



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

Anexo A

CADERNO TÉCNICO – PRODUTOS E SERVIÇOS

1. OBJETO

- 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 toda a infraestrutura e serviços que proporcionem o monitoramento e segurança para o ambiente tecnológico do CREA-SP incluindo as respectivas unidades localizadas no Estado de São Paulo.

2. FORNECIMENTO

2.1. Tabela Fornecimento

Item	Quantidade	Especificação	Unidade
1	36	Fornecimento de infraestrutura de monitoramento composta por hardware e softwares conforme os requisitos mínimos exigidos nesse termo, incluindo o fornecimento de videowall específicos a ser instalados nas dependências do CREA-SP.	Meses
2	36	Prestação de serviços de NOC e SOC (Serviços de monitoramento de disponibilidade, performance e gestão de chamados, bem como, correlação de eventos de segurança cibernética, gestão de vulnerabilidade, resposta a incidentes e gestão das soluções fornecidas conforme descrita nesse termo.)	Meses

3. REQUISITOS GERAIS

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

- 3.1.1.** Fornecimento e implementação de infraestrutura e serviços destinados a garantir a segurança das comunicações entre as 187 unidades do CREA-SP;
- 3.1.2.** 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;
- 3.1.3.** O CREA-SP possui uma rede de fibra ótica que interliga as unidades da capital. A rede é composta por fibra óptica apagada com elementos ativos que são configurados a critério do CREA SP.

- a) Sede Faria Lima
- b) Sede Rebouças,



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

- c) Sede Angélica
- d) Unidade Nestor Pestana
- e) Unidade Norte
- f) Unidade Oeste
- g) Unidade Leste
- h) Unidade Sul
- i) Unidade Barra Funda
- j) Unidade Call Center

3.1.4. Detalhes Específicos da Infraestrutura:

- a) O CREA-SP possui uma rede MPLS que interliga suas 187 unidades distribuídas no estado de São Paulo, em diversos municípios
- b) O CREA-SP possui uma interligação com a Empresa de Datacenter via Link de Fibra Óptica.
- c) O CREA-SP possui uma interligação com a Empresa de Call Center através de Link dedicado.

3.1.5. A Rede do Crea-SP possui quatro saídas para internet.

- a) Na unidade Faria Lima, com 200 Mbps
- b) Na unidade Angélica, com 200 Mbps
- c) Na unidade Nestor Pestana, com 200Mbps
- d) No Datacenter da empresa contratada do CREA-SP com capacidade de 300Mbps

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

- a) 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 potenciais vulnerabilidades de forma a mitigar ataques e consequentemente danos a este Conselho;
- b) A descrição pormenorizada dos serviços está detalhada no Item respectivo.
- c) 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.

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

- a) Potenciais e futuros problemas e gargalos – Preventiva;
- b) Falhas causando Degradação de desempenho e suas respectivas causas –



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

- Corretiva;
- c) Interrupção dos Serviços e suas respectivas causas;
 - d) Corretiva; Detecção de ameaças cibernéticas à sistemas, tais como como tentativas de invasão e/ou paralisação: páginas web, aplicativos e bases de dados;
 - e) solução de problemas de segurança encontrados com agilidade e eficiência;
 - f) monitorar e analisar processos de forma contínua para identificar riscos de segurança na infraestrutura de TI.
 - g) Além disso os serviços prestados atuarão em tempo real e sobre todos os sistemas monitorados, para:
 - h) registrar e documentar todas as ocorrências acima listadas incluindo as que ameacem a segurança do ambiente de TI;
 - i) 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;
 - j) acompanhar a resolução dos problemas e apontar as soluções e providências tomadas;
 - k) 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.
 - l) 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 vigência do contrato.

4. REQUISITOS DOS SERVIÇOS

- 4.1.** Todos os serviços deverão ser prestados por meio de Centro de operações de NOC/SOC o qual deverá ser disponibilizado pela CONTRATADA, nas instalações do CREA-SP na Av. faria Lima, 1059, São Paulo/SP, e em suas próprias instalações, em total conformidade com a especificação deste Termo de Referência, e de acordo com os requisitos mínimos descritos a seguir:
- 4.2.** Possuir em operação NOC/SOC, no mínimo, 2 (dois) canais de comunicação IP dedicados com a Internet, com provedores distintos, para a prestação de serviços de monitoramento e suporte remoto via VPN site-to-Site com a CONTRATADA.
- 4.3.** Não serão aceitos contratos com links xDSL, devido ao baixo NMS ofertado pelas operadoras de telecomunicação para este tipo de tecnologia.
- 4.4.** Possuir NOC/SOC, com no mínimo, 2 (duas) linhas de telefonia fixa, celular ou por IP, de diferentes operadoras. Os números de telefone deverão ser fornecidos pela CONTRATADA.



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

- 4.5.** Efetuar registro de entrada e saída dos profissionais e visitantes, com identificação individual, em todos os acessos ao NOC/SOC, objetivando a proteção de qualquer informação relativa à CONTRATANTE.
- 4.6.** O perímetro do NOC/SOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido.
- 4.7.** A Contratada deverá disponibilizar "Central de Atendimento" para realização de requisições de execução de serviços ou resolução de dúvidas, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante número do tipo 0800 ou com custo local para São Paulo. Esse serviço poderá ser disponibilizado em meio eletrônico e/ou e-mail.
- 4.8.** Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.
 - 4.8.1.** Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.
- 4.9.** O Centro de operações NOC/SOC da contratada deverá dispor de uma solução de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI).
- 4.10.** A ferramenta de gestão de chamados deverá ter seus processos de gestão de incidentes, gestão de problemas, gestão de requisições e gestão de mudanças aderentes ao modelo ITIL v4;
- 4.11.** A solução de gestão de chamados deverá realizar o controle automático dos ANSs (Acordos de Nível de Serviço) dos chamados, notificando e escalonando os chamados próximos de um rompimento;
- 4.12.** A solução de gestão de chamados deverá possibilitar o envio automático, por e-mail, de relatórios à usuários pré-determinados pela contratante;
- 4.13.** A solução de gestão de chamados deverá possuir API de integração via REST/SOAP.
- 4.14.** A Ferramenta de gestão de chamados deve ser um produto acabado, totalmente funcional e que atenda a todas as especificações técnicas estabelecidas neste termo de referência. Não serão aceitas versões incompletas ou beta do software. O software deve



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

estar pronto para uso imediato, sem a necessidade de atualizações ou modificações para cumprir os requisitos estabelecidos;

4.15. Serviços Gerenciados de Monitoramento de Ambiente Tecnológico – NOC

4.15.1. A CONTRATADA deverá monitorar todo o parque tecnológico utilizando-se da ferramenta atual em produção. No presente, a ferramenta atual em produção é a plataforma ZABBIX.

4.15.2. O Monitoramento, no horário compreendido entre 08:00hs e 19:00hs de 2ª a 6ª feira, deverá ser feito por profissionais que deverão estar alocados nas instalações físicas do CREA-SP na Av. Faria Lima 1059 - Pinheiros, São Paulo - SP, 01452-000. Fora do horário estabelecido neste item o monitoramento deve ser feito diretamente pelo NOC/SOC da CONTRATADA em suas próprias instalações físicas, de forma ininterrupta.

4.15.3. A equipe do NOC deverá ser formada por profissionais N1, profissionais N2 e Gerente de NOC, cujas formação e experiência mínima constam deste Termo de Referência;

4.15.4. Das atividades da equipe do NOC como sendo N1;

4.15.4.1. Receber alertas das soluções os eventos e incidentes na ferramenta de monitoramento (zabbix e/ou equivalente(s)).

4.15.4.2. Analisar os eventos da Ferramenta de monitoramento, realizando a triagem dos mesmos e abertura de tickets na ferramenta ITSM do CREA-SP.

4.15.4.3. Realizar o suporte ao usuário final do CREA-SP referente a solução dos problemas identificados;

4.15.4.4. Participar das reuniões de câmara e plenárias presencialmente dando o suporte necessário;

4.15.4.5. Visitar as unidades na Capital de São paulo para solucionar problemas identificados;

4.15.4.6. Definir prioridade dos eventos considerados de acordo com escala de criticidade definidas junto a CONTRATANTE.

4.15.4.7. Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATADA.

4.15.4.8. Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA.

4.15.4.9. Encaminhar eventos que não sejam de sua alçada ao N2 de acordo com os playbooks definidos pela CONTRATADA.



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

4.15.4.10. Acompanhar e encerrar os eventos após sua solução.

4.15.4.11. Sugerir ao Gerente do NOC/CREA-SP melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.

4.15.5. Das atividades da equipe do NOC como sendo N2;

4.15.5.1. Realizar todas as atividades de N1 quando/se necessário.

4.15.5.2. Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATANTE.

4.15.5.3. Reclassificar eventos e rever a prioridade, quando houver divergência de entendimento com relação ao definido pelo N1.

4.15.5.4. Analisar os eventos identificados, criando documento de Resposta a com as devidas ações de contenção, remediação e erradicação sugeridas as equipes resolvidoras.

4.15.5.5. Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA.

4.15.5.6. Na ocorrência de eventos de alta criticidade, alertar o Gerente do NOC formalmente, assim como proceder com matriz de escalonamento prevista.

4.15.5.7. Redirecionar incidentes para equipe N1 após tratativas realizadas para acompanhamento e encerramento.

4.15.5.8. Realizar atividades de Predição de Eventos de Performace, em busca ativa por atividades suspeitas no ambiente da CONTRATANTE.

4.15.5.9. Realizar atividades de tuning nas ferramentas oferecidas pela CONTRATADA para aprimorar a cobertura dos eventos em segurança cibernética.

4.15.5.10. Revisar atividades de parseamento, buscando que as ferramentas proporcionem dados qualitativos em seus eventos.

4.15.5.11. Acompanhar e suportar integrações entre os ativos de rede da CONTRATANTE junto a solução oferecida da CONTRATADA.

4.15.5.12. Sugerir ao Gerente do NOC melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.

4.15.5.13. Realizar melhorias nos playbooks após alinhamento entre partes interessadas.

4.15.5.14. Gerar relatórios técnicos dos eventos.



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

4.15.6. Das atividades Gerenciais do gerente do NOC

- 4.15.6.1.** Coordenar tecnicamente os serviços e o andamento das atividades, projetos e demandas das equipes N1 e N2 do NOC;
- 4.15.6.2.** Supervisionar os perfis profissionais do N1 e N2 delegar responsabilidades e serviços às equipes e acompanhar seu desempenho;
- 4.15.6.3.** Gerir o cumprimento de metas e indicadores estabelecidos;
- 4.15.6.4.** Elaborar relatórios de acompanhamento dos indicadores de serviço, assim como propostas de melhorias da execução do serviço e de sua medição;
- 4.15.6.5.** Garantir o bom desempenho da equipe;
- 4.15.6.6.** Manter a equipe N1 e N2 devidamente treinada e apta a prestar os serviços ora contratados;
- 4.15.6.7.** Fornecer informações solicitadas pela CONTRATANTE;
- 4.15.6.8.** Assegurar que os processos operacionais tenham melhoria contínua e atendam aos Indicadores e metas acordadas em contrato;
- 4.15.6.9.** Realizar auditorias dos atendimentos dos eventos e incidentes cibernéticos e tickets realizados pelos perfis profissionais de N1 e N2, com o objetivo de avaliar e aferir a observância aos padrões, procedimentos e qualidade do serviço prestado, bem como o cumprimento dos scripts, playbooks, padrões de cordialidade e empatia exigidos;
- 4.15.6.10.** Apresentar Relatório de acompanhamento de indicadores de uso de recursos, atendimento, desempenho e utilização do serviço.
- 4.15.6.11.** Interagir com a equipe técnica da CONTRATANTE no atendimento aos quesitos CONTRATUAIS e melhoria dos serviços prestados.

4.15.7. A CONTRATADA, deverá fornecer e implantar nas dependências do CREA-SP, situado à Av. Faria Lima 1059 - Pinheiros, São Paulo - SP, 01452-000 toda(s) a(s) plataforma(s) de hardware(s) e software(s) especificadas neste Termo de Referências necessárias prestação dos serviços ora especificados neste Termo de Referência por parte da que estará alocada nestas mesmas dependências.

4.15.8. A contratada terá a responsabilidade de gerenciar de forma abrangente a ferramenta ZABBIX, englobando a adição, modificação e configuração de métricas de monitoramento



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

conforme as necessidades do ambiente da contratante. Além disso, caberá à contratada realizar ajustes técnicos na ferramenta, garantindo sua eficácia e precisão no acompanhamento de indicadores e eventos relevantes para o bom funcionamento dos sistemas e serviços monitorados.

4.15.9. A CONTRATADA deverá fornecer toda a solução de monitoramento complementar necessária, para que seja monitorado os links de internet de forma externa, bem como qualquer outro elemento a ser monitorado que esteja listado neste Termo de Referência.

4.15.10. Os serviços de monitoração deverão ser prestados sob o regime de atuação 24x7x365, da seguinte forma:

4.15.10.1. 2ª a 6ª feira das 08:00hs as 19:00hs deverão ser prestados, impreterivelmente, pela equipe alocada nas dependências do CREA-SP e com supervisão do NOC nas dependências da CONTRATADA.

4.15.10.2. 2ª a 6ª feiras das 19:01hs às 7:59hs, sábados, domingos e feriados a partir do NOC nas dependências da CONTRATADA.

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

4.15.11.1. Monitoramento de Rede:

- A contratada deve prover monitoramento contínuo e em tempo real de todos os ativos de tecnologia que compõe a rede, servidores e sistemas do CREA-SP, nas dependências da sede do CREA-SP da Av. Faria Lima, com equipe especializada e de comprovada experiência. Utilizará infraestrutura avançada, a ser disponibilizada nas dependências do CREA-SP, incluindo hardware e software, para assegurar a detecção precoce e resposta a problemas de desempenho, falhas e ameaças à segurança. Elementos a serem monitorados:

4.15.11.2. Rede:

- Status (Online/Offline);
- Velocidade de conexão;
- Latência;
- Perda de pacotes;
- Jitter;
- Total de dispositivos conectados;

4.15.11.3. Monitoramento de Links de Comunicação 3.2.G.G.1. Rede de Fibra Apagada

- A contratada deverá realizar o monitoramento contínuo de todos os links de fibra apagada e seus respectivos equipamentos usados para iluminar a rede da contratante, visando garantir a integridade e a disponibilidade da comunicação. É de responsabilidade da



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

contratada abrir chamado junto à operadora de telecomunicações para investigar e resolver problemas nos links, tais como perdas de pacote, latência excessiva e indisponibilidade. O objetivo é assegurar um ambiente de rede estável e eficiente para suportar as operações da contratante de forma ininterrupta.

4.15.11.4. MPLS

- A contratada deverá realizar o monitoramento contínuo de todos os links MPLS da contratante, visando garantir a integridade e a disponibilidade da comunicação. É de responsabilidade da contratada abrir chamado junto à operadora de telecomunicações para investigar e resolver problemas nos links, tais como perdas de pacote, latência excessiva e indisponibilidade. O objetivo é assegurar um ambiente de rede estável e eficiente para suportar as operações da contratante de forma ininterrupta.

4.15.11.5. Internet

- A contratada deverá realizar o monitoramento contínuo de todos os links Internet da contratante, visando garantir a integridade e a disponibilidade da comunicação. É de responsabilidade da contratada abrir chamado junto à operadora de telecomunicações para investigar e resolver problemas nos links, tais como perdas de pacote, latência excessiva e indisponibilidade. O objetivo é assegurar um ambiente de rede estável e eficiente para suportar as operações da contratante de forma ininterrupta.

4.15.11.6. Access Points (APs):

- Status (Online/Offline);
- Número de dispositivos conectados;
- Detecção automática de novos dispositivos.

4.15.11.7. Servidores:

- Status (Online/Offline);
- Temperatura;
- Uso de CPU e memória;
- Logs de sistema;
- Número de usuários conectados;
- Detalhes de conexão (usuário, data e hora);
- Aplicações: Configuração de monitoramento conforme requisitos do CREA, incluindo parâmetros específicos de desempenho e segurança. Registro e análise de logs para detecção precoce de incidentes ou falhas;
- Acompanhamento do número de sessões e usuários ativos

4.15.11.8. Monitoramento de Servidores e de Nuvem.

- O serviço incluirá monitoramento abrangente de servidores, tanto locais quanto



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

hospedados em ambientes de nuvem, utilizando técnicas avançadas e ferramentas especializadas. Este monitoramento visa garantir a máxima disponibilidade, eficiência operacional e segurança dos dados.

4.15.11.9. Monitoramento de Nuvem:

- Gestão de recursos e serviços em nuvem, com foco na otimização de custos e performance;
- Monitoramento de serviços de nuvem para conformidade com políticas de segurança e governança;
- Avaliação da integridade e desempenho de instâncias, funções e contêineres na nuvem.
- Monitoramento de tráfego em ambientes de nuvem;

4.15.11.10. Monitoramento de Máquina Virtual. Monitoramento de Aplicativos.

4.15.11.11. 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.

4.15.11.12. Monitoramento de Máquinas Virtuais:

- Status (Online/Offline);
- Temperatura;
- Uso de CPU e memória;
- Logs de sistema;
- Número de usuários conectados;
- Detalhes de conexão (usuário, data e hora);
- Aplicações: Configuração de monitoramento conforme requisitos do CREA, incluindo parâmetros específicos de desempenho e segurança. Registro e análise de logs para detecção precoce de incidentes ou falhas;
- Acompanhamento do número de sessões e usuários ativos
- Detecção e alerta de falhas de sistema, sobrecarga de recursos ou outros problemas de performance;

4.15.11.13. Monitoramento de Banco de Dados.

4.15.11.14. Este serviço é dedicado ao monitoramento contínuo e abrangente de bancos de dados (PostgreSQL, MySQL, DB2, SQL Server 2008 e PostgreSQL), garantindo sua performance, integridade, segurança e disponibilidade. Funcionalidades do Serviço Incluem:

- Performance e Otimização: Monitoramento em tempo real do desempenho dos bancos



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

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;

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

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

4.15.11.16. 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.

4.15.11.17. Todos os incidentes identificados durante a monitoração deverão ser automaticamente registrados na ferramenta de ITSM (Gestão de Serviços de TI). Este registro deverá ocorrer de forma imediata e precisa, garantindo a integridade e rastreabilidade de todas as ocorrências.

4.15.11.18. Monitoramento da rede Wi-Fi.

- Este serviço é dedicado ao monitoramento contínuo e abrangente no que tange a rede Wi-Fi e seus componentes (Controladora Cisco 5520, Access Points linha 28XX) garantindo sua performance, integridade, segurança e disponibilidade. Funcionalidades do Serviço Incluem:
- Monitoramento de performance e disponibilidade.
- Número de conexões por SSID
- Quantidade de clientes por Access Point.
- Portas de conexão
- Processamento
- Memória
- Fonte de alimentação

4.16. Instalação do Centro de Monitoramento CREA-SP.

4.16.1. A CONTRATADA deverá fornecer, instalar e manter, na sede Faria Lima do CREA-SP, toda(s) a(s) plataforma(s), composta(s) por Hardware(s) e Software(s), especificadas neste Termo de Referência, as quais são responsáveis pela(s) coleta(s) da(s) informações e respectivo monitoramento de todo o ambiente de TI do CREA-SP, descrito neste Termo.

4.16.2. A CONTRATADA fornecer sistema completo de visualização que por sua vez, deve ser projetado e fabricado para operação contínua, 24 horas por dia, 7 dias por semana, incluindo todo o hardware, software e os recursos necessários de modo a permitir a



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

visualização e operação do sistema;

- 4.16.3.** O Painel Gráfico deverá formar uma matriz (03 colunas x 02 linhas) com 6 módulos/monitores, totalizando um único display, ou a critério da CONTRATANTE, formar duas matrizes com 03 colunas x 02 linhas e 02 colunas x 02 linhas respectivamente;
- 4.16.4.** Solução para controle dinâmico de conteúdo, capaz de gerenciar múltiplos monitores, fisicamente instalados como conceito de vídeo Wall, permitindo controle local e remoto;
- 4.16.5.** A solução proposta deverá seguir os preceitos "bundle", ou seja, contemplar todo o hardware e o software necessário ao funcionamento do vídeo wall, incluindo interfaces físicas eventuais licenças (se aplicáveis);
- 4.16.6.** Permitir a criação de múltiplos tipos de mosaico, além de autorizar a desativação da(s) interface(s) de saída inutilizadas;
- 4.16.7.** Tecnologia: LED.
- 4.16.8.** Diagonal do Módulo LED de tamanho 65".
- 4.16.9.** Montagem: Horizontal ou Vertical.
- 4.16.10.** Nível de Contraste mínimo: 1200:1.
- 4.16.11.** Resolução nativa mínima Individual do Módulo: 1920x1080 pixels.
- 4.16.12.** Interfaces mínimas: 1 x HDMI; 1 x DVI-D; 1 x RJ45; 1 x Display Port, RS-232 (entrada e saída): 1 x áudio (3.5mm), serão aceitos adaptadores para portas DVI e Display Port.
- 4.16.13.** Alimentação Elétrica do Painel bivolt: 100- 230 Vca – 50/60 Hz com chaveamento automático.
- 4.16.14.** Possuir compatibilidade com suportes padrão VESA · MTBF: 50.000 horas.
- 4.16.15.** Requisitos Mínimos do Gerenciador de imagens para Vídeo Wall.
- 4.16.16.** O Controlador do painel gráfico deve ser fornecido completo com todos os recursos de hardware, software básicos (sistema operacional) e software gerenciado gráfico, com suas respectivas licenças necessárias para a perfeita operação dos painéis gráficos de visualização;
- 4.16.17.** Deverá ter capacidade para decodificar em um único monitor no mínimo 06 (seis) imagens de vídeo streaming.
- 4.16.18.** Compatibilidade com o formato de vídeo H.264 e H.265;



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

- 4.16.19.** Suportar fontes de conteúdo com resolução 4K;
- 4.16.20.** O controlador gráfico e o software de controle do Vídeo Wall deve ser do mesmo fabricante, ou o software deverá ser instalado exclusivamente em equipamento homologado pelo fabricante do software;
- 4.16.21.** O controlador gráfico deve permitir transformar o conjunto de telas numa única tela lógica de alta resolução com no mínimo a resolução total dos monitores;
- 4.16.22.** Deve permitir conexão com a rede ethernet 100/1000 Mbps com conector RJ45;
- 4.16.23.** Deve permitir a exibição simultânea de múltiplos aplicativos via rede TCP/IP e as entradas de vídeo digital;
- 4.16.24.** O hardware deve possuir capacidade de processamento, memória, placas gráficas e discos compatível com a exibição de imagens em tempo real, na resolução nativa, sem atrasos de atualização e exibição e permitir o gerenciamento de múltiplas fontes de informações simultaneamente;
- 4.16.25.** Plataforma de gerenciamento de imagem baseado em "nodes" interconectados entre si, onde a falha de um node não afeta o funcionamento do restante do painel;
- 4.16.26.** Deve ser possível a visualização simultânea de janelas de aplicativos em tempo real. As janelas de aplicativos deverão ser móveis e de dimensão livre, controladas através do software de gerenciamento do painel gráfico;
- 4.16.27.** Captura de tela de servidores, workstations e aplicações Microsoft.
- 4.16.28.** O software de ser capaz de capturar as janelas de aplicações mesmo que estejam em segundo plano. O sistema deverá permitir a visualização no painel, de aplicativos gráficos sem conflito de cores entre as aplicações e sem limitação de layouts possíveis, respeitando a resolução de vídeo nativa;
- 4.16.29.** Deve possuir configuração de layout de exibição com definição de posicionamento e dimensão das janelas de aplicativos;
- 4.16.30.** Deve permitir que o usuário customize por dimensionamento ou recorte da fonte que ele disponibilizará no Vídeo Wall;
- 4.16.31.** Deve permitir que usuários tenham privilégios diferenciados. Isto é, o software de gerenciamento do painel gráfico deverá permitir multiusuários com permissões diferenciadas para cada usuário.
- 4.16.32.** Os tipos de aplicações mínimas que deverão ser suportadas e controladas pelo software de gerenciamento: Vídeo Streaming (RTSP) e Cópias de Desktops.



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

- 4.16.33. Deverá incluir todo o hardware, software e os recursos necessários de modo a permitir a visualização e operação do sistema;
- 4.16.34. O controlador deverá permitir a visualização simultânea dos sinais provenientes dos encoders de captura de áudio e vídeo e também diretamente na rede através de protocolo RTSP;
- 4.16.35. Devem ser fornecidos no mínimo 6 (seis) encoders para codificação e vídeo DVI ou HDMI e áudio estéreo.
- 4.16.36. Devem ser fornecidos no mínimo 6 (seis) decoders para decodificação de sinal de vídeo;
- 4.16.37. Cada monitor do videowall deve ser ligado a uma porta de vídeo de saída através de cabo HDMI ou DVI, não sendo aceitas soluções com cascadeamento de vídeo;
- 4.16.38. Deve possuir no mínimo 4 canais distintos de saída DVI, HDMI ou DisplayPort, compatíveis com a porta de entrada do monitor do Item 01 deste Termo de Referência;
- 4.16.39. Os sistemas computacionais devem ser fornecidos acompanhados de todos os softwares e respectivas licenças, com direito de uso permanente, que sejam necessários à execução das tarefas e aplicativos descritos e/ou que sejam disponibilizados pela solução ofertada.
- 4.16.40. A CONTRATANTE disponibilizará pontos de elétrica e rede para conectividade.
- 4.16.41. É de responsabilidade da CONTRATADA o reparo, substituição e manutenção de quaisquer componentes ou softwares integrantes a solução.
- 4.17. **Serviços de Monitoramento de Segurança Cibernética – SOC**
 - 4.17.1. Prestação de Serviços Gerenciados obrigatoriamente através de SOC –Security Operations Center/Centro de Operações de Segurança.
 - 4.17.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados a CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.
 - 4.17.1.2. Cabe ressaltar que toda a prestação dos serviços a serem contratados se dará através e sob o fornecimento na forma de SERVIÇOS onde os softwares necessários para a proteção do ambiente são fornecidos e operados pela contratada.



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

- 4.17.1.3.** A CONTRATADA, que garantirá a aplicação contínua das melhores práticas. Tal modelo evidencia-se mais efetivo e possibilita a utilização de produtos, serviços, soluções de segurança por um menor custo, haja vista a possibilidade de utilização de recursos em escala, por serem compradas em grande quantidade pelo fornecedor para atender a diversos clientes e, dessa maneira obtendo vantagens de preços aquisitivos.
- 4.17.1.4.** Portanto, considerando a importância dos serviços de segurança de TIC e para a proteção dos diversos ativos, serviços e sistemas da CONTRATANTE, aliado à insuficiência de profissionais especializados em seu quadro de colaboradores e necessários ao atendimento dessa demanda, torna-se essencial para a adequada proteção do ambiente tecnológico a contratação de Prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA.
- 4.17.1.5.** Prestação de Serviços Gerenciados de Segurança da Informação com o fornecimento de Solução de Correlação e Gerenciamento de Eventos de Segurança (SIEM), Solução de EDR, Solução de proteção de APIs, bem como Solução de WAF contemplando também Análise de Vulnerabilidades, Pentest e Suporte Técnico aos Serviços contratados. Atendimento de Chamados através de Sistema de Service Desk, também e inclusive a prestação concomitante dos demais Serviços, dos quais deverão ser prestados por uma única empresa vencedora deste termo de referência, descritos nos itens abaixo e no inteiro teor deste TR:

4.17.2. Centro de Operação de Operações de Segurança (SOC):

- 4.17.2.1.** Os Serviços Gerenciados de Segurança deverão ser prestados por meio de estrutura de SOC - Security Operation Center, a qual deverá ser fornecida pela CONTRATADA, obrigatoriamente nas dependências do CREA-SP, situado à Av. Faria Lima, 1509, - Pinheiros, São Paulo - SP, 01452-000, e executado por profissionais, das 08:00h às 19:00h, nas mesmas dependências e instalações aqui descritas. Fora do horário aqui indicado, o serviço deve ser prestado em ambiente físico da própria CONTRATADA. O SOC deverá sustentar e operar toda a solução e produtos que estiverem relacionados com a Segurança da Informação, assim como do Parque Computacional da CONTRATANTE, com a realização continuada de ações proativas voltadas para mantê-lo estável, seguro, em pleno e normal funcionamento, sempre disponível e inalterada.
- 4.17.2.2.** A CONTRATADA deverá disponibilizar ferramenta automatizada para prover os serviços de monitoramento e visibilidade de ataques cibernéticos como serviço assim como equipe técnica capacitada para analisar os indicadores fornecidos pelas ferramentas, indicando proativamente a existência de incidentes cibernéticos, sendo definido como um evento com potencial de ocasionar uma possível violação na política de segurança da informação da CONTRATANTE. A CONTRATADA deverá notificar a CONTRATANTE diante da detecção de qualquer evento suspeito,



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

provendo todo o embasamento que respalde a notificação encaminhada.

- 4.17.2.3.** As atividades de monitoramento consistem em detecção, triagem, categorização, priorização, análise inicial, notificação, contenção (quando aplicável), resposta a incidente com recomendações para contenção, mitigação, erradicação, assim como escalonamento (quando aplicável).
- 4.17.2.4.** A equipe do SOC deverá ser formada por profissionais N1, profissionais N2 e Gerente de SOC, nas quantidades e experiências mínimas constantes deste Termo de Referência;
- 4.17.2.5.** Esse serviço será dividido em dois níveis (nível 1-N1 e nível 2-N2), com foco nos Ativos e Sistema de TIC da CONTRATANTE.
- 4.17.2.6.** Avaliações de incidentes devem seguir Frameworks consolidados no mercado de segurança da informação, como SANS e NIST.
- 4.17.2.7.** Incidentes devem ser enriquecidos com Threat Modelings consolidados no mercado de segurança da informação, como MITRE, CVSS e Cyber Kill Chain.
- 4.17.2.8.** Essas metodologias são reconhecidas internacionalmente como as melhores práticas de segurança cibernética e devem ser aplicadas pela CONTRATADA para garantir a conformidade com as normas e regulamentações aplicáveis.
- 4.17.2.9.** Monitorar e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados), propondo ações corretivas e de melhorias.
- 4.17.2.10.** Cabe a equipe técnica da CONTRATADA, apoiar as integrações pertinentes para que os logs de segurança sejam encaminhados adequadamente as soluções de monitoramento.
- 4.17.2.11.** Nos processos de integrações, a CONTRATADA se compromete a aplicar sua expertise em monitoramento para a seleção dos dados que realmente se requerem para o monitoramento do ambiente TIC da CONTRATANTE.
- 4.17.2.12.** Como processo contínuo, a CONTRATADA realizará processos de Tunning nos serviços ofertados, visando qualificar os eventos identificados e diminuir detecções de eventos classificados como falso positivo.
- 4.17.2.13.** A CONTRATADA executará o monitoramento do ambiente TIC da CONTRATANTE em busca de Precursores, Incidentes e Indicadores de Comprometimento assim como qualquer alerta de segurança disponível.
- 4.17.2.14.** Durante o processo de Triagem, comportamentos suspeitos poderão ser notificados



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

até que comportamentos comuns sejam identificados e documentados, evitando assim sobrecarga futura da equipe de SI da CONTRATANTE.

- 4.17.2.15.** A Classificação e Priorização dos incidentes de segurança seguirão modelos adotados pela CONTRATADA, seguindo rigorosamente os Frameworks adotados pelo mercado de segurança cibernética.
- 4.17.2.16.** Caso a CONTRATANTE requeira revisão de Classificações e Prioridades, estas devem ser realizadas em comum acordo durante o processo de contratação dos serviços.
- 4.17.2.17.** A contenção de determinados tipos de eventos, ficará a cargo da CONTRATADA, e o mesmo deverá ser documentado em procedimentos e playbooks pela CONTRATADA.
- 4.17.2.18.** Com base em ferramentas de Threat Intelligence, públicas ou privadas, os incidentes em segurança cibernética serão enriquecidos pela CONTRATADA provendo o adequado insumo para a tomada de decisão da equipe de técnica da CONTRATANTE.
- 4.17.2.19.** A CONTRATADA, deve, por meio de seu documento de Resposta a Incidente, subsidiar a equipe de SI da CONTRATANTE no que tange aos procedimentos para adequada contenção, remediação e erradicação de um incidente.
- 4.17.2.20.** Incidentes de segurança terão seus respectivos documentos de Resposta a Incidente lavrados assim como seu adequado registro em ferramenta de ITSM.
- 4.17.2.21.** Incidentes de segurança cibernética que sejam prioritários e atendam critérios de criticidades dispostos neste documento, terão seu fluxo de escalonamento seguidos conforme alinhado entre partes interessadas.
- 4.17.2.22.** Para incidentes críticos, a equipe de CSIRT da CONTRATADA deverá ser engajada no suporte a contenção, remediação e erradicação, sem custos adicionais a CONTRATANTE.
- 4.17.2.23.** A CONTRATADA se dispõe a realizar buscas ativas, Threat Hunting, nas soluções de segurança ofertadas em busca de eventos anômalos que possam afetar integridade, disponibilidade e confidencialidade dos ativos TIC da CONTRATANTE.
- 4.17.2.24.** Incidentes e requisições podem ter como natureza de contato, telefone, e-mail, chat e portal de autoatendimento.
- 4.17.2.25.** Independente da natureza de contato realizada, o ITSM deverá gerar código único de registro para posterior acompanhamento.



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

- 4.17.2.26.** A ferramenta de ITSM notificará a Contratante com número único de registro assim como permitirá a contratante o acompanhamento de seus incidentes e requisições.
- 4.17.2.27.** O registro dos eventos deverá ser realizado na ferramenta de ITSM da CONTRATANTE.
- 4.17.2.28.** Registros nas ferramentas de ITSM, tanto para incidentes, requisições e mudanças, devem seguir as melhores práticas oferecidas por Frameworks como ITIL.
- 4.17.2.29.** Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades.
- 4.17.2.30.** É de responsabilidade da CONTRATADA a criação, revisão e manutenção de tais procedimentos operacionais, sendo de responsabilidade da CONTRATANTE apenas participar como aprovador sempre que um procedimento for criado e/ou sofrer algum tipo de alteração.
- 4.17.2.31.** É de responsabilidade da CONTRATADA manter uma base de conhecimento, com todos os procedimentos pré-estabelecidos e aprovados pela CONTRATANTE. Tal base de conhecimento deve fazer parte do sistema de acompanhamento de chamados, e a qualquer tempo deve estar acessível à CONTRATANTE para consultas, aprovações e alteração de novos procedimentos.
- 4.17.2.32.** Ao final do contrato a CONTRATADA deve realizar a consolidação da base de conhecimento e entregar ao CREA em formato digital, editável (docx).
- 4.17.2.33.** A CONTRATADA deve realizar integração de sua ferramenta de ITSM, com o ITSM (GLPI) da CONTRATANTE, formando uma base de conhecimento de todos os incidentes e requisições de serviço unificada.
- 4.17.2.34.** A CONTRATADA deve desenvolver e implementar uma variedade de playbooks de atendimento de incidentes que abordem os diferentes tipos de incidentes de segurança que possam ocorrer nos ativos de TIC da CONTRATANTE.
- 4.17.2.35.** Esses playbooks devem incluir procedimentos claros para avaliação de incidentes, priorização, categorização, triagem e resposta.
- 4.17.2.36.** A CONTRATADA deve fornecer um conjunto abrangente de indicadores de segurança e dashboards na plataforma Graphana, ou equivalentemente, personalizados para que a CONTRATANTE possa avaliar continuamente a eficácia dos serviços.
- 4.17.2.37.** A Contratada deve fornecer acesso de leitura aos analistas do CREA-SP aos Logs de Eventos da ferramenta de todas as ferramentas segurança utilizadas na solução fornecida ao CREA-SP.



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

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

4.17.2.39. A CONTRATADA realizará reuniões periódicas visando apresentar pontos que requeiram atenção de partes interessadas, assim como alinhamento de expectativas com a CONTRATANTE.

4.17.3. Das atividades da equipe do SOC como sendo N1;

4.17.3.1. Receber alertas das soluções de segurança e registrar os eventos e incidentes na ferramenta de ITSM.

4.17.3.2. Analisar os eventos registrados na ferramenta de ITSM, realizando a triagem dos verdadeiros positivos e falsos positivos.

4.17.3.3. Definir prioridade dos eventos considerados como verdadeiros positivos de acordo com escala de criticidade definidas junto a CONTRATANTE.

4.17.3.4. Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATADA.

4.17.3.5. Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA, em especial com buscas em registros de SIEM e dados de CTI.

4.17.3.6. Encaminhar eventos que não sejam de sua alçada ao N2 de acordo com os playbooks definidos pela CONTRATADA.

4.17.3.7. Acompanhar e encerrar os eventos após sua solução.

4.17.3.8. Sugerir ao Gerente do SOC/CREA-SP melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.

4.17.3.9. Suportar as tratativas requeridas nas respostas a incidente de Segurança Cibernética.

4.17.3.10. Propor melhorias nos controles relacionados ao ambiente.

4.17.3.11. Operar ferramenta de EDR, que deverá ser fornecida pela contratada, realizando configurações, melhorias, assim como tomando ações efetivas como isolamento e varredura de dispositivos.

4.17.3.12. Operar ferramenta de WAF, que deverá ser fornecida pela contratada, validando regras, bloqueando ameaças e adequando solução ao negócio.

4.17.3.13. Operar ferramenta de Proteção de APIs, que deverá ser fornecida pela contratada,



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

validando regras, bloqueando ameaças e adequando solução ao negócio.

4.17.3.14. Atuar no tratamento em vulnerabilidades identificadas, seja por meio de atualizações, patching, hardening ou soluções que mitiguem as detecções.

4.17.3.15. Suportar mudanças e adequações na Infraestrutura de Segurança.

4.17.3.16. Auxiliar na composição de documentação de procedimentos aderentes ao modelo de negócio.

4.17.3.17. Realizar acompanhamento de métricas e KPIs requeridos pela CONTRATANTE.

4.17.3.18. Participar de forma propositiva das reuniões sobre Segurança Cibernética.

4.17.4. Das atividades da equipe do SOC como sendo N2;

4.17.4.1. Realizar todas as atividades de N1 quando/se necessário.

4.17.4.2. Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATANTE.

4.17.4.3. Reclassificar eventos como falso positivo ou rever a prioridade, quando houver divergência de entendimento com relação ao definido pelo N1.

4.17.4.4. Analisar os eventos identificados, criando documento de Resposta a Incidente com as devidas ações de contenção, remediação e erradicação sugeridas as equipes resolvidoras.

4.17.4.5. Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA, em especial com buscas em registros de SIEM e dados de CTI.

4.17.4.6. Na ocorrência de eventos de alta criticidade, alertar o Gerente do SOC formalmente, assim como proceder com matriz de escalonamento prevista.

4.17.4.7. Redirecionar incidentes para equipe N1 após tratativas realizadas para acompanhamento e encerramento.

4.17.4.8. Realizar atividades de Threat Hunting, em busca ativa por atividades suspeitas no ambiente da CONTRATANTE.

4.17.4.9. Realizar atividades de tuning nas ferramentas oferecidas pela CONTRATADA para aprimorar a cobertura dos eventos em segurança cibernética.

4.17.4.10. Revisar atividades de parseamento, buscando que as ferramentas proporcionem



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

dados qualitativos em seus eventos.

4.17.4.11. Acompanhar e suportar integrações entre os ativos de segurança da CONTRATANTE junto a solução oferecida da CONTRATADA.

4.17.4.12. Sugerir ao Gerente do SOC/CREA-SP melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.

4.17.4.13. Realizar melhorias nos playbooks após alinhamento entre partes interessadas.

4.17.4.14. Gerar relatórios técnicos dos eventos e incidentes de segurança cibernética

4.17.5. Das atividades Gerenciais do Gerente do SOC

4.17.5.1. Coordenar tecnicamente os serviços e o andamento das atividades, projetos e demandas das equipes N1 e N2 do SOC;

4.17.5.2. Garantir a operação de todas as ferramentas e sistemas utilizados, os quais deverão ser fornecidos pela contratada, pelas equipes corretas para atender aos requisitos especificados neste termo.

4.17.5.3. Supervisionar os perfis profissionais do N1 e N2 delegar responsabilidades e serviços às equipes e acompanhar seu desempenho.

4.17.5.4. Gerir o cumprimento de metas e indicadores estabelecidos

4.17.5.5. Elaborar relatórios de acompanhamento dos indicadores de serviço, assim como propostas de melhorias da execução do serviço e de sua medição;

4.17.5.6. Garantir o bom desempenho da equipe;

4.17.5.7. Manter a equipe N1 e N2 devidamente treinada e apta a prestar os serviços ora contratados;

4.17.5.8. Fornecer informações solicitadas pela CONTRATANTE;

4.17.5.9. Assegurar que os processos operacionais tenham melhoria contínua e atendam aos Indicadores e metas acordadas em contrato;

4.17.5.10. Realizar auditorias dos atendimentos dos eventos e incidentes cibernéticos e tickets realizados pelos perfis profissionais de N1 e N2, com o objetivo de avaliar e aferir a observância aos padrões, procedimentos e qualidade do serviço prestado, bem como o cumprimento dos scripts, playbooks, padrões de cordialidade e empatia exigidos;



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

4.17.5.11. Apresentar Relatório de acompanhamento de indicadores de uso de recursos, atendimento, desempenho e utilização do serviço.

4.18. Serviços de Gerenciamento e Correlação de Eventos de Segurança–SIEM

4.18.1. A CONTRATADA deverá disponibilizar ferramenta de gerenciamento e correlação de eventos de segurança da informação (Security Information and Event Management) SIEM, incluindo toda infraestrutura computacional.

4.18.2. A CONTRATADA deverá fornecer a solução, que será utilizada como ferramenta durante a vigência do contrato para prestação de serviços de SOC.

4.18.3. A CONTRATADA deverá fornecer acesso a dashboards de forma unificadas das tecnologias que comporão o ecossistema de serviços e ou, acesso de leitura aos consoles e interfaces gráficas das ferramentas fornecidas.

4.18.4. A CONTRATADA deverá fornecer aos analistas do CREA-SP acesso de leitura aos logs de todas as ferramentas utilizadas para prestação do serviço de SIEM.

4.18.5. Capacidades técnicas:

4.18.5.1. Coletar Logs;

4.18.5.2. Parsear/Analisar;

4.18.5.3. Normalizar;

4.18.5.4. Categorizar;

4.18.5.5. Analisar;

4.18.5.6. Correlacionar;

4.18.5.7. Score de risco;

4.18.5.8. Alertar e notificar;

4.18.5.9. Permitir a autenticação dos usuários por meio de serviço de diretório como Microsoft Active Directory (AD) e/ou LDAP;

4.18.5.10. RBAC – Role Based Access Control;

4.18.5.11. SSO- Single Sign On;

4.18.5.12. Os logs deverão receber uma pré-filtragem de modo a otimizar o envio ao SIEM de logs



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

relevantes ao que tange segurança cibernética;

- 4.18.5.13.** Atuar com agentes responsáveis pela coleta de eventos (LOG), se necessário, quando não há forma nativa de conexão, de acordo com o ambiente corporativo e solução ofertada;
- 4.18.5.14.** Recurso agente-less, para dispositivos como Firewalls, switches, roteadores, redes IDS entre outros;
- 4.18.5.15.** a solução deve ser ofertada na última versão estável, disponível no momento da contratação, de todos os módulos e componentes desta especificação;
- 4.18.5.16.** Armazenar eventos e registros processados por um período mínimo de 12 meses após o término de vigência do contrato;
- 4.18.5.17.** Correlacionador de eventos;
- 4.18.5.18.** Console de administração, operação, monitoramento e pesquisa da solução;
- 4.18.5.19.** Detectar ataques como: Brute Force e SQL injection;
- 4.18.5.20.** Monitorar eventos de Docker Container;
- 4.18.5.21.** Monitorar eventos de IaaS, PaaS e SaaS (AWS, Google Cloud e MS Azure);
- 4.18.5.22.** Monitorar e coletar dados de soluções Microsoft como: Microsoft Office 365, Microsoft Windows Defender e Microsoft Graph;
- 4.18.5.23.** Detectar Vulnerabilidades;
- 4.18.5.24.** FIM- File integrity monitoring;
- 4.18.5.25.** Malware Detection;
- 4.18.5.26.** Assessment de configuração de segurança;
- 4.18.5.27.** Scripts de resposta;
- 4.18.5.28.** Todos os módulos e componentes que compõem a solução deverão se integrar de forma nativa;
- 4.18.5.29.** visando constituir um ambiente homogêneo de monitoração, análise, investigação, inteligência, defesa cibernética e resposta a incidentes.

4.18.6. REQUISITOS DE INFRAESTRUTURA



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

- 4.18.6.1.** A solução deve contemplar o fornecimento de todo o hardware e do software necessário para o pleno funcionamento, disponibilizando acesso aos logs de forma online e via navegação web.
- 4.18.6.2.** Para fins de dimensionamento, deverá ser considerada uma volumetria mínima de 320Gbytes/Dia e 29 Milhões de Eventos/Dia.
- 4.18.6.3.** A solução deve contemplar o fornecimento do hardware e do software necessários para o pleno funcionamento, disponibilizando acesso aos logs de forma online via interface web;
- 4.18.6.4.** Todos os elementos (appliances físicos ou virtuais e licenças de software) necessários à prestação deste serviço serão de propriedade da CONTRATADA, os quais deverão ser disponibilizados à CONTRATANTE durante a vigência do contrato.

4.18.7. REQUISITOS GERAIS

- 4.18.7.1.** A administração da solução deve usar uma conta individualizada para cada usuário administrador, independente da funcionalidade gerenciada;
- 4.18.7.2.** Toda a comunicação entre os componentes deverá ser feita através de protocolos seguros como HTTPS, SSL E TLS 1.2 ou superior;
- 4.18.7.3.** Suportar IPv4 e IPv6;
- 4.18.7.4.** Apto a tratar, no mínimo, os seguintes protocolos: IP, SYSLOG E SSH.
- 4.18.7.5.** Fornecer regras pré-programadas (out-of-the-box), bem como permitir que novas regras sejam criadas.
- 4.18.7.6.** Deve permitir a visualização dos dispositivos gerenciados por localização, host e tipo;
- 4.18.7.7.** Deve permitir adição, visualização, edição e exclusão da localização de dispositivos;
- 4.18.7.8.** Manter seu próprio log de auditoria;
- 4.18.7.9.** Deve permitir a correlação de eventos provenientes de logs, devidamente estruturados em metadados;
- 4.18.7.10.** Deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
- 4.18.7.11.** Deve ter configuração de fuso horário e conexão com servidor NTP equivalente aos dispositivos do CREA-SP;



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

- 4.18.7.12.** Deve sincronizar o horário de seus componentes utilizando o serviço NTP equivalente aos dispositivos do CREA-SP;
- 4.18.7.13.** Deve armazenar no mínimo os seguintes dados: eventos, alertas, e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração;
- 4.18.7.14.** Deve implementar o expurgo dos dados de forma automática com a personalização do período do expurgo;
- 4.18.7.15.** De forma a permitir seu uso em auditorias e processos forenses, não deve ser possível, sob nenhuma hipótese, a seleção, alteração e exclusão de eventos individuais. Deve ser possível apenas o expurgo de eventos conforme a política de retenção, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros;
- 4.18.7.16.** Todos os elementos necessários à prestação dos serviços deverão ser integráveis entre si, mantendo-se como uma única solução sem restrições aos requisitos constantes nestas especificações técnicas, e aos do parque computacional da CONTRATANTE.

4.18.8. MÉTRICAS DE INGESTA E RETENÇÃO

- 4.18.8.1.** Para fins de dimensionamento, deverá ser considerada uma volumetria mínima de 320Gbytes/Dia e 29 Milhões de Eventos/Dia.
- 4.18.8.2.** Suportar retenção pelo período mínimo de 12 meses após o término de vigência do contrato.
- 4.18.8.3.** Deve ter a capacidade de definir políticas diferentes de retenção dos dados.

4.18.9. MECANISMO DE PESQUISA

- 4.18.9.1.** Deve contemplar pesquisas e análises de texto;
- 4.18.9.2.** Ser escalável e atuar com alta disponibilidade;
- 4.18.9.3.** Near real-time;
- 4.18.9.4.** Opção de configuração como Nó único ou Cluster de nós.
- 4.18.9.5.** Funcionalidade de ajuda (helper) para facilitar a criação de queries;
- 4.18.9.6.** Deve implementar indexação baseada em campo e palavra-chave para acelerar buscas;



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

4.18.10. RELATÓRIOS

- 4.18.10.1.** Deve permitir o agendamento de geração de relatórios e o envio deles por e-mail;
- 4.18.10.2.** Deve possuir ferramenta ou interface gráfica para desenho de modelos de relatórios ou dashboards personalizados;
- 4.18.10.3.** Deve permitir gerar relatórios, no mínimo, nos seguintes formatos: PDF e CSV;
- 4.18.10.4.** Deve permitir que o usuário defina quais campos do evento serão exportados;
- 4.18.10.5.** Deve permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;
- 4.18.10.6.** Deve possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
- 4.18.10.7.** Deve permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;

4.18.11. DASHBOARD INTEGRADO

- 4.18.11.1.** Status do ambiente, dos logs de eventos, além de apresentar resultados de consultas tempestivas, quando se fizerem necessárias.
- 4.18.11.2.** Visão consolidada das métricas de segurança, para todos os ativos de rede monitorados.
- 4.18.11.3.** Personalizável.
- 4.18.11.4.** Análise dos eventos de segurança da informação em near real-time.
- 4.18.11.5.** Análises Drill-Down, permitindo obter detalhes de um gráfico geral, descendo aos níveis de análise conforme necessidade;
- 4.18.11.6.** Conformidade: PCI DSS, GDPR, CIS, HIPAA E NIST 800-53.
- 4.18.11.7.** Dashboard com foco em detecção de vulnerabilidades, exibindo inclusive CVE atribuída.
- 4.18.11.8.** Dashboard com foco em FIM- File Integrity Monitoring.
- 4.18.11.9.** Dashboard com foco em ambientes Cloud.

4.18.12. THREAT HUNTING



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

- 4.18.12.1.** Efetuar a análise dos eventos de segurança da informação em tempo real;
- 4.18.12.2.** Possibilitar a análise por drill-down, permitindo detalhá-la a partir de um gráfico geral, descendo aos níveis da análise conforme necessidade;
- 4.18.12.3.** Deve apresentar relatórios de eventos, alertas e incidentes em nível técnico (analítico, drill down) e gerencial (sintético / dashboards);
- 4.18.12.4.** Deve permitir filtrar e selecionar os eventos que serão tratados pelo SOC no caso de incidentes evidenciados;
- 4.18.12.5.** Deve implementar o gerenciamento de conectores: adição, edição de conectores, atualização de parâmetros, gerenciar os destinos e failover de logs de múltiplos conectores, envio de comandos, visualização interativa de diagnóstico, edição de conectores customizados e compartilhamento de conectores;
- 4.18.12.6.** O correlacionador deve fornecer mecanismo de priorização de eventos, alertas e incidentes com base, pelo menos, nos seguintes critérios:
- severidade do evento;
 - criticidade do ativo;
- 4.18.12.7.** O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução;
- 4.18.12.8.** A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes;
- 4.18.12.9.** Deve fornecer a funcionalidade de geração de alertas via dashboard e e-mail para incidentes de alta criticidade detectados no correlacionamento de eventos;
- 4.18.12.10.** Deve ser capaz de contextualização, utilizando dados de diferentes origens (rede, servidor, aplicações) em uma única console, otimizando e auxiliando o processo de análise de resposta a incidentes;
- 4.18.12.11.** Ter a funcionalidade de visualização de eventos e alertas de segurança em near real-time;
- 4.18.12.12.** Deve permitir o registro de ações tomadas e planejadas acerca dos eventos;
- 4.18.12.13.** Deve possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;
- 4.18.12.14.** Threat Hunting por Mitre AttCck, seguindo as seguintes categorias:



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

- Initial Access;
- Execution;
- Persistence;
- Privilege Escalation;
- Defense Evasion;
- Lateral Movement;
- Collection;
- Command and control;
- Exfiltration;

4.18.13. INTEGRAÇÕES

4.18.13.1. Microsoft Windows Event Logging API;

4.18.13.2. Microsoft Security Graph API;

4.18.13.3. RestAPI;

4.18.13.4. Third-party API'S;

4.18.13.5. VirusTotal;

4.18.13.6. Microsoft Office 365;

4.18.13.7. Microsoft Azure Entra ID/ Microsoft Active Directory;

4.18.13.8. LDAP- Lightweight Directory Access Protocol;

4.18.13.9. YARA;

4.18.13.10. NIDS- Network-Based Intrusion detecting system;

4.19. Serviços de Computer Security Incident Response Team – CSIRT

4.19.1. A CONTRATADA deve disponibilizar equipe multidisciplinar responsável por responder incidentes. A equipe de CSIRT, deve atuar com uma equipe técnica, também corroborando com atividades que extrapolam o âmbito tecnológico, quando os eventos de um incidente carecem de interações com outras equipes como departamento jurídico, relações públicas, recursos humanos e compliance. Este serviço deverá englobar análise forense digital de forma a dar subsídios à CONTRATANTE em incidentes que envolvam exfiltração de dados sensíveis, comunicações com ANPD e incidentes que afetem confiança e reputação da marca do CREA-SP.

4.19.2. A contratante poderá requisitar o atendimento presencial da figura do gerente de



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

segurança a qualquer momento na sede da contratante.

4.19.3. Os serviços de análise forense digital devem englobar:

- 4.19.3.1.** Realização de análise forense digital para determinar a origem, causa e extensão dos incidentes, visando identificar possíveis violações e atividades maliciosas em segundo plano.
- 4.19.3.2.** Produção de relatórios abrangentes sobre os incidentes de segurança ocorridos, que incluem informações sobre as ações adotadas, aprendizados obtidos e recomendações para aprimoramentos futuros no ambiente empresarial.
- 4.19.3.3.** Utilização de ferramentas e tecnologias atualizadas para o monitoramento, detecção e resposta a ameaças cibernéticas.
- 4.19.3.4.** Condução de investigações minuciosas em casos de incidentes de segurança, garantindo uma abordagem detalhada.
- 4.19.3.5.** Realização da coleta e preservação de evidências digitais para embasar as investigações.
- 4.19.3.6.** Elaboração de análises dos sistemas afetados para identificar a natureza e a extensão do incidente.
- 4.19.3.7.** Identificação das causas raiz do incidente e suas implicações dentro do ambiente tecnológico.
- 4.19.3.8.** Formulação de recomendações de ações corretivas e preventivas para mitigar futuros incidentes.
- 4.19.3.9.** Identificação, análise e classificação de malwares presentes no ambiente.
- 4.19.3.10.** Determinação das funcionalidades e impactos dos malwares identificados.
- 4.19.3.11.** Extração de indicadores de comprometimento (IOCs) para auxiliar na detecção e prevenção de ameaças.
- 4.19.3.12.** Análise de metadados para compreender atividades suspeitas no ambiente digital.
- 4.19.3.13.** Monitoramento e análise do tráfego de rede em busca de atividades maliciosas.
- 4.19.3.14.** Documentação detalhada de todos os processos de análise forense realizados durante as investigações.
- 4.19.3.15.** Elaboração de relatórios claros e precisos, contendo evidências, metodologias



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

utilizadas e conclusões obtidas ao final das investigações.

4.20. Serviços de Gestão de Vulnerabilidades

- 4.20.1.** O Serviço de Gestão de Vulnerabilidades tem por objetivo identificar possíveis vulnerabilidades de segurança da informação no parque computacional e serviços de TIC do CONTRATANTE, a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
- 4.20.2.** A CONTRATADA deverá realizar varreduras com periodicidade mínima mensal de todas as aplicações, ativos e recursos apresentados como escopo do CONTRATANTE.
- 4.20.3.** É responsabilidade da CONTRATANTE informar a lista de ativos e serviços críticos de seu ambiente.
- 4.20.4.** O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. O início do processo não se limita apenas em rotinas de tempo definidas, mas poderá o CONTRATANTE também solicitar análises sob demanda a qualquer tempo.
- 4.20.5.** A CONTRATADA será responsável pelo tratamento contínuo das vulnerabilidades encontradas na infraestrutura de servidores (Sistema Operacional) da CONTRATANTE, executando atividades listadas, mas não se limitando a elas:
- 4.20.6.** A CONTRATANTE manterá informado a CONTRATADA sobre o plano de comunicação com outros prestadores de serviços, para que possam ser acionados para correção de vulnerabilidades que excedem Servidores como (infraestrutura, aplicações, banco de dados).
- 4.20.7.** Registrar Vulnerabilidade: nesta fase uma vulnerabilidade é identificada dentre os ativos de informação da CONTRATANTE. A CONTRATADA deve utilizar as ferramentas específicas de varredura nos ativos de hardware e software da CONTRATANTE. Quando a vulnerabilidade é encontrada, a mesma deve ser registrada na ferramenta designada.
- 4.20.8.** Classificar Vulnerabilidade: nesta fase a vulnerabilidade é classificada de acordo com sua criticidade. A CONTRATADA deve realizar a classificação da vulnerabilidade em conjunto com as equipes internas designadas pela CONTRATANTE.
- 4.20.9.** Notificar Vulnerabilidade e Próximo Nível Hierárquico: esta fase consiste na notificação do dono do ativo, sobre a existência da vulnerabilidade, juntamente com sua criticidade. A notificação ao dono do ativo é realizada pela equipe de local, sendo que a CONTRATADA deve prestar todo o esclarecimento acerca dos problemas existentes e potenciais decorrentes de possível exploração da vulnerabilidade.
- 4.20.10.** Proposta de solução: nesta fase a CONTRATADA deverá propor as soluções definitivas para o tratamento da vulnerabilidade, bem como, soluções de contorno e/ou mitigação de



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

curto prazo.

- 4.20.11.** Analisar Tratamento: a CONTRATADA poderá ser requisitada para analisar se a vulnerabilidade corrigida diretamente pelo dono do ativo atendeu as necessidades de segurança da informação, assim como apoiar no processo de tratamento. A CONTRATADA quando o ativo não estiver sob sua gestão, deverá repassar ao CONTRATANTE os procedimentos necessários que possibilitem a verificação da eliminação da vulnerabilidade e seu monitoramento.
- 4.20.12.** Avaliar Risco: esta fase é realizada pelo setor de gestão de segurança da informação da CONTRATANTE que atualiza os riscos de acordo com o tratamento realizado na vulnerabilidade. A CONTRATADA pode propor controles que podem ser utilizados nos modelos de avaliação de riscos, no caso de vulnerabilidades que serão mitigadas.
- 4.20.13.** A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional do CONTRATANTE, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado à CONTRATANTE.
- 4.20.14.** Após a apresentação do relatório com as vulnerabilidades, caberá ao CONTRATANTE autorizar a aplicação das correções e definir a janela de aplicação das correções;
- 4.20.15.** A CONTRATADA será responsável por acionar e assessorar as áreas internas da CONTRATANTE a respeito da melhor estratégia para mitigação das vulnerabilidades encontradas. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores.
- 4.20.16.** Todas as correções das vulnerabilidades deverão passar por um processo de aprovação pela CONTRATANTE e realizadas em janelas de atividade disponibilizada pela CONTRATANTE.
- 4.20.17.** Todo acesso ao ambiente da CONTRATANTE deve ser realizado LOCALMENTE, ou via VPN através de usuários autenticados e autorizados pela CONTRATANTE.
- 4.21. Ferramenta da Solução de Gestão de Vulnerabilidades – GV**
 - 4.21.1.** A CONTRATADA deverá fornecer a solução, que será utilizada como ferramenta durante a vigência do contrato para prestação de Gestão de Vulnerabilidade.
 - 4.21.2.** A solução deve ser licenciada como serviço para a CONTRATANTE, sendo de total responsabilidade da CONTRATADA a gestão e o dimensionamento das licenças necessárias.
 - 4.21.3.** A Solução não deve impor nenhum limite na quantidade de scanners implementados dentro da infraestrutura.



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

4.21.4. A CONTRATADA deve utilizar ferramenta(s) de gestão de vulnerabilidades que atendam aos seguintes requisitos:

- 4.21.4.1.** compatível com o padrão SCAP -v1.2 ou -v1.3 (Security Content Automation Protocol), este é um protocolo essencial e de garantia de qualidade em varreduras automatizadas em ativos de informação;
- 4.21.4.2.** capaz de escanear e gerenciar, no mínimo, 3.500 (três mil e quinhentos) ativos, podendo ser estações de trabalho, notebooks, switches, roteadores, access points, servidores de rede, servidores;
- 4.21.4.3.** de aplicações, servidores de banco de dados e aplicações web;
- 4.21.4.4.** correlacionar eventos baseados no sistema operacional, porta/protocolo, banners e vulnerabilidades;
- 4.21.4.5.** detecção de vulnerabilidades em sistemas operacionais, protocolos e dispositivos de rede, aplicações WEB, banco de dados, servidores físicos e virtuais, entre outros;
- 4.21.4.6.** verificar vulnerabilidades em ambiente Windows e Linux para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus;
- 4.21.4.7.** efetuar varredura à procura de vulnerabilidades e exploits;
- 4.21.4.8.** detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
- 4.21.4.9.** detecção de vulnerabilidades em ambientes Oracle, SQL Server e Microsoft Exchange;
- 4.21.4.10.** deverá ser utilizada ferramenta de análise de vulnerabilidade com foco em infraestrutura, em aplicações web;
- 4.21.4.11.** a descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional;
- 4.21.4.12.** agrupamento de eventos baseada em sistemas operacionais, endereços IP, nome DNS, nome NetBIOS, porta de serviços e vulnerabilidades;
- 4.21.4.13.** ter capacidade de varredura de ativos de modo intrusivo e não intrusivo;
- 4.21.4.14.** ter capacidade de selecionar e agrupar ativos encontrados, com possibilidade de



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

incluir faixa de exclusão de endereços IP para varredura;

- 4.21.4.15.** ter capacidade de definir templates de configuração de scans e de agendamento de scans;
- 4.21.4.16.** ter capacidade de configuração de usuário e senha para realização de varredura autenticada de sistemas operacionais e aplicações;
- 4.21.4.17.** ter a capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;
- 4.21.4.18.** ter a capacidade de geração de tickets para vulnerabilidades encontradas, permitindo marcar uma vulnerabilidade em determinado ativo como corrigida ou ignorada;
- 4.21.4.19.** possuir integração com a base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
- 4.21.4.20.** ter capacidade de definição de, no mínimo, 3 (três) níveis de criticidade de vulnerabilidades;
- 4.21.4.21.** possuir recurso de base de conhecimento com, no mínimo, 40.000 (quarenta mil) assinaturas de vulnerabilidades, com atualização automática a partir do site do fabricante;
- 4.21.4.22.** recurso para acompanhamento da evolução das remediações de vulnerabilidades encontradas;
- 4.21.4.23.** possibilitar a apresentação de graduação de riscos, baseada em pontuação, que permite medir o nível de riscos dos recursos e sistemas encontrados;
- 4.21.4.24.** apresentar os procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualizações de software;
- 4.21.4.25.** possibilitar a configuração de frequência e periodicidade de varreduras na rede;
- 4.21.4.26.** possuir a apresentação de relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CONTRATANTE em relação aos riscos de segurança em TI, contendo: hosts encontrados, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;
- 4.21.4.27.** possuir a capacidade de exportação de relatório de vulnerabilidades em formato PDF e CSV;



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

- 4.21.4.28.** possuir gerenciamento por WebUI (WEB User Interface) via HTTPS (Secure Hypertext Transfer Protocol) e console gráfica centralizada;
- 4.21.4.29.** possuir gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;
- 4.21.4.30.** possuir gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios;
- 4.21.4.31.** possuir gerenciamento com visualização de status dos serviços;
- 4.21.4.32.** possuir gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;
- 4.21.4.33.** possuir gerenciamento com recurso de validação de políticas de segurança antes da aplicação, responsável pela identificação de erros e inconsistências;
- 4.21.4.34.** possuir gerenciamento com recurso de replicação de configurações e atualização de software;
- 4.21.4.35.** possuir gerenciamento com recurso de monitoramento de logs, debugging e captura de pacotes;
- 4.21.4.36.** possuir gerenciamento com recurso de backup e importação automáticos de arquivos de configuração;
- 4.21.4.37.** deverá a capacidade de apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
- 4.21.4.38.** a solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução;
- 4.21.4.39.** a solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;
- 4.21.4.40.** a solução deve permitir a segregação lógica entre aplicações distintas a fim de obter a pontuação referente exposição cibernética por aplicação;
- 4.21.5.** A CONTRATADA Deverá Fornecer acesso de leitura aos analistas da CONTRATANTE ao console da ferramenta de Gestão de vulnerabilidades, a qual deverá ser fornecida pela contratada.



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

4.22. Serviços de Gestão de Ferramenta EDR (EndPoint Detection and Response)

- 4.22.1.** O Serviço de Endpoint Detection Response EDR deve ser fornecido para até 300 servidores.
- 4.22.2.** É de responsabilidade da CONTRATADA a realização da instalação, instalação dos agentes nos servidores, configuração e gestão da solução.
- 4.22.3.** É de responsabilidade da CONTRATANTE o fornecimento de acesso e permissões para que a CONTRATADA possa realizar as atividades.
- 4.22.4.** O CREA-SP possui antivírus da Kaspersky e SYMANTEC (EndPoint 14) nos seus servidores, todos instalados no Datacenter. Caso seja fornecida solução de EDR de outros fabricantes, a CONTRATADA deverá garantir que a solução fornecida seja interoperável com os Antivírus do CREA SP, de forma a não causar impactos de lentidão ou bloqueios de serviços indevidos por haver dois agentes instalados nos servidores.
- 4.22.5. REQUISITOS DO AGENTE:**
- 4.22.5.1.** A solução proposta deverá, obrigatoriamente, possuir capacidades de EDR-Endpoint Detection and Response.
- 4.22.5.2.** A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows (versões 32 e 64 bits) XP SP2 / SP3, 7, 8, 8.1 e 10;
- 4.22.5.3.** A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 e 2019;
- 4.22.5.4.** A solução proposta deve ser compatível com os seguintes sistemas operacionais: versões macOS: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) e Catalina (10.15);
- 4.22.5.5.** A solução proposta deve ser compatível com os seguintes sistemas operacionais: Versões do Linux: RedHat Enterprise Linux e CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 e 7.7 e Ubuntu LTS 16.04.5, 16.04.6, servidor 18.04.1 e 18.04.2, 64 bits";
- 4.22.5.6.** A solução proposta deve ter um consumo máximo de 120 MB de memória RAM;
- 4.22.5.7.** A solução proposta deve ter um consumo médio de menos de 2% do uso da CPU.
- 4.22.5.8.** A solução proposta deve consumir menos de 20 MB de espaço em disco;
- 4.22.5.9.** A solução proposta deve oferecer suporte à implantação em massa por meio de ferramentas como MS System Center, JAMF e Satellite.



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

- 4.22.5.10.** A solução proposta deve ter a capacidade de atualizar o terminal sem interação do usuário e sem exigir uma reinicialização.
- 4.22.5.11.** A solução proposta deve ter proteção "Anti-adulteração" no Agente;
- 4.22.5.12.** A solução proposta deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos.
- 4.22.5.13.** A solução proposta deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o conhecimento do usuário associado aos eventos;
- 4.22.5.14.** A solução proposta deve ter a opção de definir a senha para desinstalar o agente no terminal. Evitando que um usuário sem o devido privilégio remova o agente.
- 4.22.5.15.** A solução proposta deve ser capaz de gerar um instalador Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração do usuário.
- 4.22.5.16.** O coletor que será instalado nos terminais da solução proposta deve ser capaz de trabalhar por trás de um proxy.

4.22.6. REQUISITO – DETECÇÃO DE MALWARE

- 4.22.6.1.** A solução proposta deve ser capaz de funcionar no modo "offline" sem que o Agente esteja conectado à rede corporativa.
- 4.22.6.2.** A solução proposta deve ser capaz de detectar processos em execução, inícios de processos, paradas de processos e interações entre processos.
- 4.22.6.3.** A solução proposta deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do PC.
- 4.22.6.4.** A solução proposta deve ser capaz de detectar as solicitações de DNS enviadas do dispositivo.
- 4.22.6.5.** A solução proposta deve ser capaz de detectar conexões de rede a partir do dispositivo.
- 4.22.6.6.** A solução proposta deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL.
- 4.22.6.7.** A solução proposta deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção.



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

4.22.6.8. A solução proposta deve ser capaz de incorporar as técnicas MITRE ATTCK no esquema de detecção e mostrar quais técnicas foram utilizadas.

4.22.6.9. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como: nome do arquivo e hash do arquivo.

4.22.6.10. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a arquivos (Criação, Exclusão, Renomear).

4.22.6.11. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis);

4.22.6.12. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Bind);

4.22.6.13. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas aos logs do Windows (Log de eventos).

4.22.6.14. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Windows (criação de chave, exclusão de chave, conjunto de valores).

4.22.6.15. A solução proposta deve ter a capacidade de realizar consultas de texto livre para filtrar as informações disponíveis para a caça de ameaças.

4.22.6.16. A solução proposta deve ter a capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro.

4.22.6.17. A solução proposta deve ter a capacidade de agendar pesquisas armazenadas.

4.22.6.18. A solução proposta deve identificar atividades maliciosas conhecidas.

4.22.6.19. A solução proposta deve ter a capacidade de receber atualizações diárias de inteligência.

4.22.6.20. A solução proposta deve ter a capacidade de categorizar os eventos detectados em diferentes categorias (Ex: Malicioso, Suspeito, Inconclusivo, Provavelmente Seguro).

4.22.6.21. A solução proposta deve ter a capacidade de coexistir com outras soluções de segurança de endpoint do tipo de antivírus tradicional ou de nova geração.



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

4.22.7. REQUISITO – PREVENÇÃO DE MALWARE

- 4.22.7.1.** A solução proposta deve ter a capacidade de prevenir a execução de arquivos maliciosos.
- 4.22.7.2.** A solução proposta deve incorporar um mecanismo antivírus de última geração (NGAV) baseado no kernel com capacidade de "Aprendizado de Máquina".
- 4.22.7.3.** A solução proposta deve ter a capacidade de controlar dispositivos USB.
- 4.22.7.4.** A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo.
- 4.22.7.5.** A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo.
- 4.22.7.6.** A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo.
- 4.22.7.7.** A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série.
- 4.22.7.8.** A solução proposta deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados.
- 4.22.7.9.** A solução proposta deve ser capaz de bloquear o tráfego de comunicação malicioso para-CCC (Comando e Controle).
- 4.22.7.10.** A solução proposta deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real.
- 4.22.7.11.** A solução proposta deve ser capaz de evitar a criptografia de disco causada por ransomware e modificação de arquivos ou registro de dispositivos.
- 4.22.7.12.** A solução proposta deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: Ativo, desativado ou apenas criar "logs" para as regras de segurança contidas nestes.
- 4.22.7.13.** A solução proposta deve ser capaz de ser configurada em modo de simulação onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas.
- 4.22.7.14.** A solução proposta deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio.



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

4.22.7.15. A solução proposta deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o Agente instalado.

4.22.8. REQUISITO – DIFUSÃO (PÓS-INFECÇÃO)

4.22.8.1. A solução proposta deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada uma atividade causada por malware.

4.22.8.2. A solução proposta deve permitir alterar as políticas atribuídas de um dispositivo onde uma atividade causada por malware foi encontrada.

4.22.8.3. A solução proposta deve permitir o bloqueio de atividades realizadas por arquivos maliciosos.

4.22.8.4. A solução proposta deve ter a capacidade de criar exceções para processos com base na localização do arquivo (Caminho do Arquivo).

4.22.8.5. A solução proposta deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado pelo processo.

4.22.8.6. A solução proposta deve ter a capacidade de criar exceções para os processos baseados no usuário que o processo executou.

4.22.8.7. A solução proposta deve ter a capacidade de criar exceções manualmente para falsos positivos para marcar a atividade como um falso positivo e evitar a ocorrência de falhas futuras.

4.22.8.8. A solução proposta deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes.

4.22.8.9. A solução proposta deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos.

4.22.9. REQUISITO – RESPOSTA AO INCIDENTE

4.22.9.1. A solução proposta deve permitir um histórico dos eventos por no mínimo 12 meses.

4.22.9.2. A solução proposta deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses.

4.22.9.3. A solução proposta deve permitir a integração com plataformas SIEMs (Security Information and Event Management) através de syslog.



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

- 4.22.9.4.** A solução proposta deve ter a capacidade de obter instantâneos de memória ou "dumps" de memória que permitam a realização de processos forenses.
- 4.22.9.5.** A solução proposta deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA.
- 4.22.9.6.** A solução proposta deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data / hora ocorrida e atividade suspeita) para permitir a integração via API.
- 4.22.9.7.** A solução proposta deve ter a capacidade de encerrar um processo com base em sua classificação.
- 4.22.9.8.** A solução proposta deve ter a capacidade de excluir um arquivo com base em sua classificação.
- 4.22.9.9.** A solução proposta deve ter a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida.
- 4.22.9.10.** A solução proposta deve ter a capacidade de isolar os dispositivos infectados da rede.
- 4.22.9.11.** A solução proposta deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (Malicioso e Suspeito) do processo detectado.
- 4.22.9.12.** A solução proposta deve obter visibilidade total da cadeia de ataques e alterações maliciosas.
- 4.22.9.13.** A solução proposta deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo.
- 4.22.9.14.** A solução proposta deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos.
- 4.22.9.15.** A solução proposta deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso, o bloqueio de uma conexão de rede.
- 4.22.10. REQUISITO – CONTROLE DE VULNERABILIDADES E COMUNICAÇÃO**
- 4.22.10.1.** A solução proposta deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o terminal.
- 4.22.10.2.** A solução proposta deve ter capacidade para realizar um patch virtual, através da restrição de acessos de comunicação nas aplicações vulneráveis.



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

- 4.22.10.3.** A solução proposta deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter.
- 4.22.10.4.** A solução proposta deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede.
- 4.22.10.5.** A solução proposta deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado.
- 4.22.10.6.** A solução proposta deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede.
- 4.22.10.7.** A solução proposta deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo.
- 4.22.10.8.** A solução proposta deve ser capaz de visualizar e entregar informações sobre o uso dos aplicativos de rede mostrando informações como os destinos IP do tráfego gerado pelo aplicativo.

4.22.11. REQUISITO – CENÁRIO DE ATAQUE

- 4.22.11.1.** A solução proposta deve identificar e prevenir tentativas de perseguição de privilégios.
- 4.22.11.2.** A solução proposta deve bloquear ataques de ransomware conhecidos.
- 4.22.11.3.** A solução proposta deve detectar malware desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do malware e não de uma assinatura.
- 4.22.11.4.** A solução proposta deve proteger contra scripts Powershell maliciosos.
- 4.22.11.5.** A solução proposta deve proteger contra scripts CScript maliciosos.
- 4.22.11.6.** A solução proposta deve proteger contra macros maliciosas do Office.
- 4.22.11.7.** A solução proposta deve ter controle sobre dispositivos USB.

4.22.12. REQUISITO – IOT

- 4.22.12.1.** A solução proposta deve ter a capacidade de descobrir dispositivos IOT não gerenciados na rede.
- 4.22.12.2.** A solução proposta deve ter a capacidade de detectar dispositivos não gerenciados e protegidos pela solução com sistemas operacionais macOS / Linux / Windows.



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

4.22.13. REQUISITO – CONSOLE DE ADMINISTRAÇÃO

- 4.22.13.1.** A solução proposta deve estar em conformidade com os padrões de segurança de dados da indústria de cartões de pagamento (PCI DSS).
- 4.22.13.2.** A solução proposta deve estar em conformidade com o padrão HIPAA.
- 4.22.13.3.** A solução proposta deve estar em conformidade com o padrão GDPR.
- 4.22.13.4.** O console de gerenciamento da solução proposta deve permitir a integração com o "Active Directory" para garantir o cumprimento dos requisitos da política de senhas da empresa.
- 4.22.13.5.** O console de administração da solução proposta deve permitir o uso de autenticação de dois fatores (2FA) para acessá-la.
- 4.22.13.6.** O console de administração da solução proposta deve permitir a integração com SAML para autenticação do usuário no console de gerenciamento.
- 4.22.13.7.** O console de administração da solução proposta deve permitir o uso de funções granulares para administradores.
- 4.22.13.8.** O console de administração da solução proposta deve permitir o gerenciamento de ambientes multilocatários.
- 4.22.13.9.** O console de administração da solução proposta deve permitir o gerenciamento por meio da API Full Restful.
- 4.22.13.10.** A solução proposta deve ser capaz de ser totalmente gerenciada na nuvem sem a necessidade de serviços locais.
- 4.22.13.11.** A solução proposta deve ser capaz de ser gerenciada em uma arquitetura híbrida usando serviços locais complementados com outros na nuvem.
- 4.22.13.12.** O console de administração da solução proposta deve permitir a visualização dos eventos registrados nos dispositivos que requerem atenção.
- 4.22.13.13.** O console de administração da solução proposta deve permitir a visualização da saúde dos Agentes instalados.
- 4.22.13.14.** O console de administração da solução proposta deve permitir a desinstalação remota do Agente instalado nos dispositivos.
- 4.22.13.15.** O console de administração da solução proposta deve permitir a desativação /



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

ativação remota do Agente instalado nos dispositivos.

- 4.22.13.16.** O console de administração da solução proposta deve permitir a atualização remota do Agente instalado nos dispositivos.
- 4.22.13.17.** O console de administração da solução proposta deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema.
- 4.22.13.18.** O console de administração da solução proposta deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais.
- 4.22.13.19.** O console de administração da solução proposta deve permitir a exportação dos logs locais gerados pelos Agentes a partir do mesmo console.
- 4.22.13.20.** O console de administração da solução proposta deve permitir a criação de relatórios de inventário dos Agentes implantados contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, Status do Agente, último dia visto pelo console.
- 4.22.13.21.** O console de gerenciamento da solução proposta deve ter a visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado.
- 4.22.13.22.** O console de administração da solução proposta deve permitir a integração de um SMTP externo para envio de alertas por e-mail.
- 4.22.13.23.** O console de administração da solução proposta deve permitir auditorias de alterações feitas por administradores / operadores. Essas auditorias também devem ser baixadas em formato CSV.
- 4.22.13.24.** A solução proposta deve exigir que uma senha seja desabilitada por um aplicativo de terceiros.
- 4.22.13.25.** A solução proposta deve permitir o isolamento de um dispositivo através da integração de um NAC de acordo com a categoria do evento detectado.
- 4.22.13.26.** A solução proposta deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados.
- 4.22.13.27.** A solução proposta deve permitir a configuração de perfis nas informações coletadas para a função de caça a ameaças.
- 4.22.13.28.** A solução proposta deve permitir exclusões de informações que não serão



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

coletadas na função de caça a ameaças.

4.22.13.29. A solução proposta deve ser certificada pela Microsoft como uma solução antivírus e ser capaz de se integrar com o Windows Security Center.

4.22.13.30. A solução proposta deve entregar informações geradas pelos serviços de inteligência para a tomada de decisão na nuvem sobre o evento detectado.

4.22.13.31. A solução proposta deve permitir que os serviços em nuvem recategorizem uma classificação de evento.

4.22.13.32. A solução proposta deve permitir que os administradores desabilitem as notificações para um evento de descoberta.

4.22.13.33. A solução proposta deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso a páginas da web categorizadas como maliciosas.

4.22.13.34. A CONTRATADA Deve fornecer acesso de leitura ao console da ferramenta, que deverá ser fornecida pela contratada, aos analistas do CREA-SP.

4.23. Serviços de Gestão de Ferramenta WAF

4.23.1. As Ferramentas a serem disponibilizadas pela CONTRATADA deverão ser compatíveis com o ambiente tecnológico da CONTRATANTE;

4.23.2. O serviço deve atender no mínimo 90 URLs.

4.23.3. Capacidade para uma volumetria de no mínimo 19TBytes e 718 Milhões de Hits por mês.

4.23.4. Considerar para fins de dimensionamento, pico diário com volume de 1,5Tbytes.

4.23.5. REQUISITOS DO SERVIÇO

4.23.5.1. O Serviço deve ser entregue em appliance ou no formato de Serviço virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, no caso de Serviço virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATANTE.

4.23.5.2. Poderá ser entregue em equipamento único ou com composição de equipamentos do mesmo fabricante, para atender as funcionalidades exigidas.

4.23.5.3. Deve possuir e estar licenciado durante a vigência contratual minimamente com as seguintes funcionalidades: Antivírus, Reputação de IP, Serviço de defesa de preenchimento de credenciais e análise avançada de ameaças.



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

4.23.6. REQUISITOS MÍNIMOS DE PERFORMANCE

4.23.7. Deve possuir throughput mínimo para HTTP de 400(quatrocentos) Mbps;

4.23.8. Deve possuir suportar no mínimo para 04(quatro) vCPU;

4.23.9. Deve suportar quantidade ilimitada de aplicações protegidas;

4.23.10. FUNCIONALIDADES DE GERÊNCIA

4.23.10.1. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.

4.23.10.2. Deve possuir administração baseada em interface web HTTPS.

4.23.10.3. Possuir auto-complementação de comandos na CLI.

4.23.10.4. Possuir ajuda contextual na CLI.

4.23.10.5. O Serviço deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware).

4.23.10.6. Deve ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas.

4.23.10.7. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões.

4.23.10.8. Deve ser possível visualizar na interface de gerência as informações de consumo de memória.

4.23.10.9. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log.

4.23.10.10. Deve possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados.

4.23.10.11. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema.



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

- 4.23.10.12.** Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema.
- 4.23.10.13.** Deve possuir um painel de visualização com informações das interfaces de rede do sistema.
- 4.23.10.14.** A configuração de administração da Serviço deve possibilitar a utilização de perfis.
- 4.23.10.15.** Deve ser possível executar e restaurar backup via interface Web (GUI).
- 4.23.10.16.** Deve ter a opção para criptografar o backup.
- 4.23.10.17.** Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP, ou HTTPS.
- 4.23.10.18.** Deve ser possível instalar um firmware alternativo em disco e inicializá-lo manualmente em caso de falha do firmware principal.
- 4.23.10.19.** Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3.
- 4.23.10.20.** Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.
- 4.23.10.21.** O Serviço Deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.
- 4.23.10.22.** Ter a capacidade de armazenar logs em appliance remoto.
- 4.23.10.23.** A Serviço deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.
- 4.23.10.24.** O Serviço deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.
- 4.23.10.25.** O Serviço deve possuir dados analíticos contendo localização geográfica dos clientes web.
- 4.23.10.26.** O Serviço deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem.
- 4.23.10.27.** Deve ter a capacidade de gerar relatórios detalhados baseados em



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

tráfego/acessos/atividades do usuário.

4.23.10.28. Deve ter suporte a RESTful API para gerenciamento de configurações.

4.23.10.29. Deve suportar todas as funcionalidades para comunicação HTTP/2.

4.23.10.30. A CONTRATADA DEVERA fornecer acesso somente leitura aos analistas da CONTRATANTE, ao conselho de gerência da ferramenta, que deverá ser fornecida pela contratada, disponibilizada ao CREA-SP.

4.23.11. FUNCIONALIDADES DE AUTENTICAÇÃO

4.23.11.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS.

4.23.11.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos.

4.23.11.3. A Serviço Deve ser capaz de autenticar usuários através de certificados digitais pessoais.

4.23.11.4. Deve possuir base local para armazenamento e autenticação contas de usuários.

4.23.11.5. A Serviço deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS.

4.23.11.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM.

4.23.11.7. A Serviço deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.

4.23.12. FUNCIONALIDADES DE WEB APPLICATION FIREWALL

4.23.12.1. Deve ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática.

4.23.12.2. Deve implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque.

4.23.12.3. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application Security Project).



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

- 4.23.12.4.** Deve implementar recursos embarcados de antivírus para análise de arquivos, detecção e bloqueio de malwares que possam comprometer os servidores possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação.
- 4.23.12.5.** Ter a capacidade de criação de assinaturas de ataque customizáveis.
- 4.23.12.6.** Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
- 4.23.12.7.** Ter a capacidade de proteção para ataques do tipo Botnet.
- 4.23.12.8.** Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
- 4.23.12.9.** O Serviço Deve possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.
- 4.23.12.10.** Deve suportar detecção a ataques de Clickjacking.
- 4.23.12.11.** Deve suportar detecção a ataques de alteração de cookie.
- 4.23.12.12.** Deve identificar e prevenir ataques do tipo Credit Card Theft.
- 4.23.12.13.** Deve identificar e prevenir ataques Cross Site Request Forgery (CSRF).
- 4.23.12.14.** O Serviço deve possuir funcionalidade de proteção positiva contra-ataques como cross site scripting (XSS).
- 4.23.12.15.** Deve possuir proteção contra-ataques de Denial of Service (DoS).
- 4.23.12.16.** Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow.
- 4.23.12.17.** Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
- 4.23.12.18.** Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
- 4.23.12.19.** Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
- 4.23.12.20.** Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage.



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

- 4.23.12.21.** Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
- 4.23.12.22.** Deve possuir a capacidade de proteção para ataques do tipo Malformed XML.
- 4.23.12.23.** Deve Identificar e prevenir ataques do tipo Low-rate DoS.
- 4.23.12.24.** Deve possuir prevenção contra Slow POST attack.
- 4.23.12.25.** Deve proteger contra-ataques Slowloris.
- 4.23.12.26.** Deve possuir a capacidade de proteção para ataques do tipo SYN flood.
- 4.23.12.27.** Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering.
- 4.23.12.28.** O Serviço deve possuir funcionalidade de proteção positiva contra-ataques de manipulação de campo escondido.
- 4.23.12.29.** Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal.
- 4.23.12.30.** Deve possuir a capacidade de proteção do tipo Access Rate Control.
- 4.23.12.31.** Deve possuir a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DOS- Denial Of Service para qualquer política, através de Syn Cookie e Half Open Threshold.
- 4.23.12.32.** Deve permitir configurar regras de bloqueio a métodos HTTP indesejados.
- 4.23.12.33.** Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
- 4.23.12.34.** Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.
- 4.23.12.35.** Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.
- 4.23.12.36.** Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela Serviço.
- 4.23.12.37.** Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.



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

- 4.23.12.38.** Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
- 4.23.12.39.** Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha.
- 4.23.12.40.** Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos.
- 4.23.12.41.** Deve possuir a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade.
- 4.23.12.42.** Deve ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na Serviço e as requisições HTTP são enviadas aos servidores sem criptografia.
- 4.23.12.43.** O Serviço deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
- 4.23.12.44.** Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
- 4.23.12.45.** O Serviço deve ter a capacidade de armazenar certificados digitais de CA's.
- 4.23.12.46.** O Serviço deve ser capaz de gerar CSR para ser assinado por uma CA.
- 4.23.12.47.** O Serviço deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
- 4.23.12.48.** O Serviço deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões.
- 4.23.12.49.** O Serviço deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets e spammers. Tal sistema deve ser atualizado automaticamente.
- 4.23.12.50.** O Serviço Deve ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
- 4.23.12.51.** O Serviço deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location.
- 4.23.12.52.** O Serviço deve permitir criar regras definindo a ordem em que as páginas devem



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

ser acessadas para prevenir ataques como cross-site request forgery (CSRF).

- 4.23.12.53.** O Serviço deve ter a capacidade de definir restrições a métodos HTTP.
- 4.23.12.54.** O Serviço deve ter a capacidade de proteger contra a detecção de campos ocultos.
- 4.23.12.55.** Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
- 4.23.12.56.** O Serviço deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows.
- 4.23.12.57.** Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
- 4.23.12.58.** O Serviço deve gerar um relatório da análise de vulnerabilidades no formato HTML.
- 4.23.12.59.** O Serviço deve permitir a exclusão de URLs na análise de vulnerabilidades.
- 4.23.12.60.** Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 4.23.12.61.** Deve suportar redireção e reescrita de requisições e respostas HTTP.
- 4.23.12.62.** Deve permitir redirecionar requisições HTTP para HTTPS.
- 4.23.12.63.** Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
- 4.23.12.64.** Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
- 4.23.12.65.** Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
- 4.23.12.66.** Deve permitir redirecionar requisições para outro web site.
- 4.23.12.67.** Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
- 4.23.12.68.** Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
- 4.23.12.69.** Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor



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

web.

- 4.23.12.70.** Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
- 4.23.12.71.** O Serviço deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit).
- 4.23.12.72.** O Serviço deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação.
- 4.23.12.73.** Possuir capacidade de caching para aceleração web.
- 4.23.12.74.** Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
- 4.23.12.75.** Deve suportar no mínimo 500 regras de reescrita URL distintas.
- 4.23.12.76.** Deve suportar no mínimo 250 políticas de assinatura distintas.
- 4.23.12.77.** Deve suportar no mínimo 500 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1000 membros.
- 4.23.12.78.** Deve suportar no mínimo 1000 IPs virtuais configurados e ativos simultaneamente.
- 4.23.12.79.** Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré- configurado.
- 4.23.12.80.** Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.
- 4.23.12.81.** Deve ser capaz de criptografar URLs para prevenir acesso forçado e garantir que a estrutura de diretórios interna da aplicação web não seja revelada aos usuários.
- 4.23.12.82.** Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores.
- 4.23.12.83.** Deve implementar recursos de proteção de API (Application Programming Interface) através de Machine learning, implementando a análise dinâmica das chamadas de API para detecção de anomalias e bloqueando ataques direcionados a



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

aplicações baseadas em microserviços.

4.23.13. Serviços de Proteção de APIs

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

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

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

4.23.13.4. Métodos de Autenticação;

4.23.13.5. Tipos de Dados;

4.23.13.6. Mais e menos usadas;

4.23.13.7. Gerada automaticamente;

4.23.13.8. Especificações Swagger/OAS das APIs;

4.23.13.9. Detectar automaticamente e baseada em Inteligência Artificial;

4.23.13.10. Vazamento de Dados (Data leakage);

4.23.13.11. Adulteração de Dados (Data tampering);

4.23.13.12. Erros de Configuração (Misconfigurations);

4.23.13.13. Alterações nas APIs (Changes and Drift);

4.23.13.14. Violação de Política de Dados e Vulnerabilidades de API definidas pela OWASP Top 10;

4.23.13.15. Gráfico de Fluxo de Chamadas (Graphical Call Flows).

4.23.13.16. Atuar na Prevenção

4.23.13.17. Possibilitar a Interrupção da sessão TCP de comportamento suspeito se integrando com soluções de terceiros;

4.23.13.18. Possibilitar o envio de dados em tempo real (Webhook) em WAFs para criar políticas contra comportamento suspeito;



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

- 4.23.13.19.** Possibilitar a integração e atualização automática das regras de firewall para regular o comportamento suspeito;
- 4.23.13.20.** Possibilitar definição de políticas em gateways de API regulando as informações para destino ou cliente;
- 4.23.13.21.** Prevenção em linha para bloquear usuários ou APIs;
- 4.23.13.22.** Integrar com fluxos de trabalho existentes (tickets e SIEMs);
- 4.23.13.23.** Possibilitar o acompanhamento do tempo médio para atribuição, lida e resolução (MTTR – Mean Time to Resolve).
- 4.23.13.24.** Atuar a nível de Testes.
- 4.23.13.25.** Teste ativo das APIs em ambientes de pré-produção e produção.
- 4.23.13.26.** Implementação.
- 4.23.13.27.** Permitir a implementação sem a necessidade de instalação agentes;
- 4.23.13.28.** Permitir a implementação sem que haja necessidade de modificação na(s) rede(s);
- 4.23.13.29.** Possibilitar a integração com Gateways de API, load balancers, WAFs, agregadores de log;
- 4.23.13.30.** A CONTRATADA será responsável por:
 - Documentar, inventariar e manter atualizada a base de dados com as APIs.
 - implementar as políticas de proteção de APIs definidas pelo CREA-SP, monitorando, em tempo real, ameaças e atuando de forma proativa na proteção de tentativas de incidentes.

4.24. Serviços de Pentest

- 4.24.1.** A CONTRATADA deverá realizar serviços de PenTesting, do tipo DAST (Dynamic Application Security Testing), a cada 3 (três) meses.
- 4.24.2.** O alvo dos testes de invasão é o ambiente de tecnologia da informação da CONTRATANTE, incluindo:
 - 4.24.2.1.** Aplicações Web.
 - 4.24.2.2.** Servidores.



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

4.24.2.3. Banco de Dados.

4.24.2.4. Dispositivo de Rede.

4.24.3. Identificar vulnerabilidades presentes no ambiente tecnológico.

4.24.4. Avaliar a eficácia das medidas de segurança atualmente implementadas.

4.24.5. Documentar detalhadamente todas as vulnerabilidades identificadas.

4.24.6. Gerar relatórios abrangentes com recomendações específicas para a mitigação de riscos e aprimoramento da segurança cibernética da organização.

4.25. Programa Continuado de Conscientização da Importância da Segurança da Informação

4.25.1. A CONTRATADA deverá elaborar e implementar, em conformidade com a Política de Segurança do CREA-SP, programa continuado de conscientização da importância das ações preventivas e corretivas voltadas a segurança da informação, para os colaboradores do CREA-SP. O público alvo foi separado em 3 (três) categorias: Estratégico, Tático e Operacional. O público estratégico compreende o presidente, os diretores e superintendentes executivos. O público tático é formado pelos chefes de departamento e divisão, gerentes, os coordenadores de equipe e líderes de projeto. O público operacional compreende todos os funcionários da empresa não gerentes, técnicos, estagiários, incluindo os prestadores de serviço da companhia. Este programa deverá, ao longo de cada semestre, conter no mínimo:

4.25.1.1. duas palestras, sendo uma para todo o público alvo aqui descrito e a outra para o Público Estratégico;

4.25.1.2. vídeo(s) expondo situações cotidianas, a serem disponibilizados durante as palestras e na Intranet;

4.25.1.3. “QUIZ” que deverá ser disponibilizado na Intranet e no momento do login na rede, distribuído de forma aleatória para o público alvo, sendo sua leitura e resposta obrigatória para efetivação do login, ficando a responsabilidade da implementação desse mecanismo a cargo da CONTRATADA.

4.25.2. O conteúdo do programa deverá englobar:

4.25.2.1. Uso correto e aceitável dos ativos de tecnologia disponibilizados pelo CREA-SP;

4.25.2.2. Criação, manutenção e utilização correta de senhas;

4.25.2.3. Práticas corretas de mesa limpa e tela limpa;



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

- 4.25.2.4. Práticas corretas de troca de informações, sejam elas em documentos físicos e digitais, confidenciais ou não;
- 4.25.2.5. Práticas corretas de impressão de documentos, confidenciais ou não;
- 4.25.2.6. Práticas corretas de uso de internet e redes sociais, essas últimas quando liberadas para tal;
- 4.25.2.7. Práticas corretas de uso de correio eletrônico e ferramentas de colaboração;
- 4.25.2.8. Como identificar e evitar práticas de engenharia social;
- 4.25.2.9. Conversas em corredores, elevadores e outros lugares circulação de pessoas e lugares públicos.
- 4.25.2.10. Proteção contra códigos maliciosos;
- 4.25.3. A CONTRATADA deverá avaliar e apresentar relatórios, a cada seis meses, do grau de maturidade dos usuários quanto ao efetivo emprego de práticas de segurança da informação.
- 4.25.4. Serviços de Campanha de Conscientização de Segurança e Prevenção de Phishing – A CONTRATADA deverá:
 - 4.25.4.1. Elaborar cenários de phishing pertinentes e autênticos, adaptados às necessidades específicas da empresa.
 - 4.25.4.2. Criar e-mails com conteúdo convincente e realista, reproduzindo as estratégias empregadas por cibercriminosos, utilizando ferramenta para automatização desse processo.
 - 4.25.4.3. Desenvolver páginas de phishing que reproduzam fielmente interfaces de sites legítimos, com o intuito de capturar informações dos colaboradores.
 - 4.25.4.4. Monitorar e registrar as interações dos funcionários com os e-mails e páginas falsas, visando entender os padrões de comportamento e detecção de potenciais vulnerabilidades.
 - 4.25.4.5. Avaliar as taxas de cliques nos e-mails de phishing, bem como o preenchimento de informações nas páginas falsas e outros comportamentos relevantes.
 - 4.25.4.6. Gerar relatórios abrangentes contendo métricas, tendências e análises, destacando áreas de aprimoramento e oferecendo recomendações para fortalecer a segurança cibernética da organização.



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

4.25.4.7. A ferramenta deverá estar integrada com o sistema de SIEM para geração automática de relatórios.

4.26. Alocação dos Serviços

4.26.1. A CONTRATADA deverá fornecer, conforme especificado nos itens 4.26.7. e 4.26.8., profissionais que ficarão alocados na Sede da CONTRATANTE, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452 920 – São Paulo/SP, na escala de 8x5, atendendo horário comercial do Órgão, contemplado carga de 44 horas semanais.

4.26.2. A CONTRATADA deverá prover todas as ferramentas necessárias, para que os recursos possam desempenhar as funções designadas, como computadores e celulares.

4.26.3. A CONTRATADA é responsável por garantir a continuidade dos serviços, incluindo a substituição de recursos, em situações como férias, faltas não programadas ou demissões. Essa substituição deve ser realizada de forma a manter o nível de qualidade e eficiência estabelecido no contrato, assegurando assim a continuidade operacional sem interrupções prejudiciais ao funcionamento dos serviços prestados.

4.26.4. Todos os profissionais fornecidos pela CONTRATADA devem prestar atendimento presencial nas sedes Faria Lima, Angélica, Rebouças e Nestor Pestana., de 2ª a 6ª feira das 08:00hs às 19:00hs;

4.26.5. Das 19:01hs às 7:59hs a CONTRATADA deverá dispor de profissionais com mesmo perfil para atendimento remoto.

4.26.6. O dimensionamento total da equipe para prestação dos serviços deve garantir que as metas de qualidade do serviço sejam alcançadas, de modo que os serviços sejam executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais, conforme os requisitos específicos para o perfil profissional.

4.26.7. Qualificação Mínima da Composição da Equipe e Perfis Profissionais do NOC

4.26.7.1. Sobre características dos perfis e atribuições:

4.26.7.2. Analista de redes Junior

- Quantidade: 02 (dois) profissionais
- Atividades:
 - Realizar as atividades previstas para N1 do serviço de NOC – **(Das atividades da equipe do SOC como sendo N1;)**
 - Realizar as atividades previstas para o N2 do serviço de NOC **(Das atividades da equipe do SOC como sendo N2;)**



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

- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC)
Retirou
 - Conhecimentos em Infraestrutura (Servidores, Storage, Switches, Redes, Wi-Fi)

4.26.7.3. Analista de Infra (Servidores)

- Quantidade: 01 (um) profissional
- Atividades:
 - Realizar as atividades previstas para N1 do serviço de NOC – **(Das atividades da equipe do SOC como sendo N1;)**
 - Realizar as atividades previstas para o N2 do serviço de NOC **(Das atividades da equipe do SOC como sendo N2;)**
- Comprovação de Experiência anterior:
 - Comprovação de experiência anterior na instalação, configuração e manutenção de sistemas operacionais Windows, Linux e AIX em ambientes corporativos.
 - Familiaridade com ferramentas de administração centralizada como Microsoft System Center Operations Manager, Microsoft System Center Configurations Manager, WSUS (Windows Server Update Services) para servidores Windows, e ferramentas similares para servidores Linux.
 - Capacidade de monitorar e diagnosticar problemas nos servidores Windows, Linux e AIX, incluindo identificação e resolução de falhas, desempenho e gargalos de rede.
 - Experiência em configurar e aplicar Group Policy Objects (GPO) para padronização e aplicação de políticas de segurança em servidores Windows, bem como padrões de hardening em servidores Linux.
 - Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
 - Certificações reconhecidas relacionadas a administração de servidores Windows e Linux, como Microsoft Certified Solutions Associate (MCSA) e LPIC-1, respectivamente;

4.26.7.4. Gerente de NOC (Network Operating Center)

- Quantidade: 01 (um) profissional
- Comprovação de Experiência Anterior:
 - Experiência mínima comprovada de no mínimo 5 anos como Gerente e/ou Coordenador de Equipe de Tecnologia da Informação
 - Atuação comprovada de no mínimo 2 anos em Centro de Operações de Rede e/ou Centro de Operações de Segurança Cibernética
 - Experiência de no mínimo 5 anos em administração de redes de



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

Telecomunicações Locais e WAN, Fibra Óptica, Firewall, Switches, Roteadores, Dispositivos Wireless e Servidores de Aplicação e de Bancos de Dados.

- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
 - Possuir, certificação Network Security Blockbit ou equivalente emitida há no mínimo 12 (doze) meses.
 - Possuir pelo menos duas das seguintes certificações:
 - EHF - Ethical Hacking Foundation
 - EHE - Ethical Hacking Essentials
 - PDPP - Privacy and Data Protection Practitioner
 - PDPF - Privacy & Data Protection Foundation
 - CIH - Certified Incident Handler
 - Security+
 - CYSA+ (CompTIA Cybersecurity Analyst)
 - CCNA - Cisco Certified Network Associate
 - CCNP - Cisco Certified Network Professional
 - Carnegie Mellon CSIH – (Computer Security Incident Handler)
 - GCIH – (GIAC Certified Incident Handler)
 - GSOC – (GIAC Security Operations Certified),
 - ISO27001.
- Atividades:
 - Coordenar e Gerenciar a a equipe do NOC, conforme definidas no item correspondente des termo de Referência (**Das atividades Gerenciais**).

4.26.8. Da Composição da Equipe e Perfis Profissionais do SOC

4.26.8.1. Sobre características dos perfis e atribuições:

4.26.8.2. Analista de Segurança Cibernética Junior

- Quantidade: 01 (um) profissional
- Comprovação de experiência nas seguintes atividades:
 - Inteligência de Ameaças Cibernéticas.
 - Tratamento e resposta a Incidentes Cibernéticos.
 - Análise de Logs de ferramentas de Segurança Cibernética.
 - Mitigação de ataques.
 - Detecção de intrusões.
 - Segurança de redes.
 - Gestão de Vulnerabilidades.
 - Análise de Malware.
 - Conhecimento na utilização de ferramentas de Segurança Cibernética, como SIEM, WAF, e EDR, contemplando monitoramento, atividades de contenção,



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

como isolamentos e bloqueios, remediações, correções e configurações.

- Experiência mínima de 2 anos com Gestão de Vulnerabilidades, apoiando equipes técnicas nas correções, patchings, hardenings, atualizações e soluções de contorno necessárias para a segurança do ambiente da CONTRATANTE.
- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
 - Possuir, pelo menos uma, certificação como EHF, EHE, PDPP, PDPF, CIH, Security+, CYSA+, CCNA, CCNP, Carnegie Mellon CSIH, GIAC GCIH, GIAC GSOC, ISO27001.
- Atividades:
- Realizar as atividades do SOC referentes ao atendimento N1, conforme definidas **(Das atividades da equipe do SOC como sendo N1;)**
- Realizar as atividades do SOC referentes ao atendimento N2, conforme definidas **(Das atividades da equipe do SOC como sendo N2;)**
- Realizar as atividades de Gerenciamento de vulnerabilidades, conforme definidas **(Serviços de Gestão de Vulnerabilidades)**

4.26.8.3. Analista de Segurança Cibernética Senior

- Quantidade: 01 (um) profissional
- Comprovação de experiência nas seguintes atividades:
 - Inteligência de Ameaças Cibernéticas.
 - Tratamento e resposta a Incidentes Cibernéticos.
 - Análise de Logs de ferramentas de Segurança Cibernética.
 - Mitigação de ataques.
 - Detecção de intrusões.
 - Segurança de redes.
 - Gestão de Vulnerabilidades.
 - Análise de Malware.
 - Conhecimento aprofundado na utilização de ferramentas de Segurança Cibernética, como SIEM, WAF, Proteção de APIs e EDR, contemplando monitoramento, atividades de contenção, como isolamentos e bloqueios, remediações, correções e configurações.
 - Experiência mínima de 5 anos com Gestão de Vulnerabilidades, apoiando equipes técnicas nas correções, patchings, hardenings, atualizações e soluções de contorno necessárias para a segurança do ambiente da CONTRATANTE.
 - Experiência mínima de 5 anos na realização de Pentesting para Aplicações Web, Servidores, Bancos de Dados e Dispositivos de necessárias para a segurança do ambiente da CONTRATANTE.
- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da



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

computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).

- Possuir, pelo menos uma, certificação como EHF, EHE, PDPP, PDPF CIH, Security+, CYSA+, CCNA, CCNP, Carnegie Mellon CSIH, GIAC GCIH, GIAC GSOC, ISO27001.
- Atividades:
 - Realizar as atividades do SOC referentes ao atendimento N1, conforme definidas (**Das atividades da equipe do SOC como sendo N1;**)
 - Realizar as atividades do SOC referentes ao atendimento N2, conforme definidas (**Das atividades da equipe do SOC como sendo N2;**)
 - Realizar as atividades de Gerenciamento de vulnerabilidades, conforme definidas (**Serviços de Gestão de Vulnerabilidades**)

4.26.8.4. Analista de segurança (Aplicações)

- Quantidade: 02 (dois) profissionais
- Comprovação de experiência nas seguintes atividades:
 - Comprovação de experiência anterior de no mínimo 3 anos em desenvolvimento, definição de arquitetura, implantação de sistemas, suporte e manutenção em ambientes corporativos.
- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
 - Certificação certificação UML (Unified Modeling Language)
 - Sólidos conhecimentos dos princípios que regem os modelos de maturidade em desenvolvimento de software (RUP, MPS.BR, CMMI-DEV, ISO/NBR 15504)
 - Possuir treinamento em metodologia ágil SCRUM ou RUP, com no mínimo 24 horas
 - Possuir sólidos conhecimentos do PMBOK
 - Possuir experiência em implantação, suporte e e manutenção de sistemas que utilizam SGBDs relacionais como MySQL, PostgreSQL, Microsoft SQL Server 2008 e posterior e DB2.
 - Possuir no mínimo dois anos de experiência em linguagens JAVA, C# e .NET.
 - Possuir pelos menos uma das certificações: SCEA (Sun Certified Enterprise Architect), SCJD -Sun Certified Java Developer, SCWCD - Sun Certified Web Component Developer, SCBCD - Sun Certified Business Component Developer, SCDJWS - Sun Certified Developer for Java Web Services, Zend Certified PHP Engineer.
- Atividades:
 - Atuar juntamente com a equipe de desenvolvimento do CREA-SP na mitigação de vulnerabilidades de código em aplicações
 - Realizar as atividades de Gerenciamento de Vulnerabilidades relativas ao código das aplicações, conforme definidas (**Serviços de Gestão de**



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

Vulnerabilidades)

4.26.8.5. Gerente de Segurança Cibernética

- Quantidade: 01 (um) profissional
- Comprovação de experiência nas seguintes atividades:
 - Inteligência de Ameaças Cibernéticas.
 - Tratamento e resposta a Incidentes Cibernéticos.
 - Análise de Logs de ferramentas de Segurança Cibernética.
 - Mitigação de ataques.
 - Detecção de intrusões.
 - Segurança de redes.
 - Gestão de Vulnerabilidades.
 - Análise de Malware.
 - Conhecimento detalhado na utilização de ferramentas de Segurança Cibernética, como SIEM, WAF, Proteção de APIs e EDR. Contemplando monitoramento, atividades de contenção, como isolamentos e bloqueios, remediações, correções e configurações.
 - Experiência de no mínimo 5 anos em Planejamento e Gestão de Vulnerabilidades, apoiando equipes técnicas nas correções, patchings, hardenings, atualizações e soluções de contorno necessárias para a segurança do ambiente da CONTRATANTE.
 - Experiência de no mínimo 5 anos no Planejamento e Execução de Pentesting
 - Experiência comprovada de no mínimo 2 anos em Análise Digital Forense
 - Experiência mínima de 1 ano como Gerente / Coordenador de CSIRT
- Formação/Certificações
 - Curso superior completo na área de Tecnologia da Informação, Ciência da computação, engenharias ou exatas fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
 - Pós-Graduação em Perícia Forense Digital
 - Possuir obrigatoriamente certificação DFE
 - Possuir, pelo menos mais três, certificações como EHF, EHE, DFE, DCPT, CIH, Security+, CYSA+, CCNA, CCNP, Carnegie Mellon CSIH, GIAC GCIH, GIAC GSOC, ISO27001.
- Atividades:
 - Realizar as atividades definidas para o Gerenciamento do SOC, conforme definidas (**Das atividades Gerenciais do Gerente do SOC**)

4.27. SERVIÇO DE IMPLANTAÇÃO

4.27.1. Fica a cargo da CONTRATADA o dimensionamento da equipe para executar o Serviço de Implantação de forma a atender aos requisitos e aos prazos determinados neste Termo de Referência.

4.27.2. A CONTRATADA deve apresentar o documento de planejamento e o cronograma detalhado



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

para a implantação dos serviços, no prazo máximo de 10 (dez) dias, contados da data de assinatura do contrato.

- 4.27.3.** O cronograma deve contemplar, no mínimo, as seguintes atividades (e os recursos humanos e técnicos, da CONTRATANTE e da CONTRATADA, necessários à execução delas):
- 4.27.4.** Apresentação do planejamento à CONTRATANTE;
- 4.27.5.** Levantamento e documentação detalhada dos ativos que fazem parte do escopo deste projeto;
- 4.27.6.** Levantamento e documentação detalhada das topologias e infraestrutura que fazem parte do escopo deste projeto;
- 4.27.7.** A CONTRATADA deverá executar os serviços de implantação e configuração de todas as ferramentas e disponibilização de todos os profissionais no prazo de até 30 (trinta) dias, a contar da data da emissão da ordem de serviço emitido pela contratante. As atividades de planejamento, instalação/adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, deverão ser elaborados em conformidade com este Termo de Referência;
- 4.27.8.** Todas as atividades e documentações apresentadas deverão ser previamente aprovados pela CONTRATANTE.
- 4.27.9.** Plano de Implantação;
- 4.27.10.** Criação dos seguintes documentos:
- 4.27.11.** Plano de Comunicação;
- 4.27.12.** Matriz de Responsabilidade.
- 4.27.13.** 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;
 - 4.27.13.1.** 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;
 - 4.27.13.2.** A CONTRATADA, após o levantamento inicial das lacunas ou falhas de segurança da informação no ambiente da CONTRATANTE, deverá elaborar, coordenar e



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

supervisionar um plano de ação em conjunto com a CONTRATANTE, priorizando as falhas consideradas mais críticas;

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

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

4.27.15. 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;

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

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

4.27.18. 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;

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

4.28. DO NÍVEL MÍNIMO DE SERVIÇO

4.28.1. Visando assegurar a qualidade dos serviços, serão estabelecidos critérios mínimos de aceitação dos serviços aferidos mensalmente por ferramenta automatizada ou verificação da equipe de fiscalização técnica e associadas aos indicadores de níveis de serviço.

4.28.2. Todo e qualquer atendimento realizado pela equipe da Contratada deve ser registrado na ferramenta ITSM (GLPI) do CREA-SP, na entidade criada especificamente para esse fim, para computação das Métricas definidas a seguir:

4.28.3. Será responsabilidade da CONTRATADA computar os dados mensalmente e apresentar os relatórios para possibilitar ao Fiscal do Contrato aferir a qualidade do serviço apresentado, segundo as métricas a seguir:



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

- 4.28.4.** Métricas e Convenções.
- 4.28.5.** Horas expressas no formato “horas:minutos” indicam um relógio de 24 horas no fuso horário oficial Brasileiro (Brasília – GMT3);
- 4.28.6.** Horas indicadas como “horas úteis” incluem as horas de 08:00 às 19:00;
- 4.28.7.** Dias indicados como “dias úteis” incluem “horas úteis”, de segunda a sexta-feira, exceto os feriados oficiais nacionais e locais.
- 4.28.8.** Exclusões:
- 4.28.9.** Serão excluídos do cálculo de disponibilidade, os tempos de paralisação, decorrentes dos seguintes eventos:
- 4.28.10.** Janela de manutenção anual acordada entre CONTRATANTE e CONTRATADA;
- 4.28.11.** Falhas na infraestrutura provisionada pela CONTRATANTE decorrentes de eventos como:
- 4.28.12.** Perda de conexão com Internet;
- 4.28.13.** Perda de conexão com a rede corporativa;
- 4.28.14.** Acidentes operacionais internos;
- 4.28.15.** Falta de energia elétrica.
- 4.28.16.** Chamados escalados para o fabricante, em tratamento por este.
- 4.28.17.** Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados as metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade.
- 4.28.18.** Os Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança, são apresentadas, a seguir, sendo, portanto, exigências mínimas que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:
- 4.28.19.** No que se refere aos incidentes serão consideradas, as seguintes métricas:
- 4.28.19.1.** Crítica
- Mais de 80% dos funcionários (ou vários funcionários/equipes críticas) incapazes de trabalhar
 - Sistemas críticos off-line Alto risco para/violação definitiva de clientes confidenciais ou dados pessoais



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

- Infecção ou paralisação generalizada devido a ransomware ou algum outro tipo de malware;
- Danos graves à reputação - provavelmente impactarão os negócios a longo prazo

4.28.19.2. Alta

- 50% dos funcionários incapazes de trabalhar Sistemas não críticos afetados Risco de violação de dados pessoais ou sensíveis
- Potencial dano grave à reputação Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes que podem acarretar uma exploração ou vazamento de dados;
- Ocorrências\Incidentes\requisições relacionados a usuários definidos como VIP pelo contratante.

4.28.19.3. Média

- 20% da equipe incapaz de trabalhar Pequeno número de sistemas não críticos afetados Possível violação de pequenas quantidades de dados não confidenciais Baixo risco para a reputação demais servidores e sistemas apresentando instabilidade. Nenhum serviço crítico está envolvido e não existe risco de perda de dados

4.28.19.4. Baixa

- <10% da equipe não crítica afetada temporariamente (curto prazo) Impacto mínimo, se houver uma ou duas máquinas não sensíveis/não críticas afetadas nenhuma violação de dados Risco insignificante para a reputação
- Dúvidas ou apoio à implementação; Mudanças planejadas;
- Novas implementações;
- Sugestões de novos recursos ou aprimoramento do Software;
- Evidências de um bloqueio ou tratativa automatizada.

Categoria	Criticidade	Primeiro Atendimento	Tempo de Resolução	Meta	Glosa	Instrumento de medição
Incidente	Crítica	30 minutos	2 horas	≥ 98%	Glosa no valor mensal de 0,2% por incidente que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.
	Alta	45 minutos	4 horas	≥ 98%	Glosa no valor mensal de 0,2% por incidente que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.
	Média	2 horas	8 horas	≥ 98%	Glosa no valor mensal de 0,1% por incidente que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.
	Baixa	4 horas	24 horas	≥ 98%	Glosa no valor mensal de 0,1% por incidente que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.



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

4.28.19.5. No que se refere as requisições serão consideradas, as seguintes métricas:

- Alta
 - Atendimento à usuário de alta prioridade.
 - Os usuários de alta prioridade serão elencados pela Contratada em reunião de kick-off. Requisição urgente de Segurança da informação. Entende-se por requisições urgentes aquelas elencadas pela Contratada em reunião de kick-off.
 - Atendimento a demais requisições.
- Média
 - Análises, Relatórios, Mudanças de equipamentos, Atualizações, Verificações e Outros eventos sem impacto.
- Baixa
 - Atendimento a demais requisições.

Categoria	Criticidade	Primeiro Atendimento	Tempo de Resolução	Meta	Glosa	Instrumento de medição
Requisição	Alta	8 horas	16 horas	≥ 98%	Glosa no valor mensal de 0,1% por requisição que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.
	Média	24 horas	48 horas	≥ 98%	Glosa no valor mensal de 0,1% por requisição que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.
	Baixa	48 horas	96 horas	≥ 98%	Glosa no valor mensal de 0,1% por requisição que ultrapassar o limite da meta.	Extração de dados da ferramenta de ITSM.

4.28.19.6. As alterações nos Níveis Mínimos de Serviço, ou a inclusão de novo indicadores, deverão ser aprovadas em comum acordo e deverão ser registradas em documento a ser anexado ao Contrato, e ser assinado pelas partes.

4.28.19.7. Excepcionalmente, a revisão da lista também poderá ocorrer sempre que um novo serviço seja disponibilizado e levando em conta as contrarrazões, quando for o caso, da Contratada.

4.28.19.8. As glosas por descumprimento dos NMS, somadas, são limitadas ao percentual máximo de 10% (dez por cento) do valor de faturamento mensal.

4.28.19.9. Todo fechamento de chamado dever ser somente com a anuência da CONTRATANTE.

5. PERÍODO DE ADAPTAÇÃO OPERACIONAL

5.1. O período de ADAPTAÇÃO OPERACIONAL trata-se da fase em que a CONTRATADA, já em condições de executar os serviços, o faz, podendo incorrer em precariedade, haja



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

vista ainda não ter total domínio dos processos, procedimentos, normas, diretrizes, estabelecidas pela contratante.

- 5.2. O período de adaptação operacional se iniciará a partir do primeiro dia do efetivo início da execução do contrato, ou seja, após o aceite de todas implementações e início das operações período de transição Contratual, e correrá até o último dia do terceiro mês subsequente.
- 5.3. Durante o período de adaptação operacional não haverá penalidade de multa referente ao descumprimento do SLA.

6. RELATÓRIOS

- 6.1. A Contratada deverá gerar emitir relatórios mensais abrangendo, no mínimo, 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 nos componentes (rede, servidor, aplicação entre outros sistemas e aplicações.), providências tomadas e previsão de restabelecimento deles.
- 6.2. Deverão ser apresentados dois tipos de relatórios. Um relatório de Gestão e um relatório de Operação. O relatório de gestão deverá ser apresentado em reunião presencial na sede da contratante, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP até o 5º (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.