SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

TERMO DE REFERÊNCIA

Prestação de Serviços de Monitoramento de Ambiente Tecnológico

SOC (Security Operations Center)
NOC (Network Operations Center)

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) com fornecimento de infraestrutura e serviços que proporcionem segurança nas comunicações entre todas as unidades do CREA-SP.

2. SUPORTE LEGAL

2.1. A contratação fundamenta-se no disposto na Lei Federal nº 14.133, de 1° de abril de 2021;

2.2. Em consonância com a Instrução Normativa nº 05/2017 do Ministério do Planejamento, Desenvolvimento e Gestão - Secretaria de Gestão (atual Ministério da Economia), esta contratação também respeitará as regras e diretrizes que compõe a Instrução (CREA-SP) sobre os procedimentos de contratação, gestão e prorrogação de serviços e aquisição de bens para o CREA-SP e dá outras providências;

2.3. Lei Complementar no. 123/2006: Estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte;

2.4. Decreto Lei 200/1967: Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

2.5. Instrução Normativa (MPOG) n° 01/2010: Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras da Administração Pública Federal direta, autárquica e fundacional;

2.6. Instrução Normativa (SEGES/ME) no. 73/2020: Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

2.7. Instrução Crea-SP no. 2594/2018: Dispõe sobre as regras e diretrizes dos procedimentos de contratação, gestão e prorrogação de serviços e aquisições de bens para o Crea-SP e dá outras providências; e alterações posteriores, bem como demais normativos constante no Instrumento Convocatório.

3. JUSTIFICATIVA E FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. O CREA-SP é uma instituição que tem como função precípua a fiscalização do exercício das profissões nas áreas da Engenharia, Agronomia e, recentemente, Designers de Interiores, no âmbito do Estado de São Paulo, abrangendo tanto as titulações profissionais de nível superior quanto das áreas de segundo grau técnico.

Para o cumprimento de suas funções institucionais, que se constituem, em última análise, na defesa da sociedade, o CREA-SP possui considerável patrimônio, constituído por bens móveis e imóveis, assim como inúmeros serviços prestados através de plataformas, softwares, aplicativos de celulares.

3.2. Um dos aspectos fundamentais à concepção ou ao aprimoramento de uma instituição é a busca permanente pelo conhecimento da complexidade e das características da realidade na qual se propõe agir, de forma a alcançar resultados e metas traçados. Isso significa que o enfrentamento de um problema requer conhecê-lo no que tange às suas múltiplas facetas, suas causas e desdobramentos na sociedade, conhecimento este que balizará a reflexão sobre quais ações, racionais e planejadas, devem ser consideradas e promovidas.

3.3. Na busca da melhoria contínua e do aperfeiçoamento dos processos internos do CREA, busca-se a otimização da governança e processos operacionais de controles internos públicos, buscando as melhores práticas de gestão de riscos com fulcro às práticas emanadas pelo Tribunal de Contas da União -TCU e as jurisprudências que regulam e determinam práticas a serem seguintes por entes da Administração Pública Federal.

3.4. No curso da execução dos serviços no dia 06/12/2022 o CREA verificou que usuários do aplicativo do CREA receberam mensagens enviadas por um grupo de hacker que disparou diversas notificações ofensivas aos profissionais de São Paulo, assim como, de diversos outros Conselhos no Brasil como Pará, Bahia, Rio Grande do Norte, Maranhão, Amazonas, Roraima, Rondônia e Tocantins.

3.5. Diante deste fato o CREA-SP, imediatamente veio a público, emitindo uma nota de esclarecimento e informando que naquele momento o ataque não tinha causado vazamento de dados nem mesmo prejuízo a funcionalidade dos serviços.

3.6. Por sua vez, a Superintendência de Tecnologia / Gerencia Executiva deste Conselho tomou todas as medidas possíveis, como a desativação do link onde a exposição dos dados cadastrais foi identificada e a desativação do site e dos sistemas do CREA-SP. Uma empresa especializada em cibersegurança atuou em caráter emergencial para mapear e resolver a vulnerabilidade o mais rapidamente possível, além de entender a dimensão do que foi vazado. Além disso, o Crea-SP no curso de adotar todas as

providências junto às autoridades, registrou junto à Polícia Civil do Estado de São Paulo o boletim de ocorrência número 000KL6905/2022.

3.7. Diante da gravidade da situação, a equipe técnica atuou na tentativa da solução do problema, mas devido à extensão dos danos causados no ambiente tecnológico houve a necessidade de apoio de uma empresa especializada em segurança cibernética, com expertise principalmente na subárea de resposta a incidentes e suporte para segurança da informação, visando auxiliar nos trabalhos de investigação, necessidades, vulnerabilidades e problemas de segurança que poderiam causar um impacto negativo ao CREA-SP.

Apresentamos a seguir histórico de ataques cibernéticos recentes no Setor Público/Empresas do Brasil, os quais sofreram prejuízos na prestação de seus serviços:

3.8. Ministério de Saúde: sofreu um ataque cibernético na madrugada desta sexta-feira (10/12/2021). Com ele, os sites do órgão e do ConecteSUS ficaram fora do ar. Uma mensagem que dizia "*você sofreu um ransomware*" e "*50 TB de dados foram copiados e excluídos*" chegou a ser exibida pelo grupo invasor.
Em novembro de 2020, uma outra falha envolvendo o Ministério da Saúde expôs dados de 243 milhões de brasileiros na internet (incluindo informações de pessoas que morreram). Ficaram abertas para consultas indevidamente informações de pessoas cadastradas no SUS ou beneficiárias de planos de saúde.

3.9. Superior Tribunal de Justiça: Os Sistemas do STJ foram alvo de um ataque em novembro do ano passado (2020). Na ação, os cibercriminosos criptografaram dados e forçaram o Tribunal a suspender sessões e a tirar seu site do ar.

3.10. Anvisa – Agência Nacional de Vigilância Sanitária: Em setembro de 2021 o site da Anvisa também foi alvo de uma ação cibernética. A agência informou que o ataque foi do tipo *defacement* (modificação estética da página web).
Dados Retirados do portal UOL, de 10/12/2021: Ataque Cibernético no ministério da Saúde.
(https://www.uol.com.br/tilt/noticias/redacao/2021/12/10/ataque-hacker-ao-ministerio-da-saude-nao-foi-o-primeiroveja-outroscasos.htm).

3.11. Ministério do Desenvolvimento Social: "O Ministério do Desenvolvimento Social (MDS), responsável pelos 22,7 milhões de cadastros do Bolsa Família, sofreu um ataque cibernético na terça-feira, 21, e ficou com seus sistemas fora do ar."
(Fonte: https://www.baquete.com.br/noticias/23/03/2023/bolsa-familia-sofre-ataque-ddos)

3.12. Ataques generalizados a Órgãos do Governo Federal: "As investigações da Polícia Federal sobre o ataque hacker ao Ministério da Saúde apontam que o grupo também invadiu as plataformas do Ministério da Economia e de mais de 20 Órgãos do Governo Federal".
(fonte:https://www.cnnbrasil.com.br/nacional/pf-aponta-queataque-hacker-atingiu-ministerios-e-mais-de-20-de-orgaos-dogoverno/).

3.13. Ataque nas Lojas Renner: "O site das Lojas Renner voltou a funcionar no último sábado (21), dois dias depois de a empresa sofrer um ataque cibernético que afetou parte de seus sistemas e de sua operação".
(fonte: https://g1.globo.com/economia/tecnologia/noticia/2021/08/23/site-e-app-das-lojas-renner-voltam-a-funcionarapos-ataquehacker.ghtml)

3.14. Ataque Porto Seguro: "Porto Seguro (PSSA3) é a mais nova vítima dos hackers. Ataque cibernético derrubou sistemas e canais de atendimento da empresa.
(fonte: https://www.seudinheiro.com/2021/empresas/porto-seguro-ataque-hacker/)

3.15. Considerações Gerais

3.15.1. O que há de comum entre todos esses ataques bem-sucedidos é que as empresas perderam muito dinheiro e credibilidade, e que elas não estavam preparadas, portanto, é importantíssimo que o CREA-SP se prepare para futuros ataques cibernéticos.

3.15.2. O Conselho mantém informações pessoais e financeiras dos cerca de 400.000 (quatrocentos mil) profissionais, além dos registros de pessoas jurídicas, Anotações de Responsabilidade Técnica – ART, Certidões de Acervo Técnico – CAT, e demais informações de seus exercícios profissionais. O CREA-SP também mantém dados financeiros de todas as empresas que prestaram e prestam serviços a ele, sem contar os dados pessoais e financeiros dos funcionários também. Atualmente, os profissionais não precisam comparecer às Unidades físicas para solicitar determinados serviços, pois os mesmos podem ser solicitados e pagos diretamente pelo sítio eletrônico do Conselho ou pelo seu Aplicativo, assim como também emitir seus boletos de anuidade.

3.15.3. O CREA SP, conforme já comentado, se viu numa situação de grave exposição a ataques cibernéticos, os quais afetaram a prestação de serviços fundamentais aos engenheiros e profissionais credenciados, bem como também à população do Estado de São Paulo como um todo. O risco de paralisação da prestação dos serviços a todos esses profissionais registrados neste CONSELHO e, consequente danos à população em razão da degradação de desempenho ou interrupção dos diversos sistemas digitais, e/ou até ataques cibernéticos, deve ser mitigado com a maior brevidade possível.

3.15.4. Os serviços dependem cada vez mais de sistemas digitais e eletrônicos que estão interligados e conectados via redes de comunicação privada e/ou pública, no caso de acesso à Internet, e fazem uso de infraestruturas de Hardware e Software diversas e complexas, se faz mandatório o monitoramento, acompanhamento e atuação imediata de profissionais qualificados com uso de ferramental especializado e dedicado. Tais serviços abrangerão todo o sistema de comunicação do CREA SP.

3.15.5. A implantação de um serviço de NOC (Network Operations Center) para atender o CREA-SP visa o monitoramento do ambiente tecnológico, em regime de 24 (vinte e quatro) horas x 7 (sete) dias da semana e em feriados, e tem como objetivo prever e evitar falhas em equipamentos de rede e/ou serviços de TIC e sistemas críticos ao negócio do Conselho, impossibilitando ou minimizando a sua indisponibilidade ou degradação.

3.15.6. A implantação de um SOC (Security Operations Center) para atender o CREA-SP pós-cenário de desastre visa o monitoramento do ambiente tecnológico do Conselho e tem como objetivo prover serviços e soluções de detecção e validação de incidentes, análise comportamental e detecção de tráfego malicioso na infraestrutura de rede, gerenciamento de incidentes, validação e verificação de vulnerabilidade e ações de resposta imediata que visam restabelecer os serviços de TIC, em regime de 24 (vinte quatro) horas x 7 (sete) dias da semana e em feriados.

3.15.7. A implementação dos serviços de NOC e SOC se dará por meio de técnicos especializados disponíveis 24 (vinte quatro) horas x 7 (sete) dias da semana e em feriados, tanto em regime remoto quanto presencial, e ferramentas de software que permitirão o monitoramento e análise de comportamento do parque tecnológico do CREA-SP.

3.15.8. Ressalta-se a importância combinada dos serviços de NOC e SOC de modo a prevenir eventos de desastre em TI que comprometam a continuidade dos serviços do CREA-SP, visto que, sem o devido monitoramento integral do ambiente, se está sujeito à exploração de vulnerabilidades, por conseguinte, a novos ataques.

4. REQUISITOS GERAIS

4.1. Provisão de Infraestrutura e Serviços de Segurança nas Comunicações:

4.1.1. Fornecimento e implementação de infraestrutura e serviços destinados a garantir a segurança das comunicações entre as 187 unidades do CREA-SP;

4.1.2. Inclui o monitoramento contínuo de todos os ativos de TI e sistemas do Conselho, além da identificação de vulnerabilidades e a prevenção contra ataques cibernéticos;

4.1.2.1. Maiores detalhes sobre as unidades podem ser encontrados no site do CREA-SP em: Unidades de Atendimento do CREA-SP.

4.1.3. As unidades estão interligadas por uma rede MPLS (Multi Protocol Label Switching), que opera com velocidades variadas. Essa diversidade de velocidades não impacta o serviço de monitoramento graças à existência de um Concentrador de Enlaces MPLS, que integra as conexões com todas as unidades;

4.1.3.1. Detalhes Específicos da Infraestrutura:

4.1.3.1.1. Rede Core de Fibra Óptica (*Dark Fiber*): Envolve 6 (seis) unidades localizadas em São Paulo, capital;

4.1.3.1.2. Conexões de Comunicação nas Unidades Site Faria Lima e Angélica:

4.1.3.1.2.1. Dois *links* de internet com 100 Mbps cada;

4.1.3.1.2.2. Um *link* de internet com 20 Mbps;

4.1.3.1.2.3. Dois *links* de internet adicionais, cada um com 200 Mbps.

4.1.4. Para atender as necessidades do CREA-SP, deverão ser disponibilizados:

4.1.4.1. Infraestrutura completa de monitoramento centralizado, incluindo segurança, a qual deve proporcionar visibilidade, controle e gerenciamento de todos os ativos e sistemas deste Conselho, com seus respectivos desempenhos. Tal infraestrutura deve ser capaz de detectar antecipadamente potenciais gargalos, seja nas comunicações entre todas as unidades deste Conselho e entre estas e a Internet, seja nos ativos e sistemas de TI, bem como também potencias vulnerabilidades de forma a mitigar ataques e consequentemente danos a este Conselho;

4.1.4.1.1. A descrição pormenorizada dos serviços está detalhada no Item 5.

4.1.4.2. Associado à infraestrutura anteriormente citada, deverá ser disponibilizado serviços de monitoramento de todas a infraestruturas disponibilizadas, em caráter continuado e em regime de 24X7 (vinte e quatro horas por sete dias na semana), bem como suporte manutenção e geração de relatórios conforme detalhamento constante deste documento.

4.1.4.3. Estes serviços possibilitarão identificar imediatamente de forma preventiva e corretiva:

4.1.4.3.1. Potenciais e futuros problemas e gargalos – Preventiva;
4.1.4.3.2. Falhas causando Degradação de desempenho e suas respectivas causas – Corretiva;
4.1.4.3.3. Interrupção dos Serviços e suas respectivas causas – Corretiva;
4.1.4.3.4. Detecção de ameaças cibernéticas à sistemas, tais como como tentativas de invasão e/ou paralisação: páginas *web*, aplicativos, bases de dados e etc;
4.1.4.3.5. solução de problemas de segurança encontrados com agilidade e eficiência;
4.1.4.3.6. monitorar e analisar processos de forma contínua para identificar riscos de segurança na infraestrutura de TI.

4.1.4.4. Além disso os serviços prestados atuarão em tempo real e sobre todos os sistemas monitorados, para:
4.1.4.4.1. registrar e documentar todas as ocorrências acima listadas incluindo as que ameacem a segurança do ambiente de TI;
4.1.4.4.2. acionar os respectivos responsáveis seja no próprio CREA SP, seja para as respectivas contratadas por este Conselho, para prestação dos serviços eventualmente afetados ou responsáveis pelas falhas;
4.1.4.4.3. acompanhar a resolução dos problemas e apontar as soluções e providências tomadas;
4.1.4.4.4. gerar documentação através de relatórios de forma a possibilitar o acompanhamento dos chamados, tempos de resposta versus tempo contratado, possibilitando que o CREA SP realize a gestão adequada e necessária a boa prestação dos serviços a seus públicos interno e externo.

4.1.4.5. Fornecimento de infraestrutura e serviços que proporcione segurança nas comunicações entre todas as unidades do CREA-SP incluindo o monitoramento continuado de todos os ativos e sistemas de TI deste Conselho, identificando e mitigando potenciais vulnerabilidades e ataques, pelo prazo de 36 (trinta e seis) meses.

5. CARACTERISTICAS DO SERVIÇO

5.1. O serviço deve ser provido através do Network Operation Center (NOC) e Centro de Operações de Segurança (Security Operation Center - SOC):
Network Operation Center (NOC): O serviço deve incluir (mas não se limita); ao monitoramento e gestão contínua da infraestrutura de rede, garantindo a disponibilidade, desempenho e eficiência dos serviços e sistemas de TI. O NOC será responsável por identificar e resolver problemas de rede, realizar a manutenção preventiva e assegurar a continuidade dos serviços de TI;

5.1.1. Security Operation Center (SOC): Este serviço abrange (mas não se limita); ao monitoramento e análise de segurança contínuos para identificar, avaliar e responder a ameaças cibernéticas e vulnerabilidades. O SOC deve implementar

políticas de segurança, conduzir análises de risco, responder a incidentes de segurança e fornecer orientações estratégicas para melhorar a postura de segurança do CREA-SP;

5.2. Além dos NOCs e SOCs da CONTRATADA, deverá ser instalada a ferramenta de monitoramento no ambiente do CONTRATANTE, para o acompanhamento e controle do serviço de monitoramento da operação de Segurança, em um *dashboard* mostrando as atividades dos serviços.

5.2.1. A descrição pormenorizada do Item é descrita no Item 6.1;

5.3. O NOC e SOC principal deverão estar baseados e instalados em estrutura, obrigatoriamente, com as certificações ISO 27001 ISO 27701.

5.4. O SOC (Security Operations Center) deve oferecer serviços personalizados para transformar as operações de Segurança. Deve gerenciar, manter e monitorar de forma proativa a plataforma e aumentar a visibilidade de ameaças com a análise avançada de tráfego de rede.

5.5. A CONTRATADA deverá entregar este serviço por engenheiros certificados e analistas de segurança experientes de NOCs e SOCs, 24 horas por dia, 7 dias por semana.

5.6. A detecção, análise e relatórios detalhados de incidentes de segurança de ataques cibernéticos devem ser fornecidos por meio de uma combinação de ferramentas da CONTRATADA de acordo com o descrito neste Edital.

5.7. A CONTRATANTE deve fornecer toda a solução tecnológica complementar e serviço necessário para execução do serviço da CONTRATADA de acordo com o especificado neste Edital.

5.8. A CONTRATANTE deverá possuir e disponibilizar estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente;

5.9. Promover o Gerenciamento de Incidente, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos de todos os alertas oriundos do ambiente tecnológico de TIC da CONTRATANTE, integrando as equipes necessárias pelo atendimento;

5.10. Promover o Gerenciamento de Problema, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos necessários de todos os alertas oriundos do ambiente tecnológico de TIC da CONTRATANTE, integrando as equipes necessárias pelo atendimento;

5.11. Realizar a abertura de chamado junto às empresas contratadas pela CONTRATANTE em caso de indisponibilidade e/ou degradação do ambiente tecnológico da CONTRATANTE, integrando as equipes necessárias pelo atendimento;

5.12. Apresentar relatórios gerais oriundos dos sistemas que compõem a solução em qualquer tempo e sempre que solicitado pela CONTRATANTE;

5.13. Realizar atividades de liberação de Sistemas Críticos

5.13.1. Executar (dentro do escopo contrato) e/ou Acompanhar a homologação e a liberação das atualizações de aplicações críticas que suportam o negócio da CONTRATANTE (Ex.: PJe-1G, PJe- 2G, etc.), conforme solicitado pela CONTRATANTE;

5.13.2. Tais atividades deverão ser detalhadas, em modo passo a passo, em documento fornecido pela CONTRATADA e poderão ser executadas aos fins de semana e fora do horário comercial;

5.13.3. Tais atividades poderão ser executadas após o horário comercial, inclusive aos finais de semana, em regime presencial e/ou remoto;

5.13.4. A CONTRATADA não poderá alegar indisponibilidade de profissionais para a execução dos trabalhos programados, desde que comunicada pela CONTRATANTE com até 12 (doze) horas de antecedência da execução das atividades;

5.13.5. A CONTRATADA deverá disponibilizar no primeiro mês de contrato aplicativo para Android e IOS para acompanhamento de todas as informações em tempo real referente ao ambiente da Contratada e principais eventos.

6. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

6.1. Serviços Gerenciados de Monitoramento de Ambiente Tecnológico – NOC

6.1.1. A CONTRATADA deverá monitorar o parque tecnológico utilizando-se da ferramenta atual em produção.

6.1.1.1. No presente, a ferramenta atual em produção é a plataforma ZABBIX Community, cabendo a CONTRATADA adequar o seu corpo técnico em caso de troca de plataforma por parte da CONTRATANTE, sem ônus para o CREA-SP.

6.1.2. O Gerenciamento administrativo, bem como a abrangência de itens de configuração alvo da ferramenta de monitoramento do parque tecnológico será de responsabilidade da CONTRATANTE.

6.1.3. Composição dos serviços gerenciados de monitoramento de ambiente tecnológico:

6.1.4. Monitoramento de Rede:

6.1.4.1. A contratada deve prover monitoramento contínuo e em tempo real da rede, servidores e sistemas do CREA-SP, na sede da Av. Faria Lima, com

equipe especializada e de comprovada experiência. Utilizará infraestrutura avançada, incluindo *hardware* e *software*, para assegurar a detecção precoce e resposta a problemas de desempenho, falhas e ameaças à segurança.

6.1.4.2. Elementos a serem monitorados

6.1.4.3. Rede:

6.1.4.3.1. Status (Online/Offline);

6.1.4.3.2. Velocidade de conexão;

6.1.4.3.3. Latência;

6.1.4.3.4. Perda de pacotes;

6.1.4.3.5. Jitter;

6.1.4.3.6. Total de dispositivos conectados;

6.1.4.4. Access Points (APs):

6.1.4.4.1. Status (Online/Offline);

6.1.4.4.2. Número de dispositivos conectados;

6.1.4.4.3. Detecção automática de novos dispositivos;

6.1.4.5. Unified Threat Management (UTM):

6.1.4.5.1. Status (Online/Offline);

6.1.4.5.2. Roteamento adaptativo;

6.1.4.5.3. Funcionalidades: Firewall de próxima geração, prevenção contra ataques (ATP, IPS, IDS), antivírus, proteção contra malware e *ransomware*, *gateways* de segurança da *web* (SWG), VPN;

6.1.4.5.4. Controle de conteúdo e gerenciamento de tráfego;

6.1.4.5.5. Monitoramento e relatórios de tráfego em tempo real;

6.1.4.6. Servidores:

6.1.4.6.1. Status (Online/Offline);

6.1.4.6.2. Temperatura;

6.1.4.6.3. Uso de CPU e memória;

6.1.4.6.4. Logs de sistema;

6.1.4.6.5. Número de usuários conectados;

6.1.4.6.6. Detalhes de conexão (usuário, data e hora);

6.1.4.6.7. Detecção de *malware* e vírus;

6.1.4.6.8. Aplicações:

6.1.4.6.8.1. Configuração de monitoramento conforme requisitos do CREA, incluindo parâmetros específicos de desempenho e segurança.

6.1.5. Monitoramento de Servidores. Monitoramento de Nuvem.

6.1.5.1. O serviço incluirá monitoramento abrangente de servidores, tanto locais quanto hospedados em ambientes de nuvem, utilizando técnicas avançadas e ferramentas especializadas. Este monitoramento visa garantir a máxima disponibilidade, eficiência operacional e segurança dos dados;

6.1.5.1.1. Monitoramento de Servidores:

6.1.5.1.2. Análise contínua do status operacional (Online/Offline);

6.1.5.1.3. Monitoramento de indicadores críticos: temperatura, capacidade de CPU, uso de memória, espaço em disco;

6.1.5.1.4. Registro e análise de logs para detecção precoce de incidentes ou falhas;

6.1.5.1.5. Verificação de atualizações de segurança e patches;

6.1.5.1.6. Acompanhamento do número de sessões e usuários ativos;

6.1.5.1.7. Detecção de software malicioso e vulnerabilidades;

6.1.5.2. Monitoramento de Nuvem:

6.1.5.2.1. Gestão de recursos e serviços em nuvem, com foco na otimização de custos e performance;

6.1.5.2.2. Monitoramento de serviços de nuvem para conformidade com políticas de segurança e governança;

6.1.5.2.3. Avaliação da integridade e desempenho de instâncias, funções e contêineres na nuvem;

6.1.5.2.4. Monitoramento de tráfego e análise de ameaças em ambientes de nuvem;

6.1.5.2.5. Suporte para estratégias de *Disaster Recovery* e alta disponibilidade.

6.1.5.2.6. Ambos os serviços contarão com alertas em tempo real para a detecção e resposta rápida a qualquer incidente, além de relatórios detalhados para avaliação de desempenho e planejamento estratégico. A abordagem proativa na gestão de servidores e recursos em nuvem assegura uma infraestrutura de TI resiliente e segura, alinhada às necessidades do CREA-SP.

6.1.6. Monitoramento de Máquina Virtual. Monitoramento de Aplicativos.

6.1.6.1. Este serviço abrange o monitoramento detalhado de máquinas virtuais (VMs) e aplicativos, assegurando performance otimizada, segurança robusta e disponibilidade contínua. Utiliza ferramentas de última geração e metodologias avançadas para monitorar integralmente o ambiente virtualizado e o desempenho dos aplicativos.

6.1.6.2. Monitoramento de Máquinas Virtuais:

6.1.6.2.1. Monitoramento constante do status (Online/Offline) e saúde das VMs;

6.1.6.2.2. Análise de uso de recursos como CPU, memória, armazenamento e rede;

6.1.6.2.3. Detecção e alerta de falhas de sistema, sobrecarga de recursos ou outros problemas de performance;

6.1.6.2.4. Monitoramento de segurança para identificar vulnerabilidades e ameaças, incluindo a execução de antivírus e *antimalware*.

6.1.6.3. Monitoramento de Aplicativos:

6.1.6.3.1. Avaliação contínua da disponibilidade, tempo de resposta e saúde operacional dos aplicativos;

6.1.6.3.2. Análise de tráfego de aplicativos e padrões de uso para otimizar a experiência do usuário;

6.1.6.3.3. Monitoramento de transações específicas e processos críticos de negócios para identificar gargalos e melhorar a eficiência;

6.1.6.3.4. Implementação de alertas para notificação imediata de problemas que afetam a performance ou disponibilidade dos aplicativos;

6.1.6.3.5. Coleta e análise de *logs* para diagnóstico de problemas e suporte à resolução de incidentes.

6.1.7. Monitoramento de Banco de Dados.

6.1.7.1. Este serviço é dedicado ao monitoramento contínuo e abrangente de bancos de dados, garantindo sua performance, integridade, segurança e disponibilidade. Será implementado utilizando técnicas avançadas e ferramentas especializadas para monitorar de perto todos os aspectos críticos dos sistemas de banco de dados.

6.1.7.2. Funcionalidades do Serviço Incluem:

6.1.7.3. Performance e Otimização: Monitoramento em tempo real do desempenho dos bancos de dados, incluindo tempos de resposta de consultas, uso de CPU, memória, espaço em disco e eficiência de índices. Identificação e correção de gargalos de performance;

6.1.7.4. Disponibilidade e Saúde: Verificação constante do status operacional dos bancos de dados para garantir alta disponibilidade. Implementação de verificações de saúde para prevenir falhas;

6.1.7.5. Segurança: Monitoramento da segurança dos bancos de dados para detectar e mitigar vulnerabilidades. Inclui a gestão de patches de segurança, auditorias de acesso e análises para prevenção de SQL injection e outros ataques;

6.1.7.6. Backup e Recuperação: Gestão de políticas de backup para assegurar a recuperação de dados em caso de perda ou corrupção. Monitoramento da execução de backups e testes de recuperação de dados;

6.1.7.7. Análise de Logs: Coleta e análise de logs de transações e eventos para diagnóstico de problemas, auditorias de acesso e otimização de consultas;

6.1.7.8. Alertas Proativos: Configuração de alertas proativos para notificar a equipe técnica sobre questões críticas que necessitam de intervenção imediata.

6.1.8. Monitoramento utilizando Inteligência Artificial:

6.1.9. Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

6.1.9.1. *Machine learning* não supervisionado
6.1.9.2. *Machine learning* supervisionado
6.1.9.3. Deep Learning
6.1.9.4. Redes Neurais

6.1.10. A solução deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) o e visibilidade de rede.

6.1.11. A solução deve ser dotada de tecnologia baseada em Inteligência Artificial afim de identificar anomalias de comportamento e ataques sutis não identificados pelas tecnologias tradicionais de segurança da Informação

6.1.12. Não serão aceitos produtos ou serviços OpenSource.

6.1.13. A solução não deve depender de Pré-configurações baseadas na rede do órgão para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

6.1.14. A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e continua se adaptando a variações de comportamento destes durante o tempo.

6.1.15. A solução deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, é vedada qualquer forma de envio de dados para fora da rede do órgão para o funcionamento da solução.

6.1.16. A solução deve possuir mecanismos de DPI (*Deep Packet Inspection*).

6.1.17. Solução deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

6.1.18. A solução deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (*SPAN/Port Mirror*) ou através do uso de *TAP – Terminal Access Point*.

6.1.19. A solução deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

6.1.20. A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas em sua inteligência artificial.

6.1.21. A solução deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra-ataques cibernéticos.

6.1.22. A solução deve permitir a inspeção de plataformas como:

6.1.22.1. AWS
6.1.22.2. Microsoft Azure
6.1.22.3. Google G-Suite
6.1.22.4. Office 365
6.1.22.5. SalesForce
6.1.22.6. Dropbox Entreprise
6.1.22.7. Componentes virtuais (máquinas virtuais)
6.1.22.8. Endpoint para Sistemas Operacionais.
6.1.22.9. Docker, Kubernetes e AWS Fargate.

6.1.23. Deve ser dotada de única interface gráfica a qual permite o gerenciamento centralizado de todos os componentes da solução.

6.1.24. A CONTRATADA deverá executar o serviço de detecção e resposta aos incidentes baseada em Inteligência Artificial, com retenção dos logs por no mínimo 90 (noventa) dias;

7. REQUISITOS DE SERVIÇO

7.1. A necessidade de atendimento presencial, nos diversos serviços contratados, sob demanda e solicitado através de requisições de serviço, o NOC e SOC devem estar localizados no Estado do São Paulo.

7.2. A tecnologia implementada deve ser capaz de identificar e neutralizar ameaças cibernéticas automaticamente, agindo em questão de segundos. Isso é crucial para enfrentar ataques avançados, como o *ransomware* Lockbit 3.0, que tem a capacidade de criptografar 100 mil arquivos em apenas 4 minutos. Para tal, a solução de segurança deve operar de forma autônoma, ou seja, sem necessidade de intervenção humana, para responder de maneira eficaz e imediata a essas ameaças.

7.3. O Serviço de Gestão de Incidentes de Segurança deverá ser prestado em período integral (24x7 – vinte quatro horas por dia, sete dias por semana).

7.4. A qualquer momento o CONTRATANTE poderá solicitar, através de Requisição de Serviços, o atendimento presencial da CONTRATADA de qualquer dos serviços, para o tratamento de incidentes ou grave ameaça de segurança da informação.

7.5. As requisições de serviço serão solicitadas ordinariamente à CONTRATADA em reuniões mensais para serem executadas no mês subsequente a critério do CONTRATANTE, ou excepcionalmente, em caráter de urgência, através de e-mail.

7.6. CONTRATADA deve realizar de forma proativa as ações necessárias para manter o ambiente de segurança da CONTRATANTE adequado às melhores práticas do mercado, devendo:

7.6.1. Atualizar os firmwares e/ou softwares das soluções entregues como parte do objeto deste Termo de Referência (TR);
7.6.2. Propor os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes;
7.6.3. Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste TR, as mantendo documentadas e acessíveis no portal do cliente.
7.6.4. Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE;

7.7. A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todos as áreas de atuação do escopo do contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes.

7.8. manter uma rotina mensal de análise de indicadores internos e pesquisa de mercado com o objetivo de apresentar à CONTRATANTE um relatório com as inovações tecnológicas e solução que possam aumentar a qualidade e o grau de maturidade da segurança da informação do ambiente tecnológico;

7.9. Monitorar permanentemente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;

7.10. A tecnologia implementada deve ser capaz de identificar e prevenir incidentes de segurança de forma precoce, antes que possam afetar os serviços. Isso envolve a utilização de sistemas avançados de monitoramento e análise para detectar sinais indicativos de ameaças iminentes, permitindo uma resposta rápida e eficaz para mitigar possíveis impactos. A abordagem deve ser baseada em uma combinação de vigilância contínua e inteligência de segurança para garantir que as medidas

preventivas sejam aplicadas de maneira oportuna, evitando a ocorrência de incidentes antes que estes representem um risco real para a organização.

7.11. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de Tecnologia da Informação e Comunicação (TIC) do CONTRATANTE;

7.12. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;

7.13. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;

7.14. Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;

7.15. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;

7.16. Monitorar e propor soluções aos projetos/atividades em andamento, otimizando-os quanto aos requisitos de Segurança da Informação;

7.17. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

7.18. Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;

7.19. Para atendimento em especifico o NOC e SOC deve escalar para o time de elite do contratante, com intuito de realizar investigações mais especificas

8. REQUISITOS DO SERVIÇO DE RESPOSTAS A INCIDENTE

8.1. CARACTERISTICAS DO SERVIÇO

8.1.1. O Serviço de Resposta a Incidentes (CSIRT) deve se integrar ao SOC entregue pela CONTRATADA no regime 24x7x365.

8.1.2. A CONTRATANTE, quando julgar necessário, poderá solicitar atuação local do profissional em suas dependências ou nas dependências de seus clientes.

8.1.3. Todos os custos de deslocamento serão de responsabilidade da CONTRATADA, sem qualquer ônus para a CONTRATANTE.

8.1.4. O serviço de Serviço de Segurança Gerenciado da CONTRATADA deverá seguir as melhores práticas da indústria para fornecer o cumprimento adequado e processos de gerenciamento de mudanças, eventos, incidentes e gerenciamento de problemas. Esses serviços garantem que os dispositivos de segurança estejam disponíveis e que a CONTRATANTE mantenha a conformidade com os requisitos regulamentares aplicáveis.

8.1.5. A CONTRATANTE busca serviço de Resposta a Incidentes, para trazer maior proteção as aplicações publicadas através da infraestrutura da CONTRATANTE.

8.1.6. CONTRATANTE poderá solicitar a revisão sobre os resultados entregues na realização dos serviços que tenham sido feitos fora do escopo acordado no Contrato e/ou das normas, padrões, procedimentos e instruções técnicas da CONTRATANTE, ou ainda em desacordo com a legislação vigente, ficando a CONTRATADA obrigada a refazer o serviço conforme obrigação estabelecida neste Contrato, sem ônus para a CONTRATANTE.

8.1.7. Todo resultado entregue a partir dos serviços realizados pela CONTRATADA terá garantia de correções e ajustes necessários durante os 90 (noventa) dias seguintes à conclusão daqueles serviços, mesmo que essa conclusão tenha ocorrido nos últimos 90 (noventa) dias do Contrato.

8.1.8. Dentro do período de garantia, a correção de erros nos serviços entregues pela CONTRATADA deverá ser efetuada sem qualquer ônus para a CONTRATANTE, seja financeiro ou de atraso na prestação de outro(s) serviço(s), desde que, comprovadamente, não tenham se dado em razão das especificações feitas pela CONTRATANTE.

8.1.9. A garantia do serviço é estabelecida considerando-se a versão entregue. A garantia cessará apenas se a alteração for realizada na versão entregue.

8.1.10. A correção deverá ser executada pela CONTRATADA no prazo máximo de 24 (vinte e quatro) horas úteis, contadas a partir do comunicado feito pela CONTRATANTE junto à CONTRATADA sobre o defeito encontrado.

8.1.11. Extinta a vigência do CONTRATO, a CONTRATADA terá 05 (cinco) dias úteis para atendimento.

8.1.12. A não observância ao prazo para correção de defeito implica na aplicação das penalidades cabíveis.

8.1.13. Terminada a correção pertinente, a CONTRATADA enviará para o responsável pelo(s) artefato(s), designado pela CONTRATANTE, com cópia para a Gestão do Contrato, o(s) artefato(s) corrigido(s). A data e hora do envio deste comunicado serão considerados como data de término da correção.

8.1.14. O término do CONTRATO não cessará a garantia dos produtos.

8.1.15. Durante todo o período de execução dos serviços, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.

8.1.16. A CONTRATADA deve estar apta com conhecimento e ferramentas para recuperação dos principais ransowmares do mercado, sem considerar restore dos dados e shadow copys.

9. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

9.1. As Ferramentas a serem disponibilizadas pela CONTRATADA deverão ser compatíveis com o ambiente tecnológico da CONTRATANTE;
9.2. Cabe à CONTRATANTE disponibilizar de recursos e acessos aos Endpoints a serem monitorados.
9.3. Há necessidade de existir compatibilidade com os seguintes sistemas:

- Creanet,
- Creaintra,
- Creadoc,
- WEBatendimento,
- Senior,
- Implanta,

- Carteiras,
- SCI e
- Govadm.
- CREANET-INTERNO
- CREADOC
- PÁGINA WEB do CREA-SP
- CREA-API
- APLICATIVO DE FISCALIZAÇÃO
- APC-FOPAG
- CREA-BOT (MINERVA)
- ACERVO
- NUMÉRIA
- APLICAÇÕES DE ELEIÇÕES INTERNAS

SIPRO REMOTO

9.4. Todas as informações/logs listadas anteriormente e obtidas dos ativos de TI do CREA-SP devem estar integradas no Sistema de Correlação de Informações de segurança, o qual deve capturar e correlacionar estes e prover Retenção de dados de no mínimo 6 meses.

9.5. O Sistema Web Application Firewall deverá prover Proteção para 01 Domínio "Top Level Domain" (creasp.org.br), bem como Proteção para as aplicações: Agendamento; CREADOC; CREANET1; CREANETINTRA1; SERVICEAPI. Esta deverá ainda possuir Capacidade de atuação de no mínimo 10 aplicações adicionais.

9.6. O sistema de Proteção de APIs deve:

9.6.1. • Possibilitar a Descoberta, Análise, Remediação e Testes dos seguintes tipos de APIs: HTTP, RESTFul, GraphQL, SOAP, XML-RPC e gRPC;

9.6.2. • Possibilitar a descoberta, inventário: e categorização das informações das APIs, além de:

9.6.3. o Determinar se a API tem origem na Internet ou internamente;

9.6.4. o Métodos de Autenticação;

9.6.5. o Tipos de Dados;

9.6.6. o Mais e menos usadas;

9.6.7. o Gerada automaticamente;

9.6.8. o Especificações Swagger/OAS das APIs;

9.6.9. • Detectar automaticamente e baseada em Inteligência Artificial;

9.6.10. o Vazamento de Dados (Data leakage);

9.6.11. o Adulteração de Dados (Data tampering);
9.6.12. o Erros de Configuração (Misconfigurations);
9.6.13. o Alterações nas APIs (Changes and Drift);
9.6.14. o Violação de Política de Dados e Vulnerabilidades de API definidas pela OWASP Top 10 ;
9.6.15. o Gráfico de Fluxo de Chamadas (Graphical Call Flows).
9.6.16. • Atuar na Prevenção
9.6.17. o Possibilitar a Interrupção da sessão TCP de comportamento suspeito se integrando com soluções de terceiros;
9.6.18. o Possibilitar o envio de dados em tempo real (Webhook) em WAFs para criar novas políticas contra comportamento suspeito;
9.6.19. o Possibilitar a integração e atualização automática das regras de firewall para regular o comportamento suspeito;
9.6.20. o Possibilitar definição de políticas em gateways de API regulando as informações para destino ou cliente;
9.6.21. o Prevenção em linha para bloquear usuários ou APIs;
9.6.22. o Integrar com fluxos de trabalho existentes (tickets, SIEMs, etc.);
9.6.23. o Possibilitar o acompanhamento do tempo médio para atribuição, lida e resolução (MTTR – Mean Time to Resolve).
9.6.24. • Atuar a nível de Testes
9.6.25. o Teste ativo das APIs em ambientes de pré-produção e produção.
9.6.26. o Implementação
9.6.27. o Permitir a implementação sem a necessidade de instalação agentes;
9.6.28. o Permitir a implementação sem que haja necessidade de modificação na(s) rede(s);
9.6.29. o Possibilitar a integração com Gateways de API, load balancers, WAFs, agregadores de log;
9.6.30. o A implementação deve ser feita no ambiente da CONTRATADA não podendo em hipótese alguma ser feita total ou parcialmente na nuvem pública ou em nuvem de terceiros.

9.7. Dispositivos de Rede:
9.7.1. Monitoramento de Switches e Access Points:
9.7.1.1. O serviço incluirá o monitoramento contínuo e abrangente de todos os switches e access points dentro da infraestrutura de rede, totalizando 254 dispositivos. O objetivo é assegurar o funcionamento ótimo, a segurança e a alta disponibilidade destes dispositivos críticos para a rede.
9.7.1.2. Especificações do Serviço:
9.7.1.2.1. Quantidade de Dispositivos: Monitoramento de 254 dispositivos, incluindo switches e access points.
9.7.1.2.2. Tecnologia de Monitoramento: Utilização do protocolo SNMP (Simple Network Management Protocol) para a coleta de dados em tempo real sobre o desempenho e a saúde dos dispositivos, independente da marca ou modelo.

9.7.1.2.3. Métricas de Desempenho: Monitoramento de utilização de banda, erros de interface, status de portas (up/down), potência do sinal dos access points, número de dispositivos conectados, entre outros indicadores relevantes.

9.7.1.2.4. Análise de Logs: Coleta e análise de logs dos dispositivos para identificação de eventos, falhas ou comportamentos anormais.

9.7.1.2.5. Alertas e Notificações: Implementação de um sistema de alertas para notificar a equipe técnica sobre qualquer irregularidade ou falha detectada, permitindo uma resposta rápida para resolução de problemas.

9.8. SIEM

9.8.1. Sistema de Correlação de informações de segurança com no mínimo as seguintes características:

- Mínimo de 250 fontes de dados e eventos/logs de segurança;
- Retenção de dados de no mínimo 3 meses;
- Taxa mínima de tratamento de dados diários de 90 Gigabytes/dia; e
- Taxa mínima de tratamento de dados de 2.5 Terabytes mensais.

10. REQUISITOS DE INSTALAÇÃO

10.1. A CONTRATADA deverá executar no prazo máximo de 30 (noventa) dias, a contar da data do memorando de início, as atividades de planejamento, instalação/adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, em conformidade com este Termo de Referência;

10.2. Todas as atividades e documentação apresentadas deverão ser previamente aprovados pela CONTRATANTE.

10.3. A CONTRATADA, como parte da execução do Serviço de Operação e Atendimento de Requisições, deverá realizar, nos primeiros 40 (quarenta) dias de execução deste serviço, uma avaliação completa do ambiente do contratante com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) e avaliar a maturidade dos controles de segurança da CONTRATANTE;

10.4. O GAP Analysis deverá ser realizado utilizando como base um dos seguintes frameworks de segurança: NIST, CIS ou ISO, que deverá ser antecipadamente aprovado pela CONTRATANTE;

10.5. A CONTRATADA, após o levantamento inicial das lacunas ou falhas de segurança da informação no ambiente da CONTRATANTE, deverá elaborar, coordenar e supervisionar um plano de ação em conjunto com a DGTEC, priorizando as falhas consideradas mais críticas;

10.6. A CONTRATADA deverá seguir o processo de gestão de mudança (GMUD) estabelecido pela CONTRATANTE;

10.7. Todos os serviços previstos deverão ser implantados, documentados e revisados pela CONTRATADA, seguindo a metodologia ITIL 4;

10.8. A CONTRATADA, sempre que solicitada, deverá estar disponível para participar das reuniões internas com o CONTRATANTE, para prestar informações sobre os ambientes e serviços por elas executados;

10.9. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas contratadas e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto;

10.10. A CONTRATADA deverá apresentar ao CONTRATANTE o planejamento ou plano de ação de todas as mudanças no ambiente, conforme níveis de controle estabelecidos, para todas as mudanças apresentadas;

10.11. A CONTRATADA deverá acompanhar, dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização;

10.12. A CONTRATADA deverá monitorar permanente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;

10.13. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza continua e deverão minimizar a necessidade de parada do ambiente em produção;

10.14. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais, conforme os requisitos específicos para o perfil profissional;

Profissionais	Quantidade	Descrição	Qualificação Mínima	Tempo de Experiência	Certificações
Gerente de Infraestrutura de Tecnologia da informação Senior	1	Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de infraestrutura de TIC, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de operações na infraestrutura de TIC.	Ensino Superior em Gestão da Tecnologia da Informação	5 anos como Coordenador de Equipe de Tecnologia da Informação atuando em Centro de Operações de Rede e/ou Centro de Operaçãoes de Segurança Cibernética com experiência em administração de redes de Telecomunicações Locais e WAN, Fibra Óptica, Firewall, Swithces, Roteadores, Dispositivos Wireless e Servidores de Aplicação e de Bancos de Dados.	a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation 4 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Network Security BlockBit; g) Information Security Foundation (ISO 27001); h) Privacy & Data Protection Practitioner
Analista de redes e de comunicação de dados Senior	1	Profissional que atua na intercomunicação de redes locais e delonga distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.	Ensino Superior em Gestão da Tecnologia da Informação	3 anos como Analista de Suporte Pleno ou como Administrador atuando em Centro de Operações de Rede e/ou Centro de Operaçãoes de Segurança Cibernética com experiência em administração de redes de Telecomunicações Locais e WAN, Fibra Óptica, Firewall, Swithces, Roteadores, Dispositivos Wireless e Servidores de Aplicação e de Bancos de Dados.	a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation 4 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Information Security Foundation (ISO 27001); g) Network Defense Essentials NDE
Analista de redes e de comunicação de dados Pleno	1	Profissional que atua na intercomunicação de redes locais e delonga distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.	Ensino superior na área de Tecnologia.	3 anos como Analista de Suporte Junior ou como Administrador de Redes atuando em Centro de Operações de Rede e/ou Centro de Operaçãoes de Segurança Cibernética há pelo menos um ano	a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation 4 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Information Security Foundation (ISO 27001); g) Network Defense Essentials NDE
Gerente de segurança da informação	1	Profissional que atua na intercomunicação de redes locais e delonga distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.	Ensino Superior em Gestão da Tecnologia da Informação - Pós-Graduação em Perícia Forense Digital	5 anos como Analista de Suporte ou como Administrador de Redes atuando em Centro de Operações de Rede e/ou Centro de Operaçãoes de Segurança Cibernética há pelo menos um ano	a) Certified Information Security Manager (CISM); b) DCPT - Desec Certified Penetration Tester; c) Certified Information Systems Security Professional (CISSP); d) CompTIA Security+ ; e) GIAC Security Expert (GSE); f) Hacking Foundation
Administrador em segurança da informação - Sênior	1	Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança. presta serviços e controle de segurança preventivo e reativo relacionado aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na politica de segurança.	Ensino Superior em Gestão da Tecnologia da Informação	3 anos como Administrador em Segurança da Informação e com sólidos conhecimentos em implantação e gestão de sistemas de Firewall, WAF, SIEM e EDR.	a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation 4 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Information Security Foundation (ISO 27001); g) Network Defense Essentials NDE
Administrador em segurança da informação - Pleno	1	Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança. presta serviços e controle de segurança preventivo e reativo relacionado aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na politica de segurança.	Ensino superior na área de Tecnologia.	2 anos como Administrador em Segurança da Informação e com sólidos conhecimentos em implantação e gestão de sistemas de Firewall, WAF, SIEM e EDR.	a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation 4 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Information Security Foundation (ISO 27001); g) Network Defense Essentials NDE

Para cada tipo de evento deve haver um NMS correspondente, cujo não atendimento pode ser penalizado a CONTRATADA com multas e descontos nos pagamentos mensais.

10.15. Encaminhamento e Resolução de Problemas

Quando da identificação de potenciais problemas seja relacionados a degradação e/ou falhas do desempenho dos links de comunicação das redes locais, rede MPLS e/ou links de Internet, na degradação e/ou falhas do desempenho dos servidores de aplicação e bases de dados e/ou degradação e/ou falhas das aplicações e bancos de dados propriamente ditos, seja de eventos com características de tentativa de ataque cibernético ou propriamente um ataque cibernético em si, de qualquer origem e natureza, a contratada deverá abrir, imediatamente, ticket específico, sistema de acompanhamento de chamados próprio e/ou disponibilizado pelo CREA-SP, para cada caso e atuar imediatamente para prevenir e/ou remediar tais eventos. Esses tickets deverão ser direcionados ao CREA-SP e/ou à prestadora, contratada pelo CREA-SP, responsável pelo referido serviço, solicitando reparo e providências técnicas. A partir desse momento, a Contratada ficará responsável por acompanhar as tratativas dadas ao ticket em específico até a conclusão do atendimento e correlacionar o mesmo com o SLA (Service Level Agreement) contratado junto a fornecedora deste. Em se tratando de atividades executadas pelo próprio time de profissionais do CREA-SP, por requererem acessos privilegiados e alta segurança, por exemplo, os tempos de reparo e/ou reconfiguração de determinados ativos, sistemas e/ou aplicações deverão ser detalhados no caderno de serviços e assim passarem a constar do SLA de atendimento por parte dos próprios integrantes do corpo técnico do CREA-SP.

Tal procedimento tem como objetivos, garantir que degradações, falhas e ou tentativas de ataques não afetem o desempenho mínimo dos serviços prestados aos públicos interno e externo, bem como também possibilitar averiguação do cumprimento dos prazos de atendimento contratados, bem como aplicação de multas, descontos e eventuais sanções aos respectivos fornecedores.

10.16. Relatórios

10.16.1. Relatórios de Ocorrências e Tentativas de Incidentes

A Contratada deverá gerar relatórios contendo informações detalhadas das ocorrências, os quais deverão descrever os serviços afetados em decorrência de que tipo de falha, tentativa de ataque ou real ataque cibernético, em que componente (rede, servidor, aplicação e outros sistemas e aplicações.), providências tomadas e previsão de restabelecimento dos mesmos.

Deverão ser apresentados dois tipos de relatórios. Um relatório de Gestão e um relatório de Operação. O relatório de gestão deverá ser entregue até o 5ª (quinto) dia útil do mês subsequente ao mês de prestação de serviços e deverá conter um extrato sintético de todas as ocorrências e eventos objeto do serviço prestado. O relatório de operação deverá ser subdividido em dois a saber: um para eventos que tratam de desempenho, degradação e/ou falhas, mas que não tenham correlação com eventos de ataques cibernéticos e um segundo que trate especificamente de tentativas de ataques cibernéticos ou ataques reais. Os relatórios de operação devem obedecer a frequência e hierarquia de acordo com o respectivo grau de severidade conforme segue:

Eventos de Alta Criticidade

Frequência:
sempre que houver ocorrência de eventos que comprometam em 30% (trinta por cento) ou mais o desempenho dos serviços prestados para os públicos interno e/ou externo ou que causem a interrupção da prestação dos mesmos.

Tempo para envio/comunicado:

até 15 (quinze) minutos após a identificação do mesmo

Hierarquia:

Superintendência

Eventos de Média Criticidade

Frequência:
sempre que houver ocorrência de eventos que comprometam de 10% (dez por cento) a 30% (trinta por cento) o desempenho dos serviços prestados para os públicos interno e/ou externo.

Tempo para envio/comunicado:

até 30 (trinta) horas após a identificação do mesmo

Hierarquia:

Gerência

Eventos de Baixa Criticidade

Frequência:

sempre que houver ocorrência de eventos que comprometam 5% (cinco por cento) a 10% (dez por cento) o desempenho dos serviços prestados para os públicos interno e/ou externo, e/ou que eventos que estejam relacionados a identificação de potenciais futuros problemas de forma a encaminhar preventivamente solicitação de providências e estudos para implementação de soluções.

Tempo para envio/comunicado:

até 4 (quatro) horas após a identificação dos mesmos.

Hierarquia:

Gerência

10.16.2. Relatórios Mensais

A contratada deverá enviar relatório de gestão mensal consolidado o qual deverá conter, no mínimo:

10.16.2.1. Ocorrências com a respectiva indicação de:

- criticidade
- serviço interrompido / disponibilidade em %

- ativos afetados
- prestadora do serviço

- Providências e Soluções tomadas
- Responsável pela abertura e acompanhamento do chamado
- Responsável pelas providências e soluções adotadas
- Data, Hora e tempo para restabelecimento do serviço
- Correlação entre o tempo para restabelecimento do serviço e o tempo estabelecido em contrato com as respectivas prestadoras de serviço.

10.16.2.2. Desempenho, Controle de Conteúdo e Tráfego na Rede

- Desempenho da Rede e Ativos Monitorados
- Conteúdo Trafegado por usuário e aplicação
- Tráfego Geral na rede e por unidade

10.16.2.3. Gestão de Vulnerabilidade

A CONTRATADA deverá gerar relatórios completos listando todas as vulnerabilidades encontradas e indicando os riscos aos quais a CONTRANATE está exposto bem como também apontando as correções e melhorias a serem feitas.

10.16.2.4. Pentesting

A CONTRATADA deverá gerar relatórios completos listando todas as vulnerabilidades encontradas e indicando os riscos aos quais a CONTRANATE está exposto bem como também apontando as correções melhorias a serem feitas.

10.17. SLA, Tempos de Reparo e Manutenção

Toda a infraestrutura fornecida pela Contratada, objeto desta contratação, seja composta de hardware(s) e/ou software(s), esteja ou não dentro das dependências do CREA-SP, deve estar disponível e em pleno funcionamento em regime 24 X 7 X 365 (vinte e quatro horas por dia, sete dia por semana e trezentos e sessenta e cinco dias

por ano) de forma ininterrupta. Será admitida indisponibilidade dos sistemas monitoramento, gestão, proteção e prevenção a incidentes e armazenamento/retenção de informações de no máximo 0,1% (zero, vírgula um por vento) ao mês. A contratada deverá dimensionar seus sistemas de forma a atender este requisito.

INDICADOR DISPONIBILIDADE MENSAL DO SISTEMA DE MONITORAMENTO E GESTÀO (IDM)	
ITEM	DESCRIÇÃO
Finalidade	Garantir o pleno funcionamento dos sistemas de monitoramento e gestão, em condições normais de operação, conforme
Meta a cumprir	99,9% de disponibilidade mínima
Instrumento de medição	Software de Monitoramento de Rede
Forma de acompanhamento	Pelo Sistema da CONTRATANTE baseado em software SNMP
Periodicidade	Mensal
	IDM=[(To-Ti)/To]*100
Mecanismo de cálculo	Onde: IDM = índice de disponibilidade mensal do enlace em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (um mês) em minutos.
Início de vigência	Data do Termo de Recebimento Definitivo
Adequações de pagamento	IDM < 99,9% = Desconto de 1% sobre o valor mensal do circuito a cada 0,2% abaixo de 99,9% no valor do IDM. Limitada a 10% do valor mensal do contrato.
Observações	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com IDM apurado diariamente, totalizados e apresentados mensalmente por enlace.

Tabela 2 - **Indicador Disponibilidade Mensal do sistema de monitoramento e gestão (IDM)**

11. COTAÇÃO DE PREÇOS

11.1. Fornecimento de infraestrutura e serviços que proporcione segurança nas comunicações entre todas as unidades do CREA-SP incluindo o monitoramento continuado de todos os ativos e sistemas de TI deste Conselho, identificando e mitigando potenciais vulnerabilidades e ataques cibernéticos.

Item	Descrição dos serviços	Und.	Quant. / Itens	Valor de Instalação	Valor Unitário	Valor Total 12 meses
11.1	**Instalação** de infraestrutura de monitoramento unificada e centralizada composta por sistemas de hardwares e softwares com os seguintes recursos mínimos: correlação entre analytics, inteligência de ameaças e anomalias no comportamento dos usuários da rede; firewall de aplicação web; detecção e resposta de dispositivos móveis ou não móveis; controle e gerenciamento de ativos de tecnologia da informação; e abertura e acompanhamento de chamados. Todos os sistemas deverão disponibilizar informações através de dashboards os quais deverão ser disponibilizados através de no mínimo 6 monitores de 65”(sessenta e cinco polegadas) específicos a serem instalados nas dependências do CREA-SP.	Unid	1	351.368,58		351.368,58
11.2	**Serviços** de Monitoramento unificada e centralizada composta por sistemas de hardwares e softwares com os seguintes recursos mínimos: correlação entre analytics, inteligência de ameaças e anomalias no comportamento dos usuários da rede; firewall de aplicação web; detecção e resposta de dispositivos móveis ou não móveis; controle e gerenciamento de ativos de tecnologia da informação; e abertura e acompanhamento de chamados. Todos os sistemas deverão disponibilizar informações através de dashboards os quais deverão ser disponibilizados através de no mínimo 6 monitores de 65”(sessenta e cinco polegadas) específicos a serem instalados nas dependências do CREA-SP.	Mês	12		246.002,92	2.952.035,08
TOTAL						**3.303.403,66**

12. PARCELAMENTO DO OBJETO

12.1. Tendo em vista as características das soluções a serem contratadas optou-se pelo não parcelamento do objeto deste certame para fornecimento de infraestrutura e serviços que proporcione segurança nas comunicações entre todas as unidades do CREA-SP, incluindo o monitoramento continuado de todos os ativos e sistemas de TI deste Conselho e de potenciais vulnerabilidades e ataques cibernéticos.

13. PRAZO DE EXECUÇÃO

13.1. Dos contratos:

13.1.1. O prazo de execução dos contratos será em conformidade com o inciso do artigo 106 da Lei nº 14.133/2021 – Lei de Licitações e Contratos Administrativos.

13.1.2. Assim o prazo da contratação deverá ser de até 12 (doze) meses, podendo ser prorrogado conforme disposto nos artigos 107 e seguintes.

14. DO REAJUSTE

14.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data-base de apresentação do orçamento estimado. (Parágrafo 3°, art. 92 da Lei 14.133/2021).

14.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se, na ausência de um índice específico, o ICTI (Índice de Custo da Tecnologia da Informação), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

14.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

14.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

14.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

14.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

14.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

14.8. O reajuste será realizado por apostilamento.

15. PROVA DE CONCEITO

15.1. A licitante melhor classificada na etapa de lances deverá apresentar comprovação da qualificação técnica exigida, e na sequência, mediante validação da qualificação técnica pelo pregoeiro, será submetida a uma Prova de Conceito – POC, por meio da análise de admissibilidade e avaliação técnica, a fim de comprovar as funcionalidades e requisitos descritos e exigidos a seguir.

15.2 A homologação técnica da licitante ocorrerá mediante comprovação da qualificação técnica por meio dos atestados de capacidade técnica e da aprovação da POC conforme estabelecido nesse instrumento convocatório.

15.3 A adjudicação do objeto do certame dependerá da realização de Prova de Conceito. Será considerada eliminada do certame a licitante que deixar de satisfazer pelo menos 100% (cem por cento) dos requisitos de especificação da plataforma indicados a seguir;

15.4 Em caso de eliminação, será convocada a próxima licitante melhor classificada no certame e assim sucessivamente até que uma Licitante demonstre capacidade de atendimento aos requisitos exigidos no presente edital.

15.5 As datas e local de realização da POC e da retomada da sessão serão informadas na própria sessão pública e publicadas no sítio da licitação.

15.6 Demais critérios e procedimentos utilizados para a Prova de Conceito estão descritos no Roteiro da Prova de Conceito, Anexo VI.

16. DA QUALIFICAÇÃO TÉCNICA

16.1 Atestado(s) ou declarações de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, redigido(s) e assinado(s) por servidor/funcionário competente do respectivo órgão ou empresa, que comprove(em) ter a licitante prestado serviços na área de operação de Network Operation Center (NOC) e Security Operation Center (SOC),

a) Os atestados deverão conter as seguintes informações mínimas: nome e cargo da pessoa que os assina, quantitativo ou valor da prestação dos serviços;

b) A critério do pregoeiro, as licitantes deverão disponibilizar informações adicionais necessárias à comprovação da legitimidade do(s) atestado(s) ou declaração(ões) apresentado(s), inclusive cópia de pelo menos uma nota fiscal do serviço constante no documento apresentado.

c) Será aceito o somatório de atestados e/ou declarações para comprovar o quantitativo mínimo exigido, exclusivamente quando se referir a períodos concomitantes.

d) Os atestados deverão ser compatíveis em características e quantidades com o objeto da Licitação

e) Entende-se como compatíveis em características e quantidades com o objeto da Licitação.

- Fornecimento de infraestrutura de monitoramento unificada e centralizada composta por sistemas de hardwares e softwares com os seguintes recursos mínimos: correlação entre analytics, inteligência de ameaças e anomalias no comportamento dos usuários da rede; firewall de aplicação web; detecção e resposta de dispositivos móveis ou não móveis; controle e gerenciamento de ativos de tecnologia da informação.

16 DA SUBCONTRATAÇÃO

16.1 Os serviços serão executados por profissionais da contratada, sendo permitido a subcontratação de empresas para prestação dos serviços objeto deste contrato, limitado a 30%, nos termos do artigo 122, da Lei n 14.133/2021.

16.2 Em qualquer hipótese de uso de serviços de terceiros deve permanecer a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades das demais empresas, bem como responder perante o órgão Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da contratação.

17 DOS RECURSOS ORÇAMENTÁRIOS

17.1 Os serviços contratados serão suportados pela dotação orçamentária própria na classificação da conta nº 6.2.2.101.04.09.05 – Serviços de Informática - PJ.

18 DA VISTORIA

18.1 Não será exigido vistoria aos licitantes, mesmo porque, as empresas que atuam no segmento a ser licitado já possuem expertise necessária para precificar os serviços a serem prestados.

19 DA GARANTIA CONTRATUAL

19.1 Fica dispensada a garantia para a execução do contrato.

20 DOS CRITÉRIOS DE ACEITAÇÃO DO OBJETO E DEMAIS PROCEDIMENTOS

20.1 Critérios de aceitação:

20.1.1 A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

20.1.2 No prazo de até 5 dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

20.1.3 O recebimento provisório será realizado pelo fiscal técnico, administrativo e setorial ou pela equipe de fiscalização após a entrega da documentação acima, da seguinte forma:

- A contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.
- Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.
- A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou

materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

- Da mesma forma, ao final de cada período de faturamento mensal, o fiscal administrativo deverá verificar as rotinas previstas no Anexo VIII-B da IN SEGES/MP nº 5/2017, no que forem aplicáveis à presente contratação, emitindo relatório que será encaminhado ao gestor do contrato;
- No prazo de até 10 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

20.1.4 No prazo de até 10 (dez) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

- Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;
- Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
- Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização, com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

20.1.5 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

20.1.6 Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

20.2 Do pagamento:

20.2.1 O pagamento dos serviços e produtos serão realizados mediante a entrega dos mesmos, após aceitação e atesto do gestor do contrato e emissão da devida nota fiscal.

20.2.2 O CREA-SP efetuará o pagamento até o 30 (trigésimo) dia após a apresentação da nota fiscal/fatura, a qual deverá ser entregue ao Fiscal Administrativo do Contrato na Sede Faria Lima, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP, ficando a CONTRATADA obrigada a manter durante execução dos serviços os documentos apresentados na fase de habilitação.

20.2.3 As notas fiscais/faturas devem vir acompanhadas:

- Comprovante de Regularidade com o Fundo de Garantia do Tempo de Serviço– Certificado de Regularidade do FGTS CRF.
- Comprovante de regularidade para com a Fazenda Federal- Certidão de débitos relativos a créditos tributários
- Comprovante de inexistência de débitos inadimplidos perante a Justiçado Trabalho, mediante a apresentação de Certidão

20.2.4 A nota fiscal/fatura será analisada, minimamente, quanto aos itens a seguir descritos:

- Correlação entre os valores indicados na nota fiscal/fatura o da proposta da empresa.
- Ausência de emendas ou rasuras na nota fiscal/fatura.
- O correto preenchimento dos dados do CREA-SP (nome, CNPJ, dados contratuais) e da discriminação dos serviços;
- Pertinência dos cálculos aritméticos da nota fiscal/fatura – o valor total deverá corresponder ao somatório dos valores individuais lançados na mesma,
- Correlação entre o valor da nota fiscal e os valores empenhados;
- Correlação entre o CNPJ da CONTRATADA e o constante na proposta e na nota de empenho;

20.2.5 O Crea-SP efetuará retenção de impostos eventualmente incidentes sobre o valor do bem/serviço, conforme previsto na Lei Federal n° 9.430, de 27 de dezembro de 1996 e Instrução Normativa RFB no 1.234, de 11 de janeiro de 2012 e anexo;

20.2.6 A CONTRATADA é responsável pelos encargos fiscais, trabalhistas e previdenciários incidentes sobre os serviços contratados;

20.2.7 Se a CONTRATADA descumprir qualquer termo ou condição a que se obrigar no presente certame, por sua exclusiva culpa, poderá a Administração reter o pagamento, até que seja sanado o respectivo inadimplemento, não sobrevindo, portanto, qualquer ônus ao Conselho resultante desta situação;

20.2.8 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pelo CREA-SP, entre a data do vencimento e o efetivo

adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula, conforme previsto no ANEXO XI da IN SEGES/MP 05/2017:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	(6 / 100) 365	I = 0,00016438
	TX - Percentual da taxa anual = 6%		

21 DOS PROCEDIMENTOS DE FISCALIZAÇÃO CONTRATUAL

21.1 A fiscalização e o acompanhamento dos serviços serão exercidos por representante previamente designado pelo CONTRATANTE.

21.2 O conjunto de atividades compete ao gestor da execução dos contratos, auxiliado pela fiscalização e pelo público usuário, conforme o caso, de acordo com as seguintes disposições:

- Gestão da Execução do Contrato: é a coordenação das atividades relacionadas à fiscalização técnica, administrativa, setorial e pelo público usuário, bem como dos atos preparatórios à instrução processual e ao encaminhamento da documentação pertinente ao setor de contratos para formalização dos procedimentos quanto aos aspectos que envolvam a prorrogação, alteração, reequilíbrio, pagamento, eventual aplicação de sanções, extinção dos contratos, dentre outros;

- Fiscalização Técnica: é o acompanhamento com o objetivo de avaliar a execução do objeto nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação dos serviços estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório, para efeito de pagamento conforme o resultado;

- Fiscalização Administrativa: é o acompanhamento dos aspectos administrativos da execução dos serviços nos contratos com regime de dedicação exclusiva de mão de obra quanto às obrigações previdenciárias,

fiscais e trabalhistas, bem como quanto às providências tempestivas nos casos de inadimplemento;

- Fiscalização Setorial: é o acompanhamento da execução do contrato nos aspectos técnicos ou administrativos, quando a prestação dos serviços ocorrer concomitantemente em setores distintos ou em unidades desconcentradas de um mesmo órgão ou entidade; e

- Fiscalização pelo Público Usuário: é o acompanhamento da execução contratual por pesquisa de satisfação junto ao usuário, com o objetivo de aferir os resultados da prestação dos serviços, os recursos materiais e os procedimentos utilizados pela contratada, quando for o caso, ou outro fator determinante para a avaliação dos aspectos qualitativos do objeto.

21.3 A CONTRATADA deverá indicar Preposto: funcionário representante da CONTRATADA com poder decisório, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

21.4 Ao Gestor de Contrato e aos fiscais fica assegurado o direito de exigir o cumprimento de todos os itens constantes do Termo de Referência, do Edital, da proposta comercial da empresa vencedora do certame e das cláusulas do contrato, podendo ser realizadas reuniões presenciais ou não entre o Gestor e o Preposto para avaliação dos serviços prestados no período e verificação do atendimento aos requisitos contratuais.

21.5 A fiscalização não exclui e nem reduz a responsabilidade da CONTRATADA, mesmo perante terceiros, por quaisquer irregularidades nos serviços, inclusive resultante de utilização de pessoal inadequado ou sem qualificação técnica necessária, não implicando corresponsabilidade do CONTRATANTE ou de seus operadores e prepostos.

21.6 A ausência de comunicação por parte do CONTRATANTE, referente à irregularidade ou falhas, não exime a CONTRATADA das responsabilidades determinadas neste Termo de Referência.

21.7 A CONTRATADA permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante a vigência do contrato, fornecendo informações, propiciando o acesso à documentação pertinente e aos serviços em execução e atendendo às observações e exigências apresentadas pela fiscalização.

21.8 Ao CONTRATANTE é facultado o acompanhamento de todos os serviços objeto deste Termo de Referência e do contrato, juntamente com representante credenciado pela CONTRATADA.

21.9 A execução do contrato deverá, ainda, ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos seguintes aspectos, quando for o caso:

- Os resultados alcançados em relação ao contratado, com a verificação dos prazos de execução e da qualidade demandada;
- Os recursos humanos empregados, em função da quantidade e da formação profissional exigidas;
- A qualidade e quantidade dos recursos materiais utilizados;
- A adequação dos serviços prestados à rotina de execução estabelecida;
- O cumprimento das demais obrigações decorrentes do contrato; e
- A satisfação do público usuário.

21.10 O descumprimento total ou parcial das responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas no instrumento convocatório e na legislação vigente, podendo culminar em rescisão contratual.

22 DEVERES E RESPONSABILIDADES DA CONTRATANTE

22.1 São obrigações do CREA-SP:

22.1.1 Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

22.1.2 Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

22.1.3 Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

22.1.4 Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

22.1.5 Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

22.1.6 Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

22.1.7 Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

22.1.8 Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

22.1.9 Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

22.1.10 A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

22.1.11 Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

22.1.12 Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

22.1.13 A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

23 DEVERES E RESPONSABILIDADES DA CONTRATADA

23.1 São obrigações da Contratada:

23.1.1 O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

23.1.2 Manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato.

23.1.3 A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

23.1.4 Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

23.1.5 Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

23.1.6 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

23.1.7 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

23.1.8 Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

23.1.9 Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

23.1.10 Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

23.1.11 Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

23.1.12 Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

23.1.13 Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

23.1.14 Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

23.1.15 Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

23.1.16 Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

23.1.17 Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

23.1.18 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

23.1.19 Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

23.1.20 Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

23.1.21 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

23.1.22 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

23.1.23 Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

23.1.24 Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços;

23.1.25 Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

23.2 OBRIGAÇÕES PERTINENTES À LGPD

23.2.1 As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

23.2.2 Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

23.2.3 É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

23.2.4 A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de sub-operação firmados ou que venham a ser celebrados pelo Contratado.

23.2.5 Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

23.2.6 É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

23.2.7 O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

23.2.8 O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

23.2.9 O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

23.2.10 Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

23.2.10.1 Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

23.2.11 O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

24 DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

24.1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a) der causa à inexecução parcial do contrato;
b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;
d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

24.2 Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

d) Multa:
- Moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (trinta) dias;
- O atraso superior a 90 (noventa) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
- Compensatória, para as infrações descritas nas alíneas “e” a “h”, das infrações, de 3% (dois por cento) do valor do Contrato.
- Compensatória, para a inexecução total do contrato prevista na alínea “c”, das infrações, de 2% (um por cento) do valor do Contrato.
- Para infração descrita na alínea “b”, das infrações, a multa será de 2% (um por cento) do valor do Contrato.
- Para infrações descritas na alínea “d”, das infrações, a multa será de 0,5% (meio por cento) do valor do Contrato.
- Para a infração descrita na alínea “a”, das infrações, a multa será de de 2% (um por cento) do valor do Contrato.

24.3 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

24.4 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

24.4.1 Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

24.5 Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a

diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

24.6 Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

24.7 A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

24.8 Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

24.9 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

24.10 A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

24.11 O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

24.12 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

24.13 Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

24.14 O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

24.15 Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

24.16 Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

24.16.1 ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

24.16.2 poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual

25 ANEXOS

- ANEXO II – Endereços Unidades do CREA-SP
- ANEXO III – Modelo de planilha de custos, quando da necessidade de mão de obra.
- ANEXO IV – Modelo de planilha de custos demais serviços.
- ANEXO V – Modelo de propostas de preços.
- ANEXO VI – POC – Prova de Conceito

ANEXO VI – POC – Prova de Conceito

1.1 ROTEIRO DA PROVA DE CONCEITO – POC

1.2 O CREA-SP, objetivando garantir a eficiência do processo licitatório, executará PROVA DE CONCEITO – POC, onde busca-se estancar as deficiências do CREA-SP de forma célere.

1.3 O Pregoeiro, logo após a definição da licitante classificada em primeiro lugar, efetuará a convocação da realização da POC, para análise de admissibilidade e avaliação técnica por parte da Comissão Técnica, constituída e coordenada pela equipe do CREA-SP, que deverá efetuar, a análise e comprovação dos requisitos técnicos e funcionais, conforme Roteiro da Prova de Conceito – POC.

1.4 Toda a infraestrutura de (hardware e software) necessária para demonstração do atendimento aos requisitos é de responsabilidade do licitante, assim como a massa de dados/informações necessárias para a demonstração. A plataforma para realização da POC deverá ficar disponível na WEB até o encerramento da realização da POC.

1.5 A POC será presencial, as datas e local de realização da POC e da retomada da sessão serão informadas na própria sessão pública e publicadas no sítio da licitação.

1.6 Será concedida uma única oportunidade de aplicação da POC por licitante.

1.7 A aceitação da solução proposta pela licitante ocorrerá mediante análise de admissibilidade e avaliação técnica (POC), conforme segue:

1.8 A realização da avaliação técnica e análise de admissibilidade (POC), deverá iniciar em até 02 (dois) dias úteis, contados da data da convocação pelo Pregoeiro.

1.9 A realização dos testes de admissibilidade da plataforma deverá ocorrer no horário comercial (09 horas às 18 horas) em dia previamente acordado entre as partes em ambiente disponibilizado pelo CREA-SP.

1.10 Caso a licitante não compareça e/ou não dê início aos testes de admissibilidade, conforme o roteiro de testes apresentado, dentro do prazo estipulado de até 24 (vinte e quatro) horas após convocação, a licitante será desclassificada e será convocada a próxima colocada.

1.11 O licitante, por meio do seu representante legal, acompanhado e orientado pela Comissão Técnica, deverá realizar, no prazo máximo de até 01 (um) dia útil, a análise e

avaliação de admissibilidade, no ambiente WEB por ele (licitante) disponibilizado, visando à realização do roteiro de testes de comprovação técnica, descrito no Roteiro da Prova de Conceito – POC, podendo ser prorrogado, mediante a justificativa e aprovação da Administração.

1.12 O roteiro de testes de comprovação da POC deverá ser executado e comprovado pelo licitante, sob o auxílio e orientação do CREA-SP, por meio da Comissão Técnica.

1.13 Será homologada a plataforma que atenda ao percentual mínimo de 100% (cem por cento) dos requisitos exigidos no Roteiro da Prova de Conceito – POC.

1.14 Caso a plataforma ofertada atenda aos critérios mínimos de 100% (cem por cento) dos requisitos exigidos no Roteiro da Prova de Conceito – POC, será emitido laudo de conformidade e o objeto licitatório será adjudicado à respectiva licitante declarada vencedora.

1.15 Caso não atenda aos critérios mínimos de 100% (cem por cento) exigidos, a plataforma apresentada será considerada inapta e a licitante será desclassificada, convocando-se sucessivamente o próximo classificado, conforme os critérios de seleção de proposta previstos no edital de licitação.

1.16 Para a realização da prova de conceito a LICITANTE convocada deverá comprovar as funcionalidades/requisitos técnicos, conforme o roteiro de teste abaixo:

NOME:_____

EMPRESA:_____

#	Item	SIM	NÃO	COMENTÁROS	NÃO AVALIADO
01	**Demonstrar que possui alertas no SOC em mais de 70% dos casos de Uso do framework Mitre ATT&CK**				
	O Security Operations Center (SOC) demonstra consistentemente uma eficácia superior na detecção de ameaças, alcançando uma taxa de alertas superior a 70% em diversos casos de uso. Essa notável conquista é resultado do emprego estratégico e meticuloso do framework Mitre ATT&CK, que nos permite mapear e entender as táticas, técnicas e procedimentos (TTPs) utilizados por adversários cibernéticos. Ao alinhar nossos recursos de segurança com as técnicas detalhadas no Mitre ATT&CK, conseguimos identificar padrões comportamentais e indicadores de comprometimento, permitindo-nos antecipar e responder				

	proativamente às ameaças. Essa abordagem orientada por padrões nos permite elevar nossa postura de segurança, garantindo que mais de 70% dos casos de uso sejam prontamente identificados e mitigados. Ao incorporar as melhores práticas do Mitre ATT&CK em nossas operações diárias, fortalecemos nossa capacidade de antecipar, adaptar e responder de maneira eficaz ao cenário de ameaças em constante evolução.				
02	**Demonstrar que o serviço está apto a identificar e responder ataques baseado em machine learning e inteligência artificial.**				
	Ao empregar algoritmos avançados de machine learning, analisamos continuamente padrões de comportamento e anomalias, permitindo-nos identificar potenciais ameaças de forma proativa. Nossa inteligência artificial, alimentada por conjuntos de dados robustos, oferece uma compreensão aprofundada do contexto, possibilitando respostas rápidas e precisas. O serviço não apenas se destaca na identificação precoce de ameaças, mas também na resposta efetiva, garantindo a contenção e a mitigação rápida de incidentes. Nossa abordagem baseada em machine learning e IA não apenas fortalece a segurança, mas também proporciona uma defesa adaptativa capaz de aprender e evoluir diante de novas ameaças, mantendo a integridade dos sistemas e dados de nossos clientes. Ao adotar essa tecnologia de ponta, nosso serviço se posiciona como um guardião robusto, preparado para enfrentar os desafios emergentes no cenário cibernético, proporcionando uma camada adicional de proteção para garantir a segurança digital em todos os níveis.				
03	**Demonstrar capacidade de responder a ataques ransomware com sucesso de recuperação**				
	Nossa organização reforça sua posição como uma entidade resiliente e preparada para enfrentar os desafios iminentes representados pelos ataques de ransomware. Diante da crescente ameaça representada por ataques ransomware, desenvolvemos e implementamos estratégias de resposta que visam não apenas conter a propagação do ataque, mas também restaurar operações normais de maneira eficaz e eficiente. Nossa abordagem análise forense avançada e tecnologias de ponta para mitigar os danos causados por esses ataques.				

	Ao demonstrar uma taxa de sucesso notável na recuperação após ataques ransomware, reiteramos nosso compromisso inabalável com a segurança cibernética e a continuidade dos negócios. Estamos preparados não apenas para resistir a esses ataques, mas também para restaurar a normalidade operacional com rapidez e eficácia, salvaguardando os interesses e a confiança de nossos stakeholders				
04	Comprovar as habilidades de conhecimento técnico				
	Simulação do ambiente no estilo Capture the Flag (CTF). A bandeira digital geralmente é um arquivo ou uma sequência específica de caracteres que os participantes precisam encontrar e extrair de servidores, aplicativos ou outros alvos de teste. Essa competição simula cenários do mundo real em que os participantes precisam usar suas habilidades em hacking ético, resolução de problemas e análise de sistemas para encontrar vulnerabilidades e explorá-las para obter as bandeiras.				