao ser detectado sucesso na realização de DoS ou DDoS, a contratante deverá cessar, imediatamente este ataque de forma que o ambiente possa responder normalmente aos seus usuários;

4.3.18.2.5 Resistência a spoofers;

4.3.18.2.6 Implantação de coletores de pacotes (packet sniffers), controles remotos e outras ferramentas de monitoração, quando e onde couber;

4.3.18.2.7 Testes remotos de quebra de senhas via dicionário e/ou força bruta, inclusive à sistema de diretório de usuários (LDAP) e Bancos de Dados;

4.3.18.2.8 Busca por vulnerabilidades quanto à personificação de máquinas confiadas (trusted hosts) e eventuais anomalias de roteamento;

4.3.18.2.9 Vulnerabilidades quanto à adulteração do DNS (DNS spoofing);

4.3.18.2.10 Vulnerabilidades associadas a diversos serviços como Web Servers, FTP Servers, Mail Servers, DNS servers, SSH Servers, etc.;

4.3.18.2.11 Associadas a Vulnerabilidades aplicações web expostas ao público interno;

4.3.18.2.12 Vulnerabilidades associadas ao elemento humano, utilizando-se, inclusive, engenharia social;

4.3.18.2.13 Vulnerabilidades físicas de controle de acesso às instalações do CFM, assim como a documentações e a equipamentos;

4.3.18.2.14 Identificar os compartilhamentos de pasta e níveis de permissão através de varredura no parque computacional. Esses compartilhamentos devem ser apresentados em conjunto com os relatórios;

4.3.18.2.15 Vulnerabilidades associadas a desktops;

4.3.18.2.16 Vulnerabilidades associadas com redes sem fio;

4.3.18.2.17 Tentativas de acesso não autorizado à rede sem fio (Wi-fi);

4.3.18.2.18 Captura de dados da rede sem fio (Wi-fi);

4.3.18.2.19 Negação de serviços (DoS) e man-in-the-middle no ambiente de rede sem fio (Wi-fi).

4.3.19 Encontradas vulnerabilidades exploráveis ou potencialmente exploráveis, deverão ser efetuados testes de intrusão em

profundidade, de forma a determinar até onde (e em que condições) as eventuais vulnerabilidades podem ser utilizadas por um eventual atacante, e a extensão prática de um ataque.

4.3.20 Os serviços executados nesta etapa não devem se resumir ao uso de ferramentas, devendo incluir procedimentos e técnicas não oferecidas por nenhuma ferramenta conhecida.

4.3.21 A contratada não deverá alterar a integridade das informações, ou seja, não deve alterar as informações de servidores e sistemas que possam comprometer os serviços prestados pelo CFM.

4.3.22 Os serviços deverão ser executados nas dependências do CFM, de segunda à sexta, no horário das 08:00h às 18:00h.

4.3.23 O teste de invasão só poderá acontecer mediante autorização do Gerente de Infraestrutura e com anuência do Coordenador de Tecnologia da Informação.

4.3.24 Deverá ser comunicado ao Coordenador da COINF o andamento da análise, inclusive, se durante o teste de invasão encontrar alguma questão crítica.

4.3.25 Toda e qualquer modificação/alteração da configuração de um ativo no andamento do teste deve ser documentada e comunicada imediatamente, para aprovação da equipe de Infraestrutura do CFM.

APLICAÇÃO WEB

4.3.26 Esta solução consiste em analisar a segurança de software em produção, a exemplo de teste de invasão, na modalidade conhecida como “CAIXA PRETA – BLACK BOX”, nos sistemas utilizados pelo CFM, e em conformidade com as melhores práticas utilizadas pelo mercado, tais como OWASP – The Open Web Application Security Project (www.owasp.org).

4.3.27 A aplicação objeto de análise aprofundada será informada na Ordem de Serviço.

4.3.28 Para algumas aplicações, será necessário que a CONTRATANTE possua um certificado digital A3 (Token e Nuvem) – Pessoa Física - da ICP Brasil, dentro do prazo de validade, para que seja possível o acesso (login) aos sistemas. É de responsabilidade e custos da CONTRATADA a emissão do certificado digital A3.

4.3.29 O objetivo será o de verificar o comportamento dos sistemas em relação às expectativas de confidencialidade das informações trocadas nas mensagens, resistência às tentativas de burlar o controle de acesso e boa utilização de algoritmos criptográficos, entre outros. O diagnóstico de segurança das aplicações deverá incluir a avaliação do grau de confiança da aplicação nos dados oriundos do

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

usuário e possibilidade de operações de by-pass.

4.3.30 Deverão ser realizados testes de invasão dos tipos:

4.3.30.1 “Cross Site Scripting (XSS)”;

4.3.30.2 “Injeção de Código;

4.3.30.3 “Inclusão Remota de Arquivos (RFI)”;

4.3.30.4 “Referência Direta a Objetos”;

4.3.30.5 “Vazamento de informações”, onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda.

4.3.31 Exploração de bugs conhecidos tais como buffer overflow, race conditions, XSS, SQL Injection, command injection, cookie/session poisoning, CSRF, etc., para negação de serviço ou obtenção de acesso privilegiado.

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

4.3.33 Deverá ser realizado testes de invasão baseado em “Gerenciamento de Sessões”;

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

4.3.35 Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações.

4.3.36 Resistência das aplicações quanto a ataques do tipo “Man in the Middle”.

4.3.37 Níveis de risco oriundos de configurações de permissões de acesso na aplicação.

4.3.38 Possibilidade de imposição de identidade por exploração de falhas de autorização, caso existam.

4.3.39 Análise do comportamento da aplicação para averiguar se a partir de falhas de segurança na aplicação é possível interagir com recursos do sistema operacional e banco de dados que suporta a mesma.

4.3.40 Análise do comportamento da aplicação em relação aos sistemas operacionais que as abrigam procurando identificar falhas que possam ser exploradas por usuários com acesso aos sistemas, mas não autenticados pelas aplicações;

4.3.41 Outros tipos de testes técnicos de segurança da aplicação, a depender das suas características intrínsecas.

4.3.42 Entre as atividades a serem realizadas pela Contratada, referentes aos testes de segurança sobre aplicativos em produção, considera-se, no mínimo:

4.3.42.1 Desenvolver escopo detalhado, considerando objetivos e funcionalidades a serem testadas. O serviço deve incorporar, entre outras regras, as que tratem:

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.3.42.1.1 Como arquivos de malware serão utilizados para testar cada aplicativo;

4.3.42.1.2 Se a realização de cada teste será amplamente divulgada ou se será de conhecimento restrito;

4.3.42.1.3 Como consequências legais serão tratadas caso um dos resultados do teste seja a permissão de acesso não autorizado a outros aplicativos e ou conteúdo sigiloso;

4.3.42.1.4 Como a indisponibilidade (negação de serviço) pode ser prevenida se serviços ou processos forem interrompidos por uma invasão bem sucedida do teste.

4.3.43 Os serviços referentes a esta atividade poderão ser executados de forma totalmente remota, apenas se a aplicação estiver disponível na Internet. Caso a aplicação esteja disponível apenas na Intranet (localmente) da CONTRATANTE, os serviços deverão ser executados de forma local, isto é, na sede da CONTRATANTE.

4.3.44 Encontradas vulnerabilidades exploráveis, deverão ser efetuados testes de intrusão em profundidade, de forma a determinar até onde e em que condições as eventuais vulnerabilidades poderiam ser utilizadas por um eventual atacante, e a extensão prática de um ataque. Deverão ser sugeridas políticas, configurações ou ações que venham a conter ou detectar ataques de mesma natureza.

4.4 Fator de Ponderação: Métrica de Urgência e Complexidade

4.4.1 A OS deve conter o detalhamento das atividades, os prazos, a quantidade de USTs que serão consumidas e o Fator de Ponderação (FP) (complexidade x urgência), obtido a partir da multiplicação da complexidade pela urgência, como mostra o quadro a seguir:

Fator de Ponderação (FP)		**Complexidade**		
		Alta (1,5)	**Média (1,25)**	**Baixa (1,0)**
Urgência	**Alta (1,5)**	Complexidade e Urgência Alta (2,25)	Complexidade Média e Urgência Alta (1,88)	Complexidade Baixa e Urgência Alta (1,5)
	Média (1,25)	Complexidade Alta e Urgência Média (1,88)	Complexidade e Urgência Média (1,56)	Complexidade Baixa e Urgência Média (1,25)

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

	Baixa (1,0)	Complexidade Alta e Urgência Baixa (1,5)	Complexidade Média e Urgência Baixa (1,25)	Complexidade e Urgência Baixa (1)

4.4.2 Detalhamento da Urgência

Classificação	Descrição	Fator
Baixa	Quando o serviço executado será em um ativo que está em pleno funcionamento e a atividade pode ser programada	**1,0**
Média	Quando o serviço executado será em um ativo que está em funcionamento, mas a atividade deve ser realizada o mais breve possível (em até 5 dias)	**1,25**
Alta	Quando o serviço deve ser realizado imediatamente	**1,5**

4.4.3 Detalhamento da Complexidade

Classificação	Descrição	Fator
Baixa	Atividades rotineiras que requeiram configurações padronizadas e bem documentadas e não causam impacto no funcionamento do ativo	**1,0**
Média	Atividades que requeiram planejamento para execução e possam causar impacto no funcionamento do ativo	**1,25**
Alta	Atividades que causam impacto no funcionamento do ativo e requeiram a parada parcial ou total da operação para ser realizada	**1,5**

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.4.4 A remuneração da OS dar-se-á pela quantidade de USTs previstas ou realizadas (o que for de menor valor), multiplicadas pelo Fator de Ponderação.

4.4.5 Exemplo para o cálculo das USTs da Ordem de Serviço:

Ordem de serviço para *Pentest* de Rede Interna:
Urgência: Média (1,25)
Complexidade: Baixa (1)
Fator de Ponderação (FP): Média (1,25) x Baixa (1) = 1,25
Tempo previsto ou realizado para realização da Ordem de Serviço: 80 UST
Remuneração: 80 (USTs) x 1,25 (FP) = 100 USTs

4.4.6 Em caso de não atendimento quanto ao prazo e USTs planejadas, irá prevalecer o valor de USTs estabelecido na Ordem de Serviço aprovada pela CONTRATANTE para a demanda.

4.5 Fases para execução dos Testes e Entregáveis

4.5.1 Cada teste de intrusão, necessariamente, deverá seguir as seguintes fases, nesta ordem com os respectivos entregáveis:

4.5.2 Planejamento

4.5.2.1 A partir de Ordem de Serviço (OS) requisitada pela CONTRATANTE inicia-se a fase de Planejamento, quando serão apresentados e discutidos os itens constantes na OS.

4.5.2.2 Na fase de planejamento serão definidos:

4.5.2.2.1 A quantidade de UST a serem consumidas.
4.5.2.2.2 Objetivo a ser alcançado.
4.5.2.2.3 Escopo definido
4.5.2.2.4 Processos e atividades permitidas ou proibidas.
4.5.2.2.5 O detalhamento do cronograma.

4.5.2.3 Com base nos entendimentos obtidos, será realizada a reunião de kickoff para essa Ordem de Serviço.

4.5.2.4 Entregáveis dessa fase: Ata de Reunião, Abertura da Ordem de Serviço e Reunião de Kickoff.

4.5.3 Descoberta

4.5.3.1 Após formalmente autorizado pela CONTRATANTE, inicia-se a fase de Descoberta, que tem como objetivo a obtenção de informações relevantes dentro do escopo do teste que possibilitam reconhecer possíveis ameaças/vulnerabilidades. Importante frisar que esta fase não deve se restringir à

utilização de ferramentas automatizadas, sendo esperada atuação manual da equipe técnica contratada, aprofundando a análise da superfície de ataque à procura de vulnerabilidades não facilmente identificáveis.

4.5.4 Exploração

4.5.4.1 O objetivo é confirmar as vulnerabilidades e identificar os impactos e riscos das ameaças porventura encontradas a partir de simulações de ataques reais. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas no CFM, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável do COINF.

4.5.4.2 Entregáveis dessa fase: Preparação do Relatório Parcial.

4.5.5 Relatório Parcial

4.5.5.1 Após a fase de Exploração, deve ser elaborado pela CONTRATADA um relatório do teste de intrusão.

4.5.5.2 Com base nos resultados obtidos das análises, a contratada deverá elaborar um Relatório Técnico de Resultados, contendo:

4.5.5.2.1 Descrição dos cenários/ambiente de análises;

4.5.5.2.2 Escopo, tipo e modalidade do teste;

4.5.5.2.3 Fontes de pesquisa, referências, equipamentos;

4.5.5.2.4 Descrição das ferramentas e técnicas utilizadas;

4.5.5.2.5 Pontos positivos encontrados na infraestrutura de segurança/aplicação da contratante;

4.5.5.2.6 Atividades realizadas, em ordem cronológica;

4.5.5.2.7 Descrição das vulnerabilidades encontradas (inclusive as detectadas mas que não obtiveram sucesso de exploração);

4.5.5.2.8 Classificação das vulnerabilidades. Deverá ser atribuído um grau de risco quantitativo (nota numérica) e qualitativo (baixo, alto, dentre outros);

4.5.5.2.9 Avaliação dos riscos associados, bem como procedimentos para saná-las ou limitá-las (plano de ação com priorização);

4.5.5.2.10 Tipos de ataques realizados;

4.5.5.2.11 Sugestões a manutenção e incremento da proteção da vulnerabilidade;

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.5.5.2.12 Apresentar as evidências dos testes (prints, filmagens, vídeos, logs e etc.);

4.5.5.2.13 Assinatura do profissional certificado.

4.5.5.3 Deverá ser realizado uma apresentação Técnica do relatório parcial, nas dependências do CONTRATANTE ou de forma Remota.

4.5.5.4 Esta apresentação terá duração de uma a quatro horas e terá o objetivo de apresentar o resultado do *Pentest*, formas de correção de vulnerabilidades e elucidar dúvidas porventura existentes por parte da equipe responsável do CFM.

4.5.5.5 O seminário deverá conter, no mínimo:

4.5.5.5.1 Descrição do ambiente e do escopo do pentest;

4.5.5.5.2 Pontos positivos e negativos encontrados na infraestrutura de segurança/aplicação da contratante;

4.5.5.5.3 Descrição das vulnerabilidades encontradas (inclusive as detectadas mas que não obtiveram sucesso de exploração), avaliação dos riscos associados, bem como procedimentos para saná-las ou limitá-las (plano de ação com priorização levando em consideração a criticidade das vulnerabilidades encontradas);

4.5.5.5.4 Resultados efetivos das análises, testes e ataques;

4.5.5.5.5 Sugestões para a manutenção e incremento da proteção;

4.5.5.6 Entregáveis dessa fase: Relatório Parcial, realização da apresentação técnica e entrega dos arquivos .doc/.ppt/.pptx.

4.5.6 Reteste

4.5.6.1 Conforme prazos estipulados, o CFM realizará as correções necessárias para as vulnerabilidades porventura encontradas e demonstradas através do Relatório Parcial do *Pentest*, sendo necessário canal de comunicação direta em horário comercial com a **CONTRATADA** para suporte técnico referente a informações e dúvidas que surgirem durante o decorrer do período.

4.5.6.2 Após as correções das vulnerabilidades porventura encontradas (atividade esta, sob responsabilidade do CFM conforme cronograma estipulado) e expressa autorização pela equipe técnica da COINF, a CONTRATADA realizará um novo teste, considerando os seguintes itens:

4.5.6.2.1 Serão testados os mesmos ativos ou sistemas requisitados na OS, seguindo as mesmas definições da fase de planejamento sem, no entanto, realizar a descoberta de novas informações relativas à superfície

de ataque;

4.5.6.2.2 O objetivo é verificar se a equipe técnica do CFM realizou o tratamento das vulnerabilidades anteriormente encontradas, a partir da confirmação de que estas não mais existem ou não podem mais ser exploradas.

4.5.6.3 Quando da realização do Reteste, caso surjam novas vulnerabilidades encontradas pela CONTRATADA, estas deverão ser mencionadas no Relatório Final do Teste, com as devidas sugestões de correção. A realização do Reteste esgota-se, porém, na primeira realização, sendo novas vulnerabilidades tratadas em novas Ordens de Serviço, a critério da equipe técnica do CFM.

4.5.6.4 Entregáveis dessa fase: Ações corretivas das vulnerabilidades pelo CFM e um novo teste seguindo os mesmos testes definidos na fase de planejamento.

4.5.7 Seminário de Apresentação e Entrega do relatório Final

4.5.7.1 Após a aplicação do reteste, será elaborado pela CONTRATADA um Relatório Final do *Pentest*, que conterá as mesmas informações do Relatório parcial, acrescidas dos resultados encontrados após a realização do Reteste. A CONTRATADA então apresentará Seminário a ser realizado de forma presencial nas dependências do CFM ou por meio de vídeo conferência, a critério da CONTRATANTE.

4.5.7.2 O Seminário deverá conter:

4.5.7.2.1 Apresentação e discussão do Relatório Final;

4.5.7.2.2 Apresentação de pontos positivos e negativos encontrados no *Pentest*;

4.5.7.2.3 Descrição das vulnerabilidades encontradas (inclusive as detectadas mas que não obtiveram sucesso de exploração), avaliação dos riscos associados, bem como procedimentos para saná-las ou limitá-las (plano de ação com priorização levando em consideração a criticidade das vulnerabilidades encontradas);

4.5.7.2.4 Resultados efetivos das análises, testes e ataques.

4.5.7.3 O relatório Final será elaborado e apresentado pela CONTRATADA em seminário agendado entre as partes, conforme cronograma, de forma presencial ou virtual, a critério do CFM. Todas as informações relacionadas ao teste, incluindo o próprio relatório, serão fornecidas de maneira segura pela

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

CONTRATADA. O referido Seminário de Apresentação do Relatório Final terá duração de uma a quatro horas e deverá ter a presença de, no mínimo, um representante da CONTRATADA integrante da equipe operacional responsável pela realização do teste de invasão.

4.5.7.4 Entregáveis dessa fase: Relatório Final do *Pentest* e realização do Seminário com a apresentação do Relatório Final.

4.5.8 Atividades de apoio

4.5.8.1 Para auxílio das atividades, poderão a critério da Contratante, ser solicitado à Contratada, os seguintes documentos de apoio:

4.5.8.1.1 Plano de trabalho com o detalhamento do escopo dos testes e cronograma de execução;

4.5.8.1.2 Apresentação inicial das ações a serem aplicadas pela contratada;

4.5.8.1.3 Relatórios de acompanhamento semanais do plano de trabalho;

4.5.8.1.4 Reuniões de status report ou checkpoint.

4.6 Requisitos de Prazo

4.6.1 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.

4.6.2 Seguem os **prazos máximos** para cada atividade para os testes:

PRAZOS PARA AS ATIVIDADES			
Atividade	**Prazo Estimado**	**Responsabilidade**	**Entregáveis**
Fase de Planejamento Reunião Inicial e abertura de ordem de serviço (OS)	1 a 5 dias	Contratada e CFM	1. Ata de Reunião 2. Abertura de OS 3. Reunião de Kickoff
Fase de Descoberta e Exploração Realização do *Pentest* e Entrega do Relatório Parcial	6 a 20 dias	Contratada	4. Relatório técnico Parcial dos resultados - Evidência dos testes e resultados 5. Entrega dos arquivos .doc/.ppt/.pptx

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

			6. Realização da apresentação Técnica
Ações corretivas das Vulnerabilidades	21 a 51 dias	CFM	7. Ações corretivas das Vulnerabilidades
Reteste	52 a 62 dias	Contratada	8. Reteste (Novo teste seguindo os mesmos testes definidos na fase de planejamento)
Realização do Seminário de Apresentação e Entrega do Relatório Final do *Pentest*	63 a 70	Contratada	9. Relatório técnico Final dos resultados 10. Seminário de Apresentação e Entrega do Relatório Final do *Pentest*

4.6.3 O prazo máximo para a CONTRATANTE aplicar correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório técnico “Teste de Invasão” será de 30 dias contados a partir do final da “Reunião para apresentação do relatório parcial de recomendações e descrição das atividades executadas durante o teste”. Esses 30 dias estão embutidos no prazo máximo de 70 dias para cumprimento da OS.

4.6.4 Este Cronograma de Atividades servirá como referência, podendo ser ajustado entre as partes na fase de Planejamento, não sendo permitido, porém, exceder o prazo máximo de 70 (setenta) dias para cada ocorrência de *Pentest*.

4.6.5 Em caso de descumprimento de prazo das ações corretivas de vulnerabilidades por parte do CFM e de forma a não prejudicar o cumprimento do cronograma a **CONTRATADA** poderá, desde que autorizada pela equipe técnica do CFM, dar início à fase de Reteste ou de Realização do Seminário de Apresentação e entrega do Relatório Final do *Pentest*, considerando apenas as informações do Relatório Parcial.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.7 Requisitos de Aceite

4.7.1 A quantidade de USTs utilizadas na O.S. deverão estar evidenciadas no Relatório Final de *Pentest*. Para cada fase da atividade deve conter a quantidade de UST.

4.7.2 A emissão do Termo de Recebimento está condicionada à entrega da atividade de Realização do Seminário de Apresentação e Entrega do Relatório Final do *Pentest*.

4.7.3 A emissão do Termo de Aceite condiciona-se à:

- Existência do Termo de Recebimento;
- Ateste das USTs efetivamente utilizadas para a execução completa da O.S.;
- Atender a todos os requisitos constantes na contratação.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.8 Requisitos de Formação da Equipe

4.8.1 A seguir estão relacionadas exigências de perfis dos profissionais que executarão os serviços 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.

4.8.2 Este item define os perfis dos profissionais das equipes da CONTRATADA que manterão relacionamento direto com a CONTRATANTE. Outros perfis poderão ser agregados às equipes a critério da CONTRATADA.

4.8.3 A CONTRATADA se compromete a alocar, em todos os serviços contratados pelo Conselho Federal de Medicina, profissionais com perfis e qualificações adequados, mantendo ao longo da vigência do contrato todas as condições que apresentaram em sua habilitação e qualificação no processo licitatório.

4.8.4 A CONTRATADA deverá selecionar, designar e manter profissionais cuja qualificação esteja em conformidade com os tipos de serviços contido na Ordem de serviço.

4.8.5 A CONTRATADA deverá alocar profissionais especialistas a fim de atender ao escopo do serviço contemplado neste certame.

4.8.6 A CONTRATADA se compromete a garantir a alocação de profissionais devidamente capacitados para solucionar problemas relacionados à prestação de serviços, incluindo os que exijam a presença física nas dependências do Conselho Federal de Medicina.

4.8.7 A CONTRATADA deverá indicar um preposto e um substituto, que será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder às questões legais e administrativas referentes ao andamento contratual.

PREPOSTO – Preposto do contrato	
Responsável por executar a gestão geral do contrato por parte da CONTRATADA, com a visão de todas as Ordens de Serviço em desenvolvimento, objetivando garantir a execução dos serviços dentro dos prazos estabelecidos e atendendo todos os requisitos de qualidade; Providenciar pronta resposta formal a todas as solicitações de esclarecimentos feitas pelo Gestor e/ou Fiscais do contrato; Participar periodicamente, a critério do Conselho Federal de Medicina, de reuniões de acompanhamento das atividades referente às OS em execução, em ambiente de interesse e com representantes do Conselho Federal de Medicina; Levar para as reuniões periódicas de acompanhamento, as situações não resolvidas em nível de gerência das OS.	
Experiência/Qualificação	**Modo de Comprovação**

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

Experiência em Gestão de contratos	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	**Modo de Comprovação**
Diploma de graduação na área de Tecnologia da Informação, devidamente reconhecido; ou Diploma de graduação em outro curso superior, acompanhado de diploma/certificação de Curso de Pós-Graduação na área de Tecnologia da Informação	Diploma de graduação na área de Tecnologia da Informação, devidamente reconhecido; ou Diploma de graduação em outro curso superior, acompanhado de diploma/certificação de Curso de Pós-Graduação na área de Tecnologia da Informação, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

RES – Responsável Técnico	
Responsável técnico por realizar as atividades relacionadas ao Pentest.	
Experiência/Qualificação	**Modo de Comprovação**
Experiência mínima de 02 (dois) anos em teste de intrusão	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	**Modo de Comprovação**
Curso superior completo na área de Tecnologia da Informação.	Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.
Profissional com pelo menos uma das seguintes certificações: • Global Information Assurance Certification (GIAC) Penetration Tester (GPEN); • GIAC Exploit Researcher and	

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

Advanced Penetration Tester (GXPN); • Offensive Security Certified Professional (OSCP). • PMP com ISO 27.002	

4.9 Requisitos de Experiência Profissional

4.9.1 Com o objetivo de garantir a qualidade dos serviços prestados, a assinatura do CONTRATO está condicionada a apresentação pela CONTRATADA de pelo menos 1 (um) profissional que esteja alocado para a prestação dos serviços, que possua pelo menos 2 (duas) das certificações listadas abaixo:

4.9.1.1 EC-Council Certified Ethical Hacker (CEH);
4.9.1.2 ECSA – EC-Council Certified Security Analyst;
4.9.1.3 EC-Council Licensed Penetration Tester (LPT) Master;
4.9.1.4 IACRB Certified Penetration Tester (CPT);
4.9.1.5 Certified Expert Penetration Tester (CEPT);
4.9.1.6 Certified Penetration Testing Expert (CPTE);
4.9.1.7 Certified Penetration Testing Specialist (CPTS);
4.9.1.8 Certified Mobile and Web Application Penetration Tester (CMWAPT);
4.9.1.9 Certified Red Team Operations Professional (CRTOP);
4.9.1.10 CompTIA PenTest +;
4.9.1.11 Global Information Assurance Certification (GIAC) Penetration Tester (GPEN);
4.9.1.12 GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);
4.9.1.13 Offensive Security Certified Professional (OSCP);
4.9.1.14 Certified Information Security Manager (CISM);
4.9.1.15 Certified Information Systems Security Professional (CISSP);
4.9.1.16 CompTIA Security+ (SY0-301);
4.9.1.17 CSSLP – Certified Secure Software Lifecycle Professional;
4.9.1.18 ECSA – EC-Council Security Analyst.

NOTA:
As certificações exigidas neste documento são aplicadas por entidades reconhecidas internacionalmente e possuem alto nível de exigência para aprovação. Tal nível de exigência garante minimamente que os profissionais aprovados possuem os requisitos necessários à prestação dos serviços descritos neste documento.

4.9.2 A CONTRATADA deverá apresentar, na execução dos serviços a lista

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

dos profissionais, com seus currículos e a comprovação da exigência de certificação acima, suas responsabilidades em cada etapa (testes externos, testes internos e análise de aplicações web), nas quais atuarão on-site (no CFM durante os testes INTERNOS) e quais atuarão remotamente e, por fim, a comprovação de seu vínculo empregatício com a CONTRATADA.

4.9.3 O Responsável Técnico deverá, durante as análises e testes, realizar de forma presencial ou remota, reuniões de checkpoint / status report para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE.

4.9.4 Ficam vedadas a subcontratação total e parcial, bem como a cessão, a transferência e a dação em garantia deste CONTRATO.

4.9.5 O descumprimento desta Cláusula ensejará a rescisão do Contrato, bem como sujeitará a Contratada às sanções estabelecidas no Contrato.

4.10 Requisitos de local de atendimento

4.10.1 O local de execução dos serviços será preferencialmente nas instalações da CONTRATADA, entretanto, para as atividades, que a critério do CONTRATANTE, necessitem de maior e frequente interação com os colaboradores e usuários da solução, a exemplo de reuniões para levantamento, detalhamento de requisitos, validação de artefatos, homologação de sistemas, entre outras, podem ser executadas nas instalações da CONTRATANTE ou em unidade regional designada por esta, sob a supervisão da COINF e em observância de seus horários de expediente.

4.10.2 O Conselho Federal de Medicina disponibilizará local de trabalho quando os serviços forem executados em suas dependências, cabendo à CONTRATADA prover os equipamentos e demais condições para que seus colaboradores tenham plenas condições de trabalho.

4.10.3 A CONTRATANTE desobriga-se de qualquer ressarcimento à CONTRATADA referente aos custos de hospedagem, transporte, alimentação e deslocamento e afins de seus colaboradores quando for necessário o deslocamento de sua equipe.

4.11 Requisitos de Garantia ou níveis mínimos de serviços exigidos

4.11.1 A garantia para os serviços de cada OS será obrigatória, e seu prazo será de, no mínimo, 3 (três) meses, a contar da data do ANEXO IV - Termo de Aceite do serviço (TA), emitido pelo Conselho Federal de Medicina.

4.11.2 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.

4.11.3 Durante o prazo de garantia, todos os eventuais erros ou falhas identificadas deverão ser corrigidos pela CONTRATADA, sem ônus para o Conselho Federal de Medicina.

4.11.4 Até o final do período contratado, a **CONTRATADA** deverá atender, as solicitações de dúvidas dos pentests realizados.

4.11.5 Caso a equipe técnica do CFM entenda haver algum risco na execução do *Pentest* que possa comprometer, em qualquer grau, o funcionamento de sistema, ativo ou processo do CFM, poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do horário comercial.

4.11.6 Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável do CFM.

4.11.7 O direito do Conselho Federal de Medicina à garantia de um serviço cessará caso o artefato envolvido nesse serviço seja alterado pelo Conselho Federal de Medicina ou por outros fornecedores a serviço da instituição.

4.11.8 Em caso de a própria CONTRATADA realizar manutenções no artefato, permanecerá o direito do Conselho Federal de Medicina à garantia.

4.11.9 O prazo de garantia deverá ser respeitado pela CONTRATADA mesmo após o término do prazo de vigência do contrato.

4.11.10 O prazo máximo para correção de defeitos não poderá ser superior a 20% (vinte por cento) do prazo definido na Ordem de Serviço (OS).

4.11.11 O descumprimento do referido prazo fica sujeito à advertência e à multa nos termos definidos no edital.

4.12 Requisitos Técnicos (vistoria técnica)

4.12.1 As licitantes DEVERÃO realizar vistoria técnica junto ao CFM, para o devido conhecimento e uniformização de entendimento quanto às condições para a prestação dos serviços objeto deste Termo de Referência e dirimir eventuais dúvidas sobre o parque tecnológico do CFM que foi omitido por questões de segurança.

4.12.2 A visita tem por finalidade avaliar as condições das instalações e infraestrutura de TI do CFM, visando ter a extensão do que é pedido no objeto deste Termo de Referência, posto que somente a descrição técnica não se faz suficientemente clara para determinar as grandezas e complexidade que serão envolvidas para suas

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

manutenções e, consequentemente, assegurem que o preço ofertado pela licitante seja compatível com as reais necessidades do CONTRATANTE (Acórdão TCU nº 727/2009-Plenário).

4.12.3 A vistoria técnica deverá ocorrer em dias úteis na sede do CFM localizada no SGAS 915 Lote 72 Asa Sul – Brasília DF ou de forma online, através da ferramenta Zoom. Vistoria Técnica será realizada mediante agendamento prévio, dentro do horário de expediente em dias úteis, das 09:00 às 12:00 horas e das 13:00 às 17:00 horas, pelo e-mail cluiz@portalmedico.org.br ou pelo telefone (61) 3445-5966.

4.12.4 A vistoria será acompanhada (presencial ou on-line) por representante do CFM, designado para esse fim.

4.12.5 A vistoria poderá ser feita em até 01 (um) dia útil anterior à data do certame.

4.12.6 Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.12.7 Após sua realização será emitida a Declaração de Vistoria Técnica pela área de licitações e contratos.

4.12.8 A Declaração de Vistoria Técnica constante no Anexo I, deverá ser devidamente preenchida, e assinada pelo responsável técnico do interessado, comprovando que a empresa tomou conhecimento de todas as informações necessárias para a execução do objeto licitado, bem como vistoriou o ambiente tecnológico do CFM. Este termo será lavrado em 2 (duas) vias e entregue uma delas ao interessado.

4.12.9 A ausência do Termo de Vistoria, na documentação de habilitação do LICITANTE, incorrerá na sua desclassificação do certame.

4.12.10 Os licitantes não poderão alegar o desconhecimento das condições e grau de dificuldade existentes no ambiente tecnológico do CFM como justificativa para se eximirem das obrigações assumidas em decorrência do contrato.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

4.13 Requisitos de Metodologia de Trabalho

4.13.1 Integrantes da equipe de fornecimento que forem considerados, pelo CONTRATANTE, desnecessários para a atividade, deverão ser substituídos, caso seja solicitado.

4.13.2 Os serviços fornecidos serão submetidos, eventualmente, a testes de segurança a serem realizados pelo CFM ou pelo seu representante contratado para este fim.

4.13.2.1 Os testes considerarão todo o ecossistema no qual a solução de TIC será instalada e operacionalizada a fim de que a simulação se dê em um ambiente o mais realista o possível.

4.13.2.2 O fornecedor responderá somente pelos componentes da solução de TIC ofertada, e deverá assegurar que os serviços fornecidos sejam capazes de aplicar um modelo de segurança adequado, mesmo que as outras camadas que façam uso da solução de TIC, falhem.

4.14 Outros Requisitos Aplicáveis

4.14.1 Os serviços prestados já deverão incluir todos os equipamentos, *softwares*, licenças e *hardwares* necessários para sua completa execução, atendendo a todos os requisitos especificados no objeto deste Termo.

4.15 Requisitos Temporais

4.15.1 Para o fiel cumprimento das obrigações, será lavrado contrato de prestação de serviços a ser celebrado entre as partes, com vigência de 24 (vinte e quatro) meses, a contar da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos por termos aditivos, até o limite de 60 (sessenta) meses, após verificação da real necessidade e com vantagens à Administração Pública, conforme o inciso II do art. 57 da Lei nº 8.666/93.

4.15.2 A licitante vencedora será convocada pela CONTRATANTE para assinar o contrato, tendo o prazo de 05 (cinco) dias úteis, contados do recebimento da notificação, para comparecer à administração, sob pena de decair o direito à contratação, sem prejuízo das penalidades previstas.

4.15.3 A recusa injustificada da referida licitante em assinar o contrato no prazo acima estabelecido, caracteriza o descumprimento total da obrigação, sujeitando-se às sanções legalmente cabíveis.

4.15.4 As Ordens de Serviço abertas no último dia do contrato deverão ser atendidas, mesmo que o prazo da atividade de seu atendimento perdure após esse período.

4.15.5 Após a assinatura do contrato, o fornecedor deve iniciar suas

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

atividades em até 10 (dez) dias, apresentando-se ao CONTRATANTE com sua equipe e pronta para receber demandas.

4.16 Requisitos de Segurança da Informação

4.16.1 Os serviços fornecidos deverão atender às normas e padrões previstos:

4.16.1.1 Na Política de Segurança da Informação (PSI) do CFM;

4.16.1.2 Na Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

4.17 Requisitos de Segurança

4.17.1 Na ocorrência da prestação de serviços presenciais, os representantes do fornecedor deverão:

4.17.1.1 Utilizar crachás de identificação da empresa;

4.17.1.2 Cumprir com os protocolos de identificação e de garantia de acesso físico ao Conselho Federal de Medicina;

4.17.1.3 Em caso de pandemia, cumprir com todos os protocolos de prevenção estabelecidos pela Casa, tais como o uso de máscara, álcool gel, distanciamento mínimo, *etc*.

4.18 Requisitos Sociais, Ambientais e Culturais

Os canais de atendimento, suporte técnico e garantia deverão estar disponíveis em Português do Brasil.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

5.1.1 Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato.

5.1.2 Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência.

5.1.3 Receber o objeto fornecido pela CONTRATADA que, conforme as inspeções realizadas, esteja em conformidade com a proposta aceita.

5.1.4 Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

5.1.5 Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato.

5.1.6 Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o provimento dos serviços de TIC.

5.1.7 Definir produtividade ou capacidade mínima de provimento dos serviços de TIC por parte da CONTRATADA, com base em pesquisas

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

de mercado, quando aplicável.

5.1.8 Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual pertençam à Administração.

5.1.9 Realizar, periodicamente, testes de Segurança da Informação nos serviços prestados.

5.2 Deveres e responsabilidades da CONTRATADA

5.2.1 Indicar formalmente preposto apto a representá-lo junto à CONTRATANTE, que deverá responder pela fiel execução do contrato.

5.2.2 Atender, prontamente, a quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

5.2.3 Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante.

5.2.4 Caso alguma vulnerabilidade grave e/ou de fácil exploração seja encontrada no decorrer do teste, a CONTRATADA será responsável pela comunicação imediata do risco à equipe do CFM responsável pelo acompanhamento do teste. Informações técnicas deverão ser enviadas de forma segura em até um dia útil.

5.2.5 Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar as demandas, de forma total ou parcial, em qualquer tempo, sempre que considerar a medida necessária.

5.2.6 Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

5.2.7 Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para o provimento dos serviços de TIC.

5.2.8 Manter a produtividade ou a capacidade mínima de provimento dos serviços de TIC durante a execução do contrato, conforme expectativa acordada previamente entre a CONTRATANTE e a CONTRATADA, e os níveis de serviços descritos no contrato.

5.2.9 Disponibilizar os meios de contato para atendimento ao cliente e comunicar a CONTRATANTE sempre que houver mudanças nesses canais.

5.2.10 Comunicar ao Conselho Federal de Medicina, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução do contrato.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

5.2.11 Manter seus funcionários ou representantes credenciados devidamente identificados quando da execução de qualquer serviço no Conselho Federal de Medicina, referente ao objeto contratado, observando as normas de segurança (interna e conduta).

5.2.12 Assumir total responsabilidade pelo sigilo da informação que seus empregados ou prepostos vierem a obter em função dos serviços prestados, respondendo pelos danos que eventual vazamento de informação, decorrentes de ação dolosa, imperícia, negligência ou imprudência, venham a ocasionar ao Conselho Federal de Medicina ou a terceiros.

5.2.13 Cooperar com a realização dos testes de Segurança da Informação, prestando todas as informações e providenciando recursos humanos, tecnológicos e quaisquer outros requeridos para sua plena execução.

5.2.14 Corrigir, diretamente ou por intermédio do fabricante do produto, quaisquer brechas de segurança detectadas na solução de TIC fornecida, mediante testes ou pela ocorrência de incidentes, sem ônus à CONTRATANTE.

5.3 Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

5.3.1 Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços.

5.3.2 Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados.

5.3.3 Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3.1 As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, *e-mail*, ou sistema informatizado, quando disponível;

5.3.3.2 A definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.

5.3.4 Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.4.1 A definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.4.2 As regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada;

5.3.4.3 As regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de

Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1 Execução dos serviços

6.1.1 Os Testes de Invasão serão demandados pelo Gerente de Infraestrutura e pelo Gerente de Sistema da COINF do CFM.

6.1.2 Os serviços serão solicitados sob demanda por meio de ordem de serviço, a ser emitida pelo CFM.

6.2 Fluxo Básico

6.2.1 Para a contratação dos serviços o Conselho Federal de Medicina encaminhará para a CONTRATADA, devidamente preenchido, o ANEXO III - Solicitação de Atendimento e demais documentos de apoio que julgar necessário.

6.2.2 Caso os dados na Solicitação de Atendimento sejam insuficientes para o entendimento da solução pretendida e estimativa preliminar de esforço e de prazo, a CONTRATADA pode solicitar mais esclarecimentos até que as dúvidas sejam sanadas.

6.2.3 A CONTRATADA deverá encaminhar ao Setor de Tecnologia da Informação, no prazo máximo de 5 (cinco) dias úteis do recebimento do ANEXO III - Solicitação de Atendimento, um Anteprojeto – ANEXO VI.

6.2.4 O escopo dos serviços deverá ser acordado entre o CFM 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.

6.2.5 A CONTRATANTE avaliará o Anteprojeto e poderá solicitar uma apresentação técnica para a CONTRATADA a fim de assegurar seu entendimento do escopo da demanda e justificar as métricas de esforço e prazo.

6.2.6 Cabe a CONTRATANTE o parecer final a respeito do escopo, prazo e esforço indicado no anteprojeto.

6.2.7 A solicitação para início da execução dos serviços ocorrerá por meio do ANEXO VII - Ordem de Serviço (OS), assinada por profissional do Conselho Federal de Medicina, formalmente designado para isso, e somente após este passo a CONTRATADA está autorizada a trabalhar na demanda.

6.2.8 A Ordem de Serviço (OS) contempla a descrição do serviço, o conjunto de atividades, artefatos a serem entregues, esforço, prazo para execução do serviço, especificações técnicas do serviço.

6.2.9 A CONTRATADA não poderá recusar a execução de nenhuma OS sob

pena de incorrer em inexecução parcial, porém poderá questionar e solicitar adequações na OS, desde que coerentes ao planejamento do serviço, ao CONTRATO e ao TERMO DE REFERÊNCIA, para garantir que a expectativa da CONTRATANTE seja atendida em termos de qualidade, prazo e escopo. Sempre cabendo à CONTRATADA acatar ou não as requisições da CONTRATADA.

6.2.10 Caso ocorram mudanças de escopo em demandas previamente autorizadas (OS com execução autorizada) cujo serviço esteja em andamento, a CONTRATADA deve realizar uma análise de impacto e apresentá-la à CONTRATANTE com as justificativas da mudança a fim de buscar nova aprovação e o devido ajuste de escopo, prazo e remuneração.

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

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

6.2.13 Os serviços deverão estar sempre de acordo com as especificações constantes nas OS.

6.2.14 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 CONTRATANTE, e ao término da execução - com o fornecimento dos respectivos relatórios pela CONTRATADA e atesto dos mesmos pelos respectivos responsáveis.

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

6.2.16 Caso o trabalho ultrapasse a quantidade de USTs estimadas, o CFM deverá ser informado imediatamente que deliberará sob a nova quantidade estimada.

6.2.17 O Termo de Recebimento de Serviço (TR) será o instrumento utilizado para atestar as entregas parciais de uma Ordem de serviço e pode apresentar as seguintes condições:

- **Entrega rejeitada** - quando o(s) artefato(s) entregue(s) não for(em) aceito(s) pelo Conselho Federal de Medicina sujeitando a CONTRATADA às penalidades estabelecidas no contrato. O Conselho Federal de Medicina deverá elencar os motivos pela qual está rejeitando os artefatos.
- **Entrega recebida** - quando o(s) artefato(s) entregue(s) for(em) recebidos integralmente pelo Conselho Federal de Medicina, não cabendo nenhum ajuste.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

- **Entrega recebido com ajustes pendentes** - quando o(s) artefato(s) entregue(s) for(em) recebido(s), entretanto, sem atender integralmente alguma condição presente na Ordem de Serviço. Neste caso o Conselho Federal de Medicina apresentará à CONTRATADA uma relação de ajustes a serem realizados, com prazo para adequação e reapresentação. Caso a CONTRATADA não os realize integralmente no prazo estabelecido, o artefato ou conjunto de artefatos será considerado rejeitado e a empresa estará sujeita às penalidades previstas para o caso.

6.2.18 Uma vez que a CONTRATADA obtenha todos os Termos de Recebimento de Serviço das entregas que compõem a Ordem de Serviço, denotando que todos os produtos estão avaliados e aprovados, e os serviços concluídos, a CONTRATANTE emitirá o Termo de Aceite (TA), o qual atesta a aceitação ou homologação do produto ou serviço contratado, caracterizando o final do serviço, objeto da OS e habilitando o pagamento à CONTRATADA.

6.2.19 O Termo de Aceite do Serviço somente será considerado válido após a assinatura de representante da área demandante do Conselho Federal de Medicina.

6.2.20 O Ateste definitivo do serviço se dará em até 10 (dez) dias corridos após a apresentação e entrega do relatório técnico e apresentação técnica citados neste Termo de Referência, pela CONTRATADA.

6.3 Ordem de Serviço (O.S)

6.3.1 A Ordem de Serviço (OS) formaliza a autorização de atendimento ao CONTRATADO, e será emitida por ferramenta definida entre o Conselho Federal de Medicina e a CONTRATADA.

6.3.2 Em caso extraordinário de indisponibilidade da ferramenta do Conselho Federal de Medicina ou da CONTRATADA, o acionamento da CONTRATADA poderá se dar por telefone ou e-mail desde que sob demanda do fiscal do contrato. Assim que o impedimento técnico for superado, a abertura formal da OS se dará normalmente sem prejuízo ao prazo de atendimento.

6.3.3 Durante a execução da demanda, a CONTRATADA poderá registrar na ferramenta de atendimento pendências do CFM e/ou impedimentos ao atendimento do serviço que indiquem risco ao cumprimento do prazo da OS. Estes casos serão analisados pela CONTRATADA, e, se julgados procedentes, podem autorizar o replanejamento das entregas do serviço.

6.3.4 Nas O.S. deverão ser contemplados, no mínimo, os seguintes tópicos (escopo):

6.3.4.1 O sistema ou ativo de tecnologia a ser testado;

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

6.3.4.2 A modalidade de *pentest* a ser realizado (Black Box, Grey Box, White Box);

6.3.4.3 Tipo de realização do *pentest* (*Pentest* Interno, Externo ou Aplicação WEB).

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

6.3.6 Para efeito de cálculo de UST da O.S, serão consideradas apenas as USTs utilizadas pelo(s) analista(s) da CONTRATADA nas fases de Descoberta, Exploração, Reteste e Elaboração de Relatórios (Parcial e Final) dos *Pentests*.

6.3.7 Não deverão ser consideradas as USTs utilizadas para execução de ferramentas automatizadas, exceto em ferramenta que há necessidade de monitoramento em dar algum input para dar andamento ao teste ou até mesmo corrigir a sua execução.

6.3.8 As USTs remanescentes de O.S que não tenham atingido o total de USTs previstas, poderão ser realocadas para Ordens de Serviço futuras.

6.3.9 As demandas contidas numa Ordem de Serviço (OS) poderão, a qualquer tempo, ser alterados, suspensos ou cancelados pelo Conselho Federal de Medicina. Nestes casos, se formalizadas até antes do início de execução dos serviços, não acarretará qualquer ônus para a CONTRATANTE.

6.3.10 Caso a solicitação de cancelamento ocorra após seu início de execução, a CONTRATANTE arcará com os custos proporcionais da CONTRATADA até o momento da formalização. Após a formalização da CONTRATANTE que a ordem de serviço foi cancelada, a CONTRATATA enviará para a CONTRATANTE um relatório com os custos incorridos para a CONTRATANTE. Após a avaliação e aprovação pela CONTRATANTE, que providenciará o devido pagamento.

6.3.11 No caso de solicitação de mudança com origem na CONTRATANTE ou na CONTRATADA. Deve, a CONTRATADA, realizar uma análise de impacto e apresentá-la à CONTRATANTE com as justificativas da mudança, a fim de buscar nova aprovação e o devido ajuste de escopo, prazo e remuneração.

6.3.12 Caso o trabalho ultrapasse a quantidade de USTs estimadas, o CFM deverá ser informado imediatamente que deliberará sob a nova quantidade estimada.

6.3.13 O CONTRATANTE reserva-se o direito de cancelar sumariamente o serviço solicitado que teve a entrega rejeitada sistematicamente pela falta de qualidade, inobservância dos padrões estabelecidos ou

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

descumprimento do prazo necessário.

6.3.14 A rejeição e o consequente cancelamento da OS pelos motivos anteriores implicará no reembolso ao CONTRATANTE dos valores pagos até o momento do cancelamento, sem prejuízo da aplicação das sanções administrativas previstas no contrato e/ou responsabilização por eventuais prejuízos decorrentes.

6.4 Termo de Recebimento e Termo de Aceite do Serviço

6.4.1 Será considerado recebido e aceito o serviço que estiver em plena conformidade com as especificações e critérios estabelecidos na OS.

6.4.2 O Termo de Recebimento de Serviço (TR) é o instrumento que atesta as entregas parciais e o Termo de Aceite (TA), por sua vez, a conclusão de todos os serviços que compõem a OS.

6.4.3 Os serviços entregues com padrão de qualidade inferior ao esperado ou além do prazo previsto submete a CONTRATADA às penalidades previstas neste documento.

6.4.4 A CONTRATANTE terá até 25% (vinte e cinco por cento) do prazo utilizado para execução do serviço, a contar da data da entrega, para realizar a sua validação/homologação e emitir o TR. Findado o maior dos períodos, emitirá o TR por decurso de prazo.

6.4.5 A CONTRATANTE terá até 25% (vinte e cinco por cento) do prazo de execução total da OS, a contar da emissão do último TR, ou 15 dias úteis, para a verificação da OS e emissão do TA. Findado o maior dos períodos, emitirá o TA por decurso de prazo.

6.4.6 A emissão do TR ou TA por decurso de prazo autoriza o pagamento, mas não dá por aceita a entrega, cabendo emissão posterior do TR ou TA definitivo ou a rejeição e consequente devolução do serviço à CONTRATADA para ajustes, não eximindo a CONTRATADA de executar a transferência de conhecimento.

6.4.7 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.

6.5 Condições de aceite

6.5.1 O Relatório Final de cada teste realizado deverá atender aos requisitos elencados neste Edital.

6.5.2 A quantidade de USTs utilizadas na O.S. deverão estar evidenciadas no Relatório Técnico de *Pentest*.

6.5.3 Ateste das USTs efetivamente utilizadas para a execução completa da O.S.

6.5.4 Atender a todos os requisitos constantes na contratação.

6.5.5 O Termo de Aceite não exclui a responsabilidade civil pela solidez e a

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

segurança dos serviços, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou contrato.

6.6 Quantidade mínima de bens ou serviços para comparação e controle

6.6.1 A contratação será mediante o consumo de USTs sendo utilizadas **sob demanda**, de forma planejada, com escopo previamente definido e combinado com a CONTRATANTE.

6.7 Mecanismos formais de comunicação

6.7.1 A CONTRATADA se obriga a disponibilizar, em até 10 (dez) dias a contar da assinatura do contrato, sem custo adicional para a CONTRATANTE, os seguintes canais de atendimento: telefone, e-mail, ferramenta de acompanhamento dos serviços e central para acionamento das ocorrências de pronto atendimento.

6.7.2 Os canais e-mail e ferramenta de acompanhamento deverão prever recepção e tratamento diferenciado das OS, por tipo de serviço, e a possibilidade de acompanhamento pela CONTRATANTE de todo o processo de atendimento.

6.8 Manutenção de Sigilo e Normas de Segurança

6.8.1 O direito patrimonial, de propriedade intelectual e autoral dos produtos gerados em decorrência da execução do objeto serão de exclusiva e permanente propriedade do CFM, constituindo segredo comercial, ficando a CONTRATADA impedida, sob pena da lei, de utilização para outros fins que não aqueles previstos no contrato.

6.8.2 A contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.8.3 A CONTRATADA deverá tomar todas as medidas cabíveis para que seus empregados cumpram estritamente a obrigação por ela assumida.

6.8.4 A CONTRATADA obriga-se a tratar como "segredos comerciais e confidenciais", quaisquer informações, dados, processos, fórmulas, códigos, fluxogramas, diagramas lógicos, dispositivos e modelos relativos aos serviços ora contratados, utilizando-os apenas para as finalidades previstas neste ajuste, não podendo revelá-los ou facilitar a sua revelação a terceiros.

6.8.5 A CONTRATADA deverá obedecer aos critérios, padrões, normas operacionais adotados pelo CFM.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

6.9 Subcontratação

6.9.1 Não será admitida a subcontratação.

6.9.2 Ficam vedadas a subcontratação total e parcial, bem como a cessão, a transferência e a dação em garantia deste CONTRATO.

6.9.3 O descumprimento desta Cláusula ensejará a rescisão do Contrato, bem como sujeitará a Contratada às sanções estabelecidas neste Contrato.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

7 – MODELO DE GESTÃO DO CONTRATO

7.1 Critérios de Aceitação

7.1.1 A prestação do serviço pela empresa não implica sua aceitação definitiva, que será caracterizada pela atestação da nota fiscal/fatura correspondente.

7.1.1.1 O recebimento definitivo ficará condicionado à observância de todas as cláusulas e condições fixadas neste instrumento e na proposta comercial.

7.1.2 Os objetos deste contrato serão recusados:

7.1.2.1 Quando entregues em divergência dos requisitos especificados deste Termo de Referência, do contrato ou da proposta comercial da CONTRATADA.

7.1.2.2 Quando forem considerados insatisfatórios, mediante testes de conformidade e verificação.

7.1.3 Ocorrendo a recusa, a CONTRATADA deverá providenciar o refazimento dos serviços prestados no prazo de entrega, contado a partir da comunicação feita pelo CONTRATANTE, dentro das condições de garantia especificadas neste Termo de Referência.

7.1.4 O recebimento provisório ou definitivo não exclui a responsabilidade civil da CONTRATA-DA em face da lei e desta contratação.

7.1.5 Ocorrendo divergências entre as exigências deste Termo de Referência e as contidas no contrato, prevalecerá o definido no Termo de Referência.

7.2 Procedimentos de Teste e Inspeção

7.2.1 Na execução do contrato, alguns papéis e responsabilidades deverão ser observados:

7.2.1.1 **Preposto:** colaborador nomeado pela CONTRATADA para representá-la o qual ficará responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao gestor do contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual;

7.2.1.2 **Gestor do Contrato**: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato;

7.2.1.3 **Fiscal Demandante do Contrato**: servidor representante da área demandante do contrato, indicado pela autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais e técnicos da solução, bem como aspectos administrativos da execução, especialmente os referentes ao

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;

7.2.1.4 **Fiscal Técnico**: servidor representante da área de Tecnologia da Informação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.

7.2.2 A fiscalização exercida pelo Gestor e/ou Fiscais do contrato ou seus substitutos não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade na execução do contrato, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior.

7.3 Supervisão da execução contratual

7.3.1 A CONTRATANTE indicará, formalmente, no ato da assinatura do contrato, as pessoas responsáveis pela sua supervisão formal e operacional, das gerencias de Infraestrutura, desenvolvimento de sistemas e unidade gestora formal do contrato.

7.3.2 A execução dos serviços deverá ser acompanhada e fiscalizada por servidor(es) especialmente designado(s) para esse fim, nos termos do artigo 67 da Lei nº 8.666/93.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

7.4 Níveis Mínimos de Serviço Exigidos

7.4.1 Disponibilidade do atendimento:

7.4.1.1 O serviço de atendimento já deverá estar disponível a partir da efetivação do contrato;

7.4.1.2 O atendimento telefônico deverá estar disponível em horário comercial (das 8 às 18 horas), de segunda a sexta-feira, exceto feriados de Brasília e nacionais;

7.4.1.3 O atendimento eletrônico por *e-mail* deverá estar disponível durante o horário comercial (das 8 às 18 horas), de segunda a sexta-feira, exceto feriados de Brasília e nacionais;

7.4.1.4 O atendimento eletrônico por meio de sistema de registro de Ordens de Serviço deverá estar disponível durante o horário comercial (das 8 às 18 horas), de segunda a sexta-feira, exceto feriados de Brasília e nacionais;

7.4.1.5 O atendimento eletrônico por acesso remoto/videoconferência deverá estar disponível durante o horário comercial (das 8 às 18 horas), de segunda a sexta-feira, exceto feriados de Brasília e nacionais;

7.4.1.6 O atendimento presencial deverá ocorrer durante o horário comercial (das 8 às 18 horas), de segunda a sexta-feira, exceto feriados de Brasília e nacionais.

7.4.2 Requisitos de qualidade e performance do atendimento:

7.4.2.1 O atendimento por e-mail (confirmação de recebimento) deverá ocorrer no mesmo dia do envio pelo CFM, dentro do horário estabelecido neste Termo de Referência.

7.4.2.1.1 *E-mails* de resposta automática não serão considerados como atendimento.

7.4.2.2 O sistema de chamados do fornecedor deverá permitir à contratante abrir um chamado e anexar arquivos, caso necessário;

7.4.2.3 Para a contagem do prazo para início de atendimento, será considerada a data e a hora do contato do fornecedor informando ao cliente seu início. Caso esse contato não seja realizado, será considerado para a contagem do prazo para solução do problema a data e a hora do contato do cliente ao fornecedor, informando o problema.

IDP – INDÍCE DE DESCONFORMIDADES DE PRAZOS DE ENTREGA DE OS	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos serviços constantes na Ordem de Serviço.

Meta a cumprir	**IDP < = 0**	A meta definida visa garantir a entrega dos serviços constantes nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da Contratante e lista de Termos de Recebimento e Termo de Aceite	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS. Será subtraída a data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.	
Periodicidade	Para cada Ordem de Serviço encerrada e com Termo de Recebimento (TR).	
Aplicação das sanções	Após a emissão do Termo de Aceite (TA)	
Mecanismo de Cálculo (métrica)	**IDP = <u>TEX – TEST</u>** **TEST** Em que: **IDP** – Índice de desconformidade de Prazo de Entrega da OS; **TEX** – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quanto a Contratada entrega os produtos da OS e haja aceitação por parte do fiscal técnico. **TEST** – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência.	
Observações	Obs. 1: Serão utilizados dias úteis na medição. Obs. 2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs. 3: A data e duração prevista deverão estar declaradas na OS	
Início de Vigência	A partir da emissão da OS	

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IDP**: De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 5% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 10% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 15% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 20% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 25% sobre o valor da OS e multa de 1% sobre o valor do Contrato.

IDQ – INDÍCE DE DEFEITOS DE QUALIDADE DE ENTREGA DE OS		
Tópico	**Descrição**	
Finalidade	Medir a qualidade na entrega dos serviços constantes na Ordem de Serviço.	
Meta a cumprir	**IDQ < = 0**	A meta definida visa garantir a entrega dos serviços constantes nas Ordens de Serviço dentro da qualidade prevista.
Instrumento de medição	Avaliação das entregas realizadas no relatório final e parcial do teste de intrusão	
Forma de acompanhamento	A avaliação será feita conforme os produtos e serviços a serem registrada na OS. Será subtraída a quantidade de entregas dos produtos da OS (desde que o fiscal técnico reconheça as entregas, com registro em Termo de Recebimento) pela quantidade de produtos definidos na OS.	
Periodicidade	Para cada Ordem de Serviço encerrada e com Termo de Recebimento (TR).	
Aplicação das sanções	Após a emissão do Termo de Aceite (TA)	
Mecanismo de Cálculo (métrica)	$$IDQ = \frac{PE - PP}{PP}$$ Em que: **IDQ** – Índice de defeitos de qualidade na Entrega da OS; **PE** – Produtos Entregues – corresponde a quantidade de produtos entregues na OS. **PP** – Produtos Previstos – quantidade de produtos previsto, constante na OS, conforme estipulado no Termo de Referência.	
Observações	Obs. 1:	

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

Início de Vigência	A partir da emissão da OS
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IDQ**: De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 5% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 10% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 15% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 20% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 25% sobre o valor da OS e multa de 1% sobre o valor do Contrato.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

7.5 Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.5.1 A licitante que, convocada dentro do prazo de validade da sua proposta, não assinar o contrato, não entregar a documentação exigida no edital ou apresentar documentação falsa, causar o atraso na execução de seu objeto, não mantiver as condições apresentadas na proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo, declarar informações falsas ou cometer fraude fiscal, garantido o direito ao contraditório e à ampla defesa, ficará impedida de licitar e contratar com a Administração Pública e será descredenciada no **Sicaf**, e do cadastro de fornecedores do CFM, pelo prazo de até 5 (cinco) anos, a que se refere o inciso XIV do art. 4º e o art. 7º da Lei nº 10.520/2002.

7.5.2 O atraso na assinatura do contrato ensejará multa no valor de 1% (um por cento) do valor total do Instrumento Contratual.

7.5.2.1 A fiscalização do contrato poderá sustar o pagamento de quaisquer faturas da contratada, no caso de inobservância de exigências da fiscalização do contrato amparadas em disposições contidas no contrato, até a regularização da situação, sem prejuízo das demais sanções cabíveis. Tal procedimento será comunicado por escrito à contratada;

7.5.2.2 Todo e qualquer atraso ocorrido por parte do fornecedor implicará em atraso proporcional no pagamento, que será feito sem quaisquer ônus adicionais para o CFM;

7.5.2.3 Poderá ocorrer diligência para apurar os casos de atraso ou de não-entrega dos serviços ofertados, caso as justificativas apresentadas não sejam consideradas satisfatórias.

7.5.3 A não-comunicação ao Conselho Federal de Medicina, por escrito, de quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução do contrato ensejará multa no valor de 1% (um por cento) do valor total do Instrumento Contratual.

7.5.4 Caso a CONTRATANTE considere insatisfatória a cooperação da CONTRATADA durante a realização de testes de segurança da informação, será aplicada multa no valor de 10% (cinquenta por cento) do valor total do Instrumento Contratual.

7.5.5 O vazamento de informações sigilosas — cometida por empregados ou prepostos da CONTRATADA — decorrentes de ação dolosa, imperícia, negligência ou imprudência, ensejará multa no valor de 50% (cinquenta por cento) do valor total do Instrumento Contratual.

7.5.5.1 O vazamento de dados pessoais sensíveis, protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), ensejará multa no valor de 50% (cinquenta por cento) do valor total do

Instrumento Contratual;

7.5.5.2 A multa descrita acima será aplicada para cada ocorrência registrada.

7.5.6 O descumprimento do item 4.9 requisitos de experiência profissional ensejará a rescisão do Contrato, bem como sujeitará a Contratada às sanções estabelecidas no Contrato.

7.5.7 A Administração, a seu critério, de forma fundamentada, poderá rescindir o contrato a qualquer tempo, observadas as disposições constantes dos artigos 77 a 80 da Lei nº 8.666/1993.

7.6 Do Pagamento

7.6.1 O pagamento do serviço será de acordo com os valores apresentados em Nota Fiscal da licitante vencedora, com base serviços executados, mensurados em USTs e de acordo com as Ordens de Serviço aprovadas pelos fiscais do Contrato, após o ateste definitivo (Termo de Aceite).

7.6.2 O Ateste definitivo (Termo de Aceite) do serviço se dará em até 15 (quinze) dias corridos após a apresentação e entrega dos relatórios citados neste Termo de Referência, pela CONTRATADA.

7.6.3 Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, no momento da aceitação, os serviços prestados não estiverem em perfeitas condições e em conformidade com as especificações estipuladas.

7.6.4 O pagamento será efetuado no prazo de até 10 (dez) dias úteis após a emissão do ANEXO 4 - Termo de Recebimento de Serviço (TR) ou do ANEXO 5 - Termo de Aceite de Serviço (TA) pelo Conselho Federal de Medicina, correspondente aos serviços executados e homologados pelos técnicos da CONTRATANTE, constantes das respectivas Ordens de Serviços mediante fatura relativa aos serviços efetivamente realizados, não sendo devido o pagamento de quaisquer valores a título de franquia ou garantia de execução de valores mínimos.

7.6.5 Para a entrega do Relatório Parcial recebida pela CONTRATANTE será emitido o ANEXO 4 - Termo de Recebimento de Serviço (TR), documento este que autoriza o faturamento do valor correspondente a 70% (setenta por cento) do valor respectiva da entrega.

7.6.6 O ANEXO 5 - Termo de Aceite de Serviço (TA) será emitido somente após o recebimento do Relatório Final do *Pentest* e realização do Seminário com a apresentação do Relatório Final prevista para a OS, efetuada a verificação dos serviços, cujo documento autoriza o faturamento do valor remanescente de 30% (trinta por cento) do valor total da OS.

7.6.7 O valor do pagamento dos serviços será calculado como sendo o valor

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

da fatura da OS, deduzindo-se a soma de glosas e multas computadas e aplicáveis na Ordem de Serviço.

7.6.8 No cálculo do valor a ser pago, são apuradas as glosas e multas.

7.6.9 Caso seja detectado qualquer erro, vício, defeito ou qualquer divergência, o serviço não será aceito, ficando a cargo do fornecedor a sua correção ou o seu refazimento, sendo sustado o pagamento, sem prejuízo às demais sanções cabíveis.

7.6.10 O valor do pagamento dos serviços será calculado como sendo o valor da fatura da OS, deduzindo-se a soma de glosas e multas computadas e aplicáveis no período.

7.6.11 No cálculo do valor a ser pago, são apuradas as glosas e multas:

VPOS = VTF − (TGOS + TMOS)

Em que:

VPOS = Valor a ser Pago na OS

VTF = Valor Total da Fatura/Nota Fiscal

TGOS = Total de Glosas da OS (Soma de todas as glosas apuradas em cada produto objeto dos Termos de Recebimento -TR).

TMOS = Total de Multas na OS

7.7 Direitos Autorais e propriedade intelectual

7.7.1 Toda e qualquer ação relativa a direitos materiais ou imateriais fundada nos serviços e/ou produtos do presente contrato eventualmente movida por terceiros contra o Conselho Federal de Medicina bem como quaisquer despesas decorrentes de qualquer ação assim movida, será de inteira e exclusiva responsabilidade da CONTRATADA, que suportará o pagamento do valor integral de eventual condenação imposta ao Conselho Federal de Medicina, o qual poderá cobrar da CONTRATADA independentemente de qualquer aviso, notificação judicial ou extrajudicial ou extrajudicial o valor respectivo desde logo reconhecido como líquido e exigível, inclusive custas, despesas processuais e honorários advocatícios.

7.7.2 São de propriedade da CONTRATANTE todos os produtos gerados aos quais se refere o objeto na vigência deste contrato, incluindo os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico

de qualquer natureza e aplicação, tais como quaisquer estudos, relatórios, descrições técnicas, documentação de sistemas, protótipos, dados, esquemas, plantas, desenhos, diagramas, fluxogramas, modelos, arquivos, conhecimentos adquiridos, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica, em conformidade com o artigo 111 da Lei nº 8.666/93, com a Lei 9.609/98, que dispõe sobre propriedade intelectual de programa de computador e com a Lei 9.610/98, que dispõe sobre direito autoral, sendo vedada qualquer comercialização destes por parte da CONTRATADA.

7.7.3 A CONTRATADA cederá ao Conselho Federal de Medicina, em caráter definitivo, os resultados produzidos durante a vigência do contrato, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

7.7.4 Para consecução do repasse de conhecimentos técnicos, a CONTRATADA deverá garantir a entrega da documentação dos serviços em mídia, de acordo com os padrões da CONTRATANTE, especificado nas Ordens de Serviço e por meio de palestras expositivas a serem estipuladas nas Ordens de Serviço a qualquer tempo decorrente de solicitação da CONTRATANTE, bem como mediante o repasse de conhecimento aos empregados da CONTRATANTE que acompanharão a execução dos serviços.

7.7.5 Todos os produtos gerados/mantidos nas Ordens de Serviço pela CONTRATADA deverão ser entregues a CONTRATANTE, que tem direito de propriedade sobre esses, sendo vedada qualquer comercialização por parte da CONTRATADA.

7.7.6 A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros nos testes de invasão ou quaisquer artefatos relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pela CONTRATANTE.

7.7.7 A CONTRATADA declara e garante que, para o cumprimento de suas obrigações relativas ao presente contrato, não infringirá patentes, licenças, copyright ou outros direitos de propriedade, nem violará quaisquer outros direitos de terceiros, inclusive royalties e taxas de licença, quer de pessoa física ou jurídica.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

7.8 Confidencialidade dos serviços

7.8.1 A CONTRATADA deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante todos os procedimentos, conforme disposições contidas no Termo de Confidencialidade, anexo a este Termo de Referência.

7.8.2 A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, processos, fórmulas, códigos-fonte, cadastros, fluxogramas, diagramas lógicos, dispositivos e artefatos, modelos ou outros materiais de propriedade da CONTRATANTE, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter acesso e conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE, tais documentos.

7.8.3 A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto sem autorização por escrito da CONTRATANTE, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

7.8.4 Cada profissional deverá assinar “Termo de Compromisso, Sigilo e Confidencialidade”, comprometendo-se a não divulgar nenhum assunto tratado nas dependências da CONTRATANTE ou a serviço dessa, salvo se expressamente autorizado.

7.8.5 A CONTRATADA deve entregar “Termo de Compromisso, Sigilo e Confidencialidade” de cada um dos seus empregados que venham a participar da prestação dos serviços objetos do contrato, devidamente assinados.

7.8.6 Cada profissional deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela CONTRATANTE não poderá ser utilizada para fins particulares e que a navegação em sítios da Internet e as correspondências em meios eletrônicos, utilizando o endereço da CONTRATANTE ou acessadas a partir dos seus equipamentos, poderão ser auditadas.

7.8.7 Cada profissional da CONTRATADA deverá assinar Termo de Compromisso conforme descrito, declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na CONTRATANTE, sendo a CONTRATADA corresponsável pelo descumprimento das normas por parte de seus profissionais.

7.8.8 A CONTRATADA também se compromete a respeitar as imposições

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

relativas ao sigilo bancário às quais à CONTRATANTE está sujeita.

7.8.9 Em relação ao tratamento de dados pessoais, durante a execução do serviço, a CONTRATADA atenderá, além das regras de responsabilidade, os critérios, procedimentos e prazos definidos na legislação de proteção de dados pessoais, em especial na Lei Geral de Proteção de Dados – LGPD (lei 13.709/2018), atendendo-se às seguintes diretrizes mínimas:

7.8.9.1 Adotar as medidas de proteção dos dados que, por razões técnicas, devam permanecer salvos, mesmo por curto espaço de tempo, no ambiente da contratada;

7.8.9.2 Não usar, copiar, compartilhar, guardar para si e/ou para terceiros, enfim, tratar os dados em referência, para quaisquer fins não expressamente previstos neste CONTRATO.

7.8.10 A não observância às obrigações de sigilo sujeitará a CONTRATADA às sanções administrativas previstas contratualmente, respondendo também na esfera civil e criminal pelas consequências advindas de seus atos.

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. O custo estimado da contratação, o valor máximo estabelecido em decorrência da identificação dos elementos que compõem o preço pode ser definido da seguinte forma:

8.2. Por meio de fundamentada pesquisa dos preços praticados no mercado em contratações similares; ou ainda por meio da adoção de valores constantes de indicadores setoriais, tabelas de fabricantes, valores oficiais de referência, tarifas públicas ou outros equivalentes, se for o caso;

8.3. Neste caso os custos foram levantados em pesquisa de preço no mercado e o valor médio anual apurado na pesquisa está apresentado na tabela abaixo, que será considerado como referencial a ser pago pela a execução do objeto deste termo de referência:

MAPA COMPARATIVO	VALOR ANUAL R$
PAINEL DE PREÇOS 01	R$ 82,02
EMPRESA A	R$ 240,00
EMPRESA B	R$ 300,00
EMPRESA C	R$ 310,00
PREÇOS MÉDIO	**R$ 233,02**

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

Para a realização testes de intrusão (*Pentest)* em infraestrutura de rede e sistemas para o Conselho Federal de Medicina foi estimado 960 USTs, o que equivale a uma valor estimado de **R$ 223.699,20 (Duzentos e vinte e três mil e seiscentos e noventa e nove reais e vinte centavos).**

Id.	Descrição do Bem ou Serviço	Quant.	Unidade de medida	Valor unitário máximo	Valor total máximo
1	Contratação de empresa especializada na prestação de serviço técnico de segurança da informação de testes de intrusão (Pentest) em infraestrutura de rede e sistemas, na forma de consumo de UST, pelo período de 24 (vinte e quatro) meses, a ser consumido sob demanda.	960	UTS	**R$ 233,02**	**223.699,20**

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1 Dotação orçamentária destacada para o Setor de Tecnologia da Informação, com aprovação orçamentária da Coordenação de Informática/CFM para execução no ano de 2022 por meio do centro de custo 36.03.

9.2 O orçamento será sigiloso até a fase de homologação desta Licitação, permitindo-se ao agente de licitação divulgá-lo, anteriormente, na fase de negociação, se assim entender conveniente.

10 – DA VIGÊNCIA DO CONTRATO

10.1 Para o fiel cumprimento das obrigações, será lavrado contrato de prestação de serviços a ser celebrado entre as partes, com vigência de 24 (vinte e quatro) meses, a contar da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos por termos aditivos, até o limite de 60 (sessenta) meses, após verificação da real necessidade e com vantagens à Administração Pública, conforme o inciso II do art. 57 da Lei nº 8.666/93.

10.2 A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada da realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

10.3 A licitante vencedora será convocada pela CONTRATANTE para assinar o contrato, tendo o prazo de 05 (cinco) dias úteis, contados do recebimento da notificação, para comparecer à administração, sob pena de decair o direito à contratação, sem prejuízo das penalidades previstas.
10.4 A recusa injustificada da referida licitante em assinar o contrato no prazo acima estabelecido, caracteriza o descumprimento total da obrigação, sujeitando-se às sanções legalmente cabíveis.

11 – DO REAJUSTE DE PREÇOS

11.1 Nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária, é obrigatória a adoção do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA.

11.2 O reajuste é cabível mediante pedido expresso da CONTRATADA até a celebração do Termo Aditivo de prorrogação, sob pena de preclusão.

11.3 Poderão ser aplicados índices negativos no período em que houver deflação, sendo este cabível ainda que a solicitação advenha apenas da própria Administração.

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1 Regime, Tipo e Modalidade da Licitação

12.1.1 O regime da execução do contrato será o de Regime Global, e o tipo e critério de julgamento da licitação será o de menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços comuns de informática.

12.1.2 A licitação será realizada na modalidade de Pregão Eletrônico, com julgamento pelo critério de menor preço, fundamentando-se na premissa de que a contratação de serviços se baseia em padrões de desempenho e de qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los.

12.1.3 Considerando-se o aspecto do projeto, faz-se necessária a contratação por meio do Sistema de Registro de Preços, para garantia da aquisição futura dos itens descritos no objeto deste Termo de Referência para o Conselho Federal de Medicina e/ou Conselhos Regionais de Medicina.

12.2 Critérios de Qualificação Técnica para a Habilitação

12.2.1 Documentação relativa à qualificação técnica

12.2.1.1 Apresentar dois ou mais Atestados de Capacidade Técnica, que demostre o correto cumprimento de obrigações equivalentes à SERVIÇOS PARA EXECUÇÃO DE TESTE DE INTRUSÃO – PENTEST.

12.2.1.2 Comprovação da aptidão para o desempenho de atividades pertinentes e compatíveis com as características, quantidades e prazos descritos no objeto deste Termo de Referência, mediante a apresentação de certidão aptidão de fornecimento já realizado anteriormente, por intermédio de atestado expedido por pessoa jurídica de direito público ou privado.

12.2.1.3 Os atestados de capacidade técnica devem se referir a prestação de serviços realizadas pela LICITANTE no Brasil.

12.2.1.4 Os atestados de capacidade técnica deverão ser emitidos por pessoas de direito público ou privado, recipientes dos serviços prestados e que tenham sido impactados diretamente pelos serviços da LICITANTE, não sendo aceitos atestados emitidos pela própria LICITANTE. Entende-se por impacto direto a pessoa jurídica que tenha participado do projeto e contribuído nas definições e validações dos resultados do trabalho realizado pela LICITANTE.

12.2.1.5 Atestado (s) de capacidade técnica, emitido (s) por pessoa jurídica de direito público ou privado que comprove que a

licitante, executou serviços com características técnicas semelhantes, compatíveis e pertinentes com o objeto desta licitação por período não inferior a 03 (três) anos e que tenham sido cumpridas as condições estabelecidas na respectiva contratação.

12.2.1.6 Os atestados de capacidade técnica deverão apresentar, obrigatoriamente, as seguintes informações:

12.2.1.6.1 Identificação da instituição responsável pela emissão, com nome, telefone e endereço completo.

12.2.1.6.2 Descrição geral dos serviços prestado;

12.2.1.6.3 Data de contratação, de conclusão e da aceitação do fornecimento;

12.2.1.6.4 Área responsável da parte do cliente;

12.2.1.6.5 Nome e telefone de contato do responsável por parte do cliente;

12.2.1.6.6 Grau de satisfação da instituição com relação ao fornecimento.

Notas

a) somente serão aceitos atestados de capacidade técnica expedidos após a conclusão do contrato que lhe deu origem ou se decorrido, no mínimo, um ano do início de sua execução, exceto se houver sido firmado para ser prestado em prazo inferior, caso em que só será aceito mediante apresentação do Contrato correspondente.

b) deverão ser disponibilizadas todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, anexando, quando solicitado, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

c) para a comprovação de experiência mínima de 03 (três) anos, será aceito o somatório de atestados, considerando períodos sucessivos de tempo, ininterruptos ou não.

d) serão aceitos atestados distintos para atendimento às exigências, porém, caso seja
apresentado um único atestado de capacidade técnico/operacional, este documento deverá atender, simultaneamente, todas as exigências.

12.2.1.7 Será permitida a apresentação de atestados de empresas do mesmo grupo econômico da LICITANTE. Entende-se que fazem parte de um mesmo grupo econômico as empresas que tenham diretores, acionistas (com mais de 5% de participação) ou representantes legais comuns, e as que dependam econômica ou financeiramente de outra empresa ou a subsidiem, e empresas sujeitas a uma mesma estrutura global — incluindo compartilhamento global de conhecimento, governança e

políticas corporativas.

12.2.1.8 A conformidade dos atestados poderá ser confirmada por meio de diligência, sendo que a sua desconformidade implicará a inabilitação da proposta, sem prejuízo de outras sanções cabíveis em virtude de falsidade das informações prestadas.

12.2.1.9 A recusa do emitente do atestado em prestar esclarecimentos e/ou fornecer documentos comprobatórios ou sofrer diligências desconstituirá o atestado de capacidade técnica e poderá configurar prática de falsidade ideológica — ensejando comunicação ao Ministério Público Federal e abertura de Processo Administrativo Disciplinar, conforme o caso, para fins de apuração de responsabilidades.

12.2.2 Justificativa à qualificação técnica

12.2.2.1 Em face da criticidade do fornecimento, é necessário comprovar que a CONTRATADA possui qualificação no fornecimento dos serviços.

12.2.2.2 Os serviços descritos nesse documento demandam conhecimento avançado em técnicas de exploração/intrusão em infraestrutura de redes e sistemas. Tal conhecimento requer que os profissionais sejam altamente qualificados e com experiência comprovada no assunto.

12.2.3 Considerações finais

12.2.3.1 O Conselho Federal de Medicina reserva-se no direito de, a qualquer tempo, realizar diligenciamento no ambiente físico da CONTRATADA ou solicitar quaisquer documentações complementares, visando aferir se todas as obrigações de ordem técnica, operacional ou administrativa, bem como a manutenção das condições de habilitação estão sendo cumpridas.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1 Este Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br

_____	_____
Integrante Requisitante	**Integrante Técnico**
Luiz Ricardo Clemencio	*Marcelo Sodré Silva*
Assessor de Tecnologia da Informação	*Chefe do Setor de Infraestrutura de TI*
Matrícula: 335	*Matrícula: 209*

Autoridade Máxima da Área de TIC
Gleidson Porto Batista *Coordenador de Tecnologia da Informação* *Matrícula: 251*

Brasília, 29 de abril de 2022.

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70400-150 Brasília DF | http://www.portalmedico.org.br