TERMO DE REFERÊNCIA

PRESTAÇÃO DE SERVIÇOS PARA FORNECIMENTO DE:

SOC (SECURITY OPERATIONS CENTER)

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

SERVIÇOS TÉCNICOS ESPECIALIZADOS

DIRETORIA DE INFRAESTRUTURA E TECNOLOGIA

Janeiro/2026

1. OBJETO

Contratação de empresa para prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação e Serviço Técnico Especializado, para o período de 36 (trinta e seis) meses.

1.1 TABELA DE COMPOSIÇÃO DOS ITENS

Item	Descrição	Unidade	Quantidade
1	Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC)	UN	01
2	Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)	1000 EPS (pacote)	144
3	Serviço de Implementação e Ativação de SOC e SIEM	UN	01
4	Serviços Técnicos Especializados de Segurança da Informação	Hora	3600

1.2 VIGÊNCIA

1.2.1 O contrato terá vigência de 36 (trinta e seis) meses, a contar da data de assinatura dos Termos de Aceite, previstos no item 10.2 deste documento, podendo ser prorrogado conforme dispõe a Lei Federal nº 13.303/2016.

2. SOLUÇÃO

2.1. Serviço de Monitoração, Notificação e Resposta a Incidentes de Segurança;

2.1.1. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC) em locais distintos, operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);

2.1.2. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:

2.1.2.1. Solução de proteção de endpoints;

2.1.2.2. Solução de prevenção contra vazamento de informações (DLP);
2.1.2.3. Solução de proteção de e-mails;
2.1.2.4. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;
2.1.2.5. Efetuar o registro dos visitantes com identificação individual e controle digital de entrada e saída, mantendo o registro armazenado e disponível para consulta por 90 dias;
2.1.2.6. Monitoramento por equipe de segurança patrimonial em regime 24x7x365;
2.1.2.7. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 90 (noventa) dias;
2.1.2.8. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações da CONTRATANTE devem assinar termo de responsabilidade e sigilo;

2.1.3. A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança em regime 24 X 7 (24 horas por dia, 7 dias da semana);
2.1.4. Deve fornecer controle dos eventos de SOC por meio de solução de gestão de operações de segurança da informação.
2.1.4.1. A solução deve possuir integração com a ferramenta de SIEM;
2.1.4.2. Estar atualizada e possibilitar acesso às principais funcionalidades, como:
2.1.4.2.1. Dashboards;
2.1.4.2.2. Detalhes de eventos;
2.1.4.2.3. Ferramentas de investigação;
2.1.4.2.4. Gerenciamento de tickets e alertas;
2.1.4.2.5. Relatórios;
2.1.4.2.6. Orquestração de trabalho coordenado em etapas manuais e automatizadas;
2.1.4.3. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática;
2.1.4.4. Permitir o recebimento de Alertas de Segurança com as seguintes características:
2.1.4.4.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;

2.1.4.4.2. Dados de origem e destino, portas de origem e destino, domínios de origem e destino, endereço MAC de origem e destino, além de informações de contexto de negócios de cada dispositivo (de origem ou destino). As informações de contexto deverão incluir endereço IP, nome do dispositivo, tipo, unidade de negócios, site, índice de criticidade e conformidade, além do proprietário, tanto para os dispositivos de origem quanto dispositivos de destino. É necessário também incluir informações de localização do dispositivo, incluindo cidade, país e geolocalização tanto dos dispositivos de origem quanto dos dispositivos de destino dos alertas;

2.1.4.4.3. A CONTRATADA deverá incluir a equipe técnica da CONTRATANTE nos alertas de segurança da informação, a critério da CONTRATANTE;

2.1.4.5. A solução deverá permitir a rastreabilidade das operações realizadas, referente à ação de tickets e em configurações;

2.1.4.6. Manter o histórico de todas as atividades realizadas pelos usuários, tais como criação de registro e atualizações de campos, vinculando o usuário que realizou cada procedimento;

2.1.4.7. Permitir a consulta e exportação das trilhas de auditoria, logs e históricos;

2.1.4.8. Prover mecanismo de proteção contra alteração e remoção indevida dos registros de auditoria;

2.1.4.9. Permitir a definição de controles de segurança, incluindo as seguintes informações: nome do controle, status de implementação, descrição, proprietário, custo operacional anual, categoria do controle (detecção/prevenção), custo fixo, localização e eficácia do controle ao longo do tempo. Desta forma, deverá ser possível avaliar a efetividade de controles implementados em face a Incidentes e Brechas de Segurança;

2.1.4.10. Permitir atrelar os controles de segurança a incidentes efetivos e inefetivos;

2.1.4.11. Possibilitar a criação de políticas de SOC com a definição de proprietário e descrição dos detalhes, além da definição das partes interessadas;

2.1.4.12. A CONTRATADA deverá fornecer à equipe técnica da CONTRATANTE, acesso em nível leitura à solução de gestão do SOC.

2.1.4.13. A solução deverá permitir a portabilidade dos dados, base de incidentes, base de conhecimento e logica dos processos definidos, podendo ser entregue em formatos: Base de Dados, arquivos texto (CSV, XML) ou PDF;

2.1.4.14. Permitir a geração de relatórios manuais e automatizados, possuindo funcionalidade de agendamento e envio por e-mail;

2.1.4.15. Possuir alguns relatórios pré-formatados, e possibilitar a exportação nos formatos CSV, PDF, MHTML, Excel e Word, para no mínimo:

2.1.4.15.1. Incidentes abertos por fase

2.1.4.15.2. Incidentes Encerrados por Duração

2.1.4.15.3. Incidentes Abertos Por Duração

2.1.4.15.4. Incidentes Abertos por severidade

2.1.4.15.5. Incidentes reabertos

2.1.4.15.6. Falso positivo por Solução

2.1.4.15.7. Tempo Médio de resolução por tipo de incidente

2.1.4.15.8. Tempo Médio entre o Alerta e o primeiro tratamento por tipo de incidente

2.1.4.15.9. Incidentes com SLA expirado por tipo de Incidente

2.1.4.15.10. Incidentes com SLA expirado por responsável

2.1.5. A CONTRATADA deve realizar as ações necessárias para identificação e solução dos incidentes de segurança por meio dos dados e alertas monitorados em Solução de SIEM, que podem comprometer a segurança dos serviços e ativos da CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição da CONTRATANTE, bem como identificar, registrar, escalar, mitigar e, caso necessário, notificar os incidentes de segurança à CONTRATANTE;

2.1.6. A CONTRATADA é responsável pelas atividades do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

2.1.6.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção.

2.1.6.2. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que

ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

2.1.6.2.1. Ataque de força bruta com e sem sucesso;
2.1.6.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;
2.1.6.2.3. Infecção de equipamentos por vírus;
2.1.6.2.4. Comprometimento de ativos da rede;
2.1.6.2.5. Realização de ações suspeitas por parte de usuários privilegiados;
2.1.6.2.6. Alertas de operação de serviços, como interrupções e falhas;
2.1.6.2.7. Ataques de negação de serviço;
2.1.6.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection;
2.1.6.2.9. Atividades de botnets;
2.1.6.2.10. Exploração de vulnerabilidades;

2.1.6.3. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

2.1.6.4. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias:

2.1.6.4.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;
2.1.6.4.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;
2.1.6.4.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de

segurança, como por exemplo, a análise de vulnerabilidades;

2.1.6.4.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

2.1.6.5. Registro de análise, todo evento detectado que for selecionado para análise deve ser registrado em Sistema de Ticket, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

2.1.6.5.1. Identificador do ticket;

2.1.6.5.2. Sensor que detectou o evento;

2.1.6.5.3. Identificador do evento gerado no sensor;

2.1.6.5.4. Limiar de detecção utilizado para enviar o evento para análise;

2.1.6.5.5. Log do evento detectado;

2.1.6.5.6. Origem e categoria do ataque;

2.1.6.5.7. Data e hora;

2.1.6.6. Triagem e Categorização de eventos, os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado;

2.1.6.7. Padronização de procedimentos de resposta à incidentes, os incidentes devem incluir procedimentos padronizados contendo as melhores práticas para seu tratamento e contenção, de modo que viabilize a execução das medidas corretivas necessárias pela CONTRATADA;

2.1.6.8. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato PDF, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

2.1.6.8.1. Classificação dos eventos de segurança;

2.1.6.8.2. Total de eventos avaliados;

2.1.6.8.3. Total de eventos escalados;

2.1.6.8.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;

2.1.6.8.5. TOP endereços de destino das ameaças;

2.1.6.8.6. TOP URLs e suas categorias;

2.1.6.8.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

2.1.6.8.8. Principais tipos de ataques;

2.1.6.8.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;

2.1.6.8.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

2.1.7. A CONTRATADA deverá ainda, no mínimo, realizar as seguintes atividades, sem se limitar a elas:

2.1.7.1. Análise de Regras e Políticas de Segurança:

2.1.7.1.1. Objetivo: Avaliar e revisar regras e políticas de segurança em vigor na CONTRATANTE.

2.1.7.1.2. Descrição: Conduzir análises de políticas e regras aplicadas a firewall, WAF, IPS, Endpoints, etc, realizar análises forenses e de tráfego de rede para identificar e mitigar riscos e aprimorar a elaboração de Playbooks de Resposta a Incidentes de Segurança da Informação.

2.1.7.2. Elaboração de Pareceres em Segurança da Informação:

2.1.7.2.1. Objetivo: Produzir relatórios detalhados e fundamentados sobre segurança da informação e analisar o nível de maturidade da estratégia de cibersegurança da CONTRATANTE (gestão de segurança e segurança cibernética).

2.1.7.2.2. Descrição: Realizar estudos e análises aprofundadas sobre aspectos de segurança da informação no ambiente de TIC da CONTRATANTE (on-premises e nuvem), gerar pareceres técnicos que ofereçam recomendações estratégicas baseadas em normas e melhores práticas, além de gap analysis para identificar áreas de melhoria.

2.1.7.3. Planos de Melhoria de Infraestrutura de Segurança:

2.1.7.3.1. Objetivo: Apoiar a melhoria contínua da infraestrutura de segurança.

2.1.7.3.2. Descrição: Auxiliar na elaboração de planos de melhoria que otimizem a segurança da infraestrutura existente. Prestar suporte na implementação de novas medidas de segurança.

2.1.7.4. Elaboração de Projetos Técnicos:

2.1.7.4.1. Objetivo: Desenvolver projetos técnicos destinados a mitigar vulnerabilidades na implantação de novos sistemas de informação, novas plataformas,

atualizações de software ou vulnerabilidades detectadas pela CONTRATANTE.

2.1.7.4.2. Descrição: Envolver-se na análise e gestão de vulnerabilidades, com foco em ações preventivas e/ou de remediação. Criar documentação técnica detalhada que aborde as vulnerabilidades identificadas, propondo soluções adequadas.

2.1.7.5. Definição e Implementação de Mecanismos de Monitoramento:

2.1.7.5.1. Objetivo: Estabelecer e implementar novos mecanismos de monitoramento e recursos de segurança.

2.1.7.5.2. Descrição: Propor e integrar novos sistemas de monitoramento que se alinhem com as plataformas de segurança da CONTRATANTE. Garantir a vigilância contínua e a pronta resposta a incidentes.

2.1.7.6. Desenvolvimento de Indicadores de Segurança:

2.1.7.6.1. Objetivo: Desenvolver e implantar novos indicadores de desempenho em segurança da informação.

2.1.7.6.2. Descrição: Criar métricas de segurança que permitam a avaliação contínua do ambiente de TI. Implementar indicadores não previstos anteriormente para cobrir novas ameaças.

2.1.7.7. Procedimentos de Auditoria Forense:

2.1.7.7.1. Objetivo: Fornecer orientações sobre auditorias forenses no ambiente de TIC.

2.1.7.7.2. Descrição: Estabelecer procedimentos padronizados para a realização de auditorias forenses.

2.1.7.8. Resposta a Incidentes de Segurança:

2.1.7.8.1. Objetivo: Apoiar na resposta eficaz a incidentes de segurança.

2.1.7.8.2. Descrição: Oferecer suporte especializado na gestão de incidentes de grande vulto. Coordenar ações de contenção, análise e remediação.

2.1.8. Um Sistema de Ticket deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes da CONTRATANTE e da própria CONTRATADA;

2.1.9. A CONTRATADA é responsável por avaliar os incidentes após o processo de triagem inicial. Caso o incidente seja confirmado, a CONTRATADA executará os seus processos e procedimentos internos para iniciar as medidas de contenção e correção,

incluindo configurações nos sensores de segurança ou outros ativos, sejam em dispositivos da CONTRATANTE OU DA CONTRATADA. A CONTRATADA registrará as ações realizadas no tíquete correspondente ao incidente;

2.1.10. Os analistas da CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone, Serviços de Troca de Mensagens ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

2.1.11. A CONTRATANTE é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;

2.1.12. A CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar a customização. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

2.1.13. Por padrão, não será fornecido nenhum tipo de acesso a dados ou sistemas da CONTRATANTE, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;

2.1.14. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia da CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente da CONTRATADA;

2.1.15. A CONTRATADA deve fornecer e, quando solicitado pela CONTRATANTE, apresentar:

2.1.15.1. Boletins periódicos, baseados nas informações de dados globais dos centros de pesquisa de ameaças, contendo novas táticas e técnicas de ataque, vulnerabilidades e

mecanismos de proteção de interesse da CONTRATANTE;

2.1.15.2. Relatórios mensais especializados para o ambiente da CONTRATANTE, incluindo informações de inteligência, como as novas vulnerabilidades identificadas, ameaças direcionadas identificadas, indicadores de ataque, reputação de endereços IP e domínios, indicadores sobre o cenário de segurança monitorado;

2.1.15.3. Relatório anual sobre a implementação do plano de ação e de resposta à incidentes;

2.1.15.4. Identificação, análise e compartilhamento de informações de ameaças relevantes e emergentes por meio de indicadores de comprometimento;

2.1.15.5. Todos os custos de atendimentos dos incidentes tratados pelo SOC estarão embutidos neste item, ou seja, não há número mínimo ou máximo para atendimentos de incidentes. Não haverá cobrança extra para este tipo de atendimento.

2.1.15.6. Todo o suporte e comunicação entre as equipes do SOC com a CONTRATANTE será em língua Portuguesa. Caso seja necessário contato com outros terceiros em outra língua, a CONTRATADA disponibilizará um funcionário com experiencia técnica que fara a tradução durante todo o período necessário para atendimento da ocorrência.

2.1.16. Alocação de Profissionais para os Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC):

2.1.16.1. Os profissionais do Centro de Operações de Segurança (SOC), em conformidade com as qualificações técnicas exigidas, deverão realizar serviço de monitoração, notificação e resposta a incidentes de segurança da informação.

2.1.16.2. Deverá ser disponibilizado pela CONTRATADA, o Centro de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), descritos em sua proposta técnica.

2.1.16.3. Os profissionais responsáveis por realizar o serviço de monitoração, notificação e resposta a incidentes de segurança da informação devem possuir, no mínimo:

2.1.16.4. Treinamento na ferramenta de GESTÃO DE SOC utilizada;

2.1.16.5. Experiência comprovada de 02 (dois) anos em monitorar, suportar e realizar a identificação e resposta à

2.1.16.6. incidentes de segurança da informação nos mais diversificados ambientes, provendo recomendações com base nas melhores práticas de segurança da informação;

2.1.16.7. Possuir conhecimento em análise e tratamento de incidentes de segurança da informação;

2.1.16.8. Pelo menos um dos profissionais do SOC deverá possuir certificação EC-Council Certified SOC Analyst (CSA);

2.1.16.9. A comprovação da capacitação técnica se dará mediante a apresentação de certificado de cada item acima no início da operação.

2.1.16.10. Em caso de incidentes a CONTRATADA poderá ser convocada para discutir planos de ação junto a outras empresas contratadas pela CONTRATANTE, no intuito de sanar o incidente relacionado. Podendo tal procedimento estar incluso nos playbooks a critério da CONTRATANTE.

2.2. Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)

2.2.1. Deve ser fornecido o serviço de ferramenta de coleta e correlação de eventos de segurança da informação;

2.2.2. O serviço deve ser fornecido provendo mecanismo de alta disponibilidade;

2.2.3. O Serviço deverá ser dimensionado para suportar o armazenamento de eventos de segurança em banco de dados dedicado, disponibilizando acesso aos logs de forma online via interface web por, no mínimo, 90 dias.

2.2.4. O serviço fornecido deve permitir a correlação de eventos provenientes de logs;

2.2.5. Associar, dinamicamente, usuários com os seguintes recursos mínimos:

2.2.5.1. Endereço de IP e nome do computador;

2.2.5.2. Endereço MAC;

2.2.5.3. Identificação do usuário logado;

2.2.6. Ser capaz de integrar em uma única console de visualização, todos os dados de logs coletados;

2.2.7. Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados coletados;

2.2.8. Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

2.2.9. Possuir regras de correlação especializadas na detecção de incidentes de segurança.

2.2.10. Dentre as regras de correlação, deverá possibilitar a criação de regras que, a partir dos diversos tipos de logs e flows, cubram os seguintes Casos de Uso:

2.2.10.1. Exfiltração de dados;

2.2.10.2. Identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados);

2.2.10.3. Comunicação de dispositivos internos com sites conhecidos por serem controladores de botnet.

2.2.11. Permitir o agendamento automático e manual de relatórios, com a possibilidade do envio por e-mail;

2.2.12. Coletar diariamente informações de fontes relevantes de inteligência de ameaças (ThreatIntelligence) para pesquisar novos tipos de ameaças.

2.2.13. Integrar com o serviço de inteligência de ameaças (ThreatIntelligence) deverá ter a capacidade de implementar técnicas de reputação categorizadas para no mínimo:

2.2.13.1. IP's/URL's mal intencionados;

2.2.13.2. Comportamento de ataque, não se limitando a:

2.2.13.2.1. Recon;

2.2.13.2.2. Weaponize;

2.2.13.2.3. Delivery;

2.2.13.2.4. Exploit;

2.2.13.2.5. Privilege Escalation;

2.2.13.2.6. Defense evasion;

2.2.13.2.7. Credencial Access;

2.2.13.2.8. Discovery

2.2.13.2.9. Exfiltration

2.2.13.3. Comportamento de malware;

2.2.13.4. Comportamento de spam;

2.2.13.5. URL's de phishing;

2.2.13.6. Atividade de botnet;

2.2.13.7. Atividade de C&C – Command&Control;

2.2.14. Integrar com o serviço de inteligência de ameaças (ThreatIntelligence) e deverá processar, normalizar, correlacionar, analisar e armazenar eventos de segurança, de forma escalável, possibilitando análise de ambientes com, no mínimo, 55.000 usuários;

2.2.15. Ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação externos, provenientes da base de conhecimento do fabricante da solução de SIEM, da base de conhecimento da própria CONTRATADA e de terceiros,

através do serviço de feeds de inteligência e alertas de ameaças direcionadas;

2.2.16. Ser capaz de detectar, em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

2.2.16.1. proxies anônimos;

2.2.16.2. endereços de rede TOR;

2.2.16.3. botnets e centros de Comando e Controle;

2.2.16.4. malware hosts;

2.2.16.5. IP's usados para scan de redes;

2.2.17. Possuir integração completa com a solução de GESTÃO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO, prevista no item 2.1.4;

2.2.18. Abrir chamados na solução de GESTÃO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO, de forma automática, sempre que detectar um potencial incidente de disponibilidade ou de segurança;

2.2.19. Permitir a criação de perfis de visualização dos eventos derivados dos dados coletados;

2.2.20. Possuir mecanismo de auditoria através da geração de logs das atividades realizadas na console de gerência e investigação;

2.2.21. Permitir a coleta de logs de forma distribuída e permitir a análise centralizada;

2.2.22. Possuir controle de acesso baseado em papéis e perfis de usuários;

2.2.23. Permitir a geração de relatórios em formatos HTML, PDF ou CSV;

2.2.24. Permitir a construção de relatórios customizados pelo usuário;

2.2.25. Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolo SYSLOG;

2.2.26. Utilizar formatos de logs/eventos nativos de cada fabricante dos dispositivos de segurança, sem utilizar um tipo de formato exclusivo e restrito, definido pelo fabricante da Solução de SIEM;

2.2.27. Permitir a definição e customização de alertas, relatórios e gráficos;

2.2.28. Ser licenciada para atender inicialmente, no mínimo, 4.000 (quatro mil) Eventos Por Segundo (EPS), para coleta, processamento, armazenamento e correlacionamento dos eventos, de forma sustentada.

2.2.29. A solução deve suportar escalabilidade na quantidade de EPS, permitindo crescimento sobre a quantidade de EPS contratada;

2.2.29.1. Será definida uma reserva de Eventos Por Segundos (EPS) prevendo um crescimento de 50% de acréscimo ao ano sobre o valor inicialmente contratado, com utilização sob demanda, podendo chegar a 15.000 EPS, durante a vigência contratual, sem garantia de execução em sua totalidade.

2.2.29.2. O valor será cobrado a partir de 4.000 EPS na ativação da solução. Após a ativação e aceite a CONTRATANTE poderá solicitar a CONTRATADA, aumento dos EPS, em pacotes de 1000 EPS, que serão pagos por demanda.

2.2.30. A solução deverá monitorar a quantidade de EPS contratada, com a obrigação de suportar picos que excedam o quantitativo estipulado, por até 8 dias no ciclo mensal de faturamento, processando o volume excedente até que este seja normalizado, sem incorrer na perda de eventos e sem incorrer em qualquer cobrança adicional por excesso ou bloqueio da solução.

2.2.31. A solução deve suportar a consolidação dos coletores de logs em um concentrador central;

2.2.32. A solução deve possuir relatórios que suportem a gestão das fontes de eventos, como data sources com erro.

2.2.33. A solução deve permitir a customização de novos relatórios baseados em dados de Logs e Flows de rede.

2.2.34. A solução deve segregar a visualização de relatórios apenas para usuários com a devida permissão;

2.2.35. A solução deve possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;

2.2.36. A solução deve possuir a funcionalidade para resolução de endereços IP, como identificação do país e organização das conexões;

2.2.37. A solução deve possuir um mecanismo de pontuação de risco no momento da análise de logs;

2.2.38. A solução deve permitir que, a partir de uma informação existente, se verifique o log que a gerou.

2.2.39. A solução deve permitir a análise avançada de eventos, podendo correlacionar eventos em uma base histórica;

2.2.40. A solução deve ser capaz de coletar e armazenar todos os logs de ativos de rede e dos dispositivos de segurança, gravando-os em formato original para posterior uso em análises forenses;

2.2.41. A solução deve ser capaz de coletar os logs dos ativos de rede e dos dispositivos de segurança de forma não intrusiva, sem a necessidade de instalação de agentes nos servidores da CONTRATANTE;

2.2.42. A autodetecção da solução deverá ser capaz de possibilitar a busca de eventos, com os seguintes recursos mínimos:

2.2.42.1. Busca em tempo real, baseada em “Google-likekeywords” e “SQL-likestructured queries”;

2.2.42.2. Possibilidade de converter os resultados procurados em relatórios ou dashboard/widgets;

2.2.43. Realizar a correlação e a geração de alertas em tempo real;

2.2.44. Suportar a criação de interpretadores (parsers) para a integração de logs não suportados nativamente;

2.2.45. Suportar a criação de interpretadores (parsers) customizados para no mínimo 20 sistemas proprietários;

2.2.46. Normalizar todos os logs recebidos de ativos de diferentes fornecedores, num formato comum;

2.2.47. Suportar de forma os logs de pelo menos 300 dispositivos diferentes de fabricantes variados;

2.2.48. Possuir capacidade de coletar e correlacionar logs de sistemas operacionais Windows, Linux, Unix e IBM z/OS;

2.2.49. Ser capaz de coletar e correlacionar logs de diversos tipos de dispositivos, tais como: firewalls, antivírus, IPS, proxies, servidores web, servidores DNS, servidores controladores de domínio, load balancers, roteadores, switches, aceleradores WAN e demais dispositivos de rede a critério da CONTRATANTE;

2.2.50. Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SNMP, SSH, Microsoft Windows Remote Management, Microsoft Windows EventLogging API, Network flow, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC/JDBC, VMWare VI-SDK e CISCO;

2.2.51. Não exigir a adição de agentes ou software nos dispositivos monitorados, exceto quando o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;

2.2.52. Permitir que os logs/eventos sejam enriquecidos/categorizados com informação de criticidade/severidade;

2.2.53. Notificar através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;

2.2.54. Gerar alertas baseados no recebimento de logs dos ativos monitorados, pelo menos, das seguintes ameaças:

2.2.54.1. Host scans, portscans, scans negados, repentino aumento ou redução do tráfego de/para certos endereços IP's;
2.2.54.2. Anomalias de Logon – excessivas falhas de logon, logon fora do expediente, logon a partir de endereços IP's não usuais;
2.2.54.3. Bloqueio de contas e passwordscans;
2.2.54.4. Botnets, worms e outros zero-daymalwares, através do cruzamento dos logs de DNS, DHCP e web proxy;

2.2.55. As regras de correlação da solução deverão permitir a detecção de thresholds ou utilizar testes e operadores lógicos para correlacionar eventos diferentes, permitindo:
2.2.55.1. Correlação por detecção de anomalia e padrão de comportamento;
2.2.55.2. Possibilitar a execução automática de scripts, a serem executados em casos "match" com a regra de correlação;
2.2.55.3. Possibilitar a configuração de política de notificação em cada regra;
2.2.55.4. O ajuste fino de regras de correlação, permitindo identificar as regras mais acionadas por eventos (que geram mais alertas);

2.2.56. Possuir um painel de controle (Dashboard), onde possa ver o log/evento coletado;
2.2.57. Fornecer painel de controle (Dashboard) que constantemente mostre o status do ambiente de correlação de eventos;
2.2.58. Possuir um dashboard integrado, com os seguintes recursos mínimos:
2.2.58.1. Visão consolidada das métricas de segurança, para todos os ativos de rede monitorados;
2.2.58.2. Customização do dashboard, adicionando relatórios e métricas;
2.2.58.3. Análise dos eventos de segurança da informação em tempo real;
2.2.58.4. Análise permitindo detalhá-la a partir de um gráfico geral, descendo aos níveis da análise conforme necessidade;

2.2.59. Ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
2.2.60. Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;

2.2.61. Oferecer uma administração centralizada que permita realizar investigações, gestão de incidentes, gestão de alertas e gestão de relatórios.

2.2.62. Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;

2.2.63. Suportar o recebimento de informações de pacotes de rede (Flow) coletados por ferramentas de terceiros, sendo capaz de analisar e correlacionar de forma contínua os dados recebidos;

2.2.64. Suportar o recebimento de informações coletadas por ferramentas de scan de vulnerabilidades de terceiros, sendo capaz de analisar e correlacionar de forma contínua os dados recebidos;

2.2.65. Ter a habilidade de receber logs/eventos oriundos de um relay de syslogs;

2.2.66. Suportar o recebimento de eventos no formato Common Event Format (CEF);

2.2.67. Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;

2.2.68. Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo.

2.2.69. Suportar de forma automática o armazenamento online (dados presentes no storage da solução) e Offline (dados presentes em sistemas de armazenamento off-line, backup, para possível restauração online);

2.2.70. Suportar algoritmos de compressão nos sistemas de armazenamento de longo prazo;

2.2.71. Permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;

2.2.72. Permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON ou CSV;

2.2.73. Possuir recurso para tratar dados arquivados e/ou recuperados;

2.2.74. Ser baseada em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação criptografada (HTTPS/TLS, versão 1.2 ou superior);

2.2.75. Suportar integração nativa com tecnologia de análise comportamental de entidade e usuário (UEBA), baseado em técnicas de machinelearning ou inteligência artificial, e análises estatísticas para a monitoração de segurança, devendo extrair os dados de usuário e entidades, ações executadas dos eventos coletados para geração de score de risco. A solução deve ser entregue com regras de correlação de análise de comportamento

de usuários e entidades prontas para uso, devendo processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM quando aplicável, ou devem considerar o total de 55.000 contas monitoradas (contas de usuários + contas de serviços), monitoração de desvios de comportamento de usuário identificando, no mínimo:

2.2.75.1. Acesso negado repetido;
2.2.75.2. Usuário acessando a VPN a partir de uma localidade atípica;
2.2.75.3. Usuário acessando a VPN a partir de horários atípicos;
2.2.75.4. Conta utilizada numa quantidade atípica de atividades;
2.2.75.5. Acesso a endereços considerados suspeitos por bases de Threatfeed/IP Reputation;
2.2.75.6. Conta de usuário criada e deletada rapidamente;
2.2.75.7. Detecção de ataque de negação de serviço pela deleção de contas;
2.2.75.8. Conta anômala em Cloud, criada a partir de uma nova localização;

2.2.76. Permitir identificar a data e hora do último login, de forma a garantir que a credencial não esteja sendo compartilhada;
2.2.77. Permitir o processamento de informações estruturadas de ameaças STIX™ (“StructuredThreatInformationeXpression”);
2.2.78. Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando a redução de erros de lógica e sintaxe;
2.2.79. Permitir a customização de perfis de visualização de eventos de acordo com o objetivo da investigação;
2.2.80. Permitir a pesquisa de eventos em Alertas, Incidentes ou Listas.
2.2.81. Permitir automação de fluxos de trabalho (playbooks);
2.2.82. Oferecer interface gráfica para criação e edição de playbooks;
2.2.83. Orquestrar respostas a incidentes de segurança de forma automática;
2.2.83.1. A orquestração e respostas a incidentes automatizada deverá iniciar, no mínimo com 10 regras implementadas, sem limites de novas regras durante a execução do contrato, sendo entre estas:
2.2.83.2. Resposta a ataques de IP's maliciosos
2.2.83.3. Bloqueio de usuários privilegiados com movimentação suspeita
2.2.83.4. Bloqueio de movimentação lateral de malware

2.2.83.5. Bloqueio de múltiplos hosts infectados pelo mesmo arquivo
2.2.83.6. Bloqueio de hosts com múltiplos malwares
2.2.83.7. Bloqueio de contas de serviços sob ataques

2.2.84. A solução deve integrar-se nativamente ou via API aos ativos da CONTATANTE;
2.2.84.1. A solução deve suportar integração com ferramentas de segurança e TI (firewall, EDR, antivírus, IAM, ITSM, e-mail, entre outras);

2.2.85. A solução deve registrar histórico de ações automatizadas e manuais;
2.2.86. A solução deve possibilitar gestão de incidentes, evidências e indicadores;
2.2.87. A solução deve permitir atuação humana (human-in-the-loop) quando necessário.

2.3. Serviço de Implementação e Ativação de SOC e SIEM

2.3.1. Serviços de implementação da solução de SOC e SIEM contempla planejamento e customização de toda solução executado pela CONTRATADA atendendo os requisitos da CONTRATANTE; e será pago em parcela única e somente no inicio do projeto após aceite formal da CONTRATANTE, mesmo que haja aumento na quantidade de EPS.
2.3.2. Todas as atividades relacionadas à implementação ocorrerão sob a responsabilidade e expensas da CONTRATADA, sem nenhum ônus adicional para a CONTRATANTE, cabendo a este somente o apoio técnico e a avaliação dos resultados, nos termos previstos neste Edital;
2.3.3. Por implementação e customização entendam-se todos os procedimentos relacionados às parametrizações e testes de quaisquer componentes das soluções ofertadas especificadas no escopo deste Edital, de modo a garantir o pleno funcionamento dos mesmos;
2.3.4. Todos os componentes requeridos para atender às funcionalidades exigidas neste Edital devem estar especificados na proposta;
2.3.5. A CONTRATADA deve criar e manter atualizada a documentação das atividades, dos processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, atas de reuniões, de modo a compor

uma documentação final da implantação a ser entregue à CONTRATANTE no final do processo;

2.3.6. A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de apoio a customização e implementação da solução, objeto deste Edital. Caso o diagnóstico aponte para problemas não relacionados aos serviços de apoio a customização e implementação da solução, a CONTRATANTE deverá executar os referidos procedimentos, desde que devidamente comprovados pela CONTRATADA, e a critério da CONTRATANTE.

2.3.7. A CONTRATADA deve, às suas expensas, alocar toda a equipe que irá executar os serviços de implementação descritos neste Edital;

2.3.8. Deverão ser alocados, pela CONTRATADA, profissionais qualificados para acompanhar o planejamento e a execução dos serviços de implementação dos componentes da solução;

2.3.9. A equipe alocada pela CONTRATADA deverá realizar as atividades do projeto, no mínimo, nas quantidades de horas descritas abaixo:

2.3.9.1. Profissionais com PERFIL TÉCNICO: 8 (oito) horas diárias, cada um, em horário comercial, durante todo o período de PLANEJAMENTO e EXECUÇÃO da implementação e integração da solução, desde a construção da versão inicial do Plano de Implantação até a emissão do Termo de Aceite;

2.3.9.2. Profissional com PERFIL GERENCIAL: 8 (oito) horas diárias, em horário comercial, durante todo o período de PLANEJAMENTO da implementação e integração da solução, desde a construção da versão inicial do Plano de Implementação, até a emissão do Termo de Aceite;

2.3.10. Dentre os profissionais alocados, a CONTRATADA deverá indicar um Gerente de Projetos, com certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos, que será o líder e responsável pela entrega dos serviços e pela implantação e integração da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital;

2.3.11. Todas as despesas referentes a transporte, alimentação, hospedagem e demais despesas operacionais da equipe alocada pela CONTRATADA ocorrerão às suas expensas;

2.3.12. A CONTRATADA disponibilizará acesso aos recursos computacionais e de apoio técnico às atividades de implementação, desde que absolutamente dentro do escopo das atividades da equipe da CONTRATANTE e a seu critério.

2.3.13. A CONTRATANTE se reserva o direito de redefinir, a qualquer momento da implementação, quaisquer fases, ações e prazos envolvidos, objetivando a garantia de atendimento dos parâmetros de qualidade, segurança, mitigação de riscos e atendimento de prazos, cabendo a CONTRATADA adequar-se às modificações propostas, refazendo atividades e documentação, caso seja necessário, desde que essas não extrapolem o escopo dos serviços aqui descritos;

2.3.14. A CONTRATADA deve apresentar à CONTRATANTE, em reunião própria, documento que balizará o acompanhamento de todo o projeto de implantação, em formato de Cronograma de Gantt, detalhando todas as fases, atividades, ações, recursos envolvidos (humanos e materiais), prazos, interdependências entre fases, atividades e ações, linha crítica temporal da implementação e quais serão os produtos gerados para cada fase, atividade e ação;

2.3.15. A CONTRATADA deve submeter o Plano de Implementação à homologação por parte da CONTRATANTE, reservando-se este o direito de requerer os ajustes necessários, observadas as melhores práticas amplamente aceitas no mercado e a realidade de seu ambiente;

2.3.16. A CONTRATADA deve englobar, no Plano de Implementação, todos os ajustes que venham a ser solicitados pela CONTRATANTE e apresentar a nova versão;

2.3.17. Os serviços de implementação contemplarão, pelo menos, a realização das seguintes macro-fases:

2.3.17.1. Homologação de funcionalidades da solução em ambiente controlado;

2.3.17.2. Implementação da solução em ambiente de produção;

2.3.17.3. Período de funcionamento experimental;

2.3.18. O Gerente de Projetos da CONTRATADA deve comunicar ao gestor da CONTRATANTE, responsável pelo acompanhamento da implementação dos serviços, a conclusão de cada macro-fase;

2.3.19. O plano de implementação deve considerar os seguintes prazos:

Nº	EVENTO	RESPONSÁVEL		PRAZO MÁXIMO (dias corridos)	A PARTIR DO FIM DO EVENTO
		CONTRATANTE	CONTRATADA		
1	Assinatura do contrato	X	X	--	
2	Entrega da versão inicial do plano de implantação		X	15	1

3	Entrega da versão final do plano de implantação		X	15	2
4	Termo de aceite do plano de implantação	X		5	3
5	Homologação dos Serviços de SOC	X	X	25	3
6	Implementação dos Serviços de SOC		X	30	3
7	Termo de aceite dos Serviços de SOC	X		5	6
8	Homologação dos Serviços de SIEM	X	X	55	3
9	Implementação dos Serviços de SIEM		X	60	3
10	Termo de aceite dos Serviços de SIEM	X		5	9

2.4. Serviços Técnicos Especializados de Segurança da Informação

2.4.1. Este item define um banco de horas de serviços técnicos especializados de segurança da informação, com utilização e pagamento sob demanda, durante a vigência contratual, sem garantia de execução em sua totalidade.

2.4.1.1. O valor estimado de consumo mensal é, em média, de 100 horas;

2.4.2. Os serviços técnicos deverão ser executados por profissionais qualificados e sempre considerando as melhores práticas do mercado, incluindo normas e regulamentações.

2.4.2.1. Conhecimento pleno de ferramentas de segurança, como SIEM, EDR, DLP, firewalls, antivírus e sistemas de detecção de intrusão (IDS/IPS);

2.4.2.2. Compreensão dos diferentes tipos de ameaças cibernéticas e suas características;

2.4.2.3. Conhecimento de frameworks de segurança, como o NIST Cybersecurity Framework;

2.4.2.4. Conhecimentos em segurança cibernética, redes e sistemas operacionais;

2.4.2.5. Capacidade de análise e investigação de incidentes de segurança;

2.4.3. Atendimento à Atividades de Operação da Segurança da Informação

2.4.3.1. Todas as atividades que sejam de atendimento à operação de Segurança da Informação, serão originadas por meio da ferramenta de ITSM da CONTRATANTE.

2.4.3.2. Todos os serviços de atendimento de atividades de operação da Segurança da Informação, serão solicitados por meio de ordem de serviço (OS), requisições de mudanças (RDM) e incidentes, abertos pela ferramenta de ITSM da CONTRATANTE e serão avaliadas e executados de acordo com os níveis de serviços definidos no ANEXO II.

2.4.4. Prazos

2.4.4.1. Item 1 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento em horário comercial (8 x 5), em dias úteis, sob demanda.

2.4.4.2. Item 2 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento 24 x 7 x 365 (24 horas por dia, sete dias por semana, 365 dias por ano), sob demanda.

2.4.5. Execução das Atividades de Operação da Segurança da Informação

2.4.5.1. No início da execução de cada atividade, a CONTRATADA deverá detalhar e incluir no plano de trabalho as Atividades a serem realizadas, impactos na infraestrutura e arquitetura do ambiente e recomendações para mitigação, caso seja necessário.

2.4.5.1.1. A CONTRATADA deverá iniciar a prestação do serviço no prazo estabelecido na própria ordem de serviço.

2.4.5.1.2. Os serviços serão e remunerados de acordo com preço previamente estabelecido para as atividades, conforme ANEXO I, independentemente do número de profissionais alocados ou do tempo efetivamente gasto na execução dos serviços.

2.4.5.2. Após o término de cada entrega prevista na atividade, a CONTRATADA deverá:

2.4.5.2.1. Apresentar relatório de conclusão dos serviços prestados detalhando todas as atividades realizadas.

2.4.5.2.2. Entregar toda documentação referente aos serviços prestados, contendo todos os documentos produzidos e gerados no contexto da sua execução, anexando à ferramenta ITSM da CONTRATANTE.

2.4.5.3. Os serviços serão prestados pela CONTRATADA remotamente.

2.4.5.3.1. Os serviços podem ser prestados nas dependências da CONTRATANTE, mediante comum acordo entre CONTRATANTE e CONTRATADA, sem ônus adicional para a CONTRATANTE.

2.4.5.3.2. Aqueles serviços que demandarem a presença física de profissionais da CONTRATADA nas dependências da CONTRATANTE deverão ser combinados em comum acordo e agendados previamente.

2.4.6. Local de prestação dos serviços

2.4.6.1. Independentemente dos cenários, dada a sensibilidade das informações tratadas no contexto dos trabalhos do SOC, é vedado o desempenho dessas tarefas em ambientes de trabalho compartilhados, tal como cafés e coworking;

2.4.7. Acesso às plataformas tecnológicas instaladas na CONTRATANTE

2.4.7.1. Controle de Acesso: Todo acesso às plataformas tecnológicas instaladas na CONTRATANTE, necessárias para a prestação dos serviços, será restrito apenas ao pessoal autorizado. Este acesso será realizado exclusivamente por meio de acesso remoto aos recursos da CONTRATANTE, utilizando credenciais de login e autenticação multifator para garantir a segurança.

2.4.7.2. Comunicação Segura: Toda comunicação entre os especialistas da CONTRATADA e as plataformas serão criptografadas. Isso inclui, mas não se limita a comunicações via rede, transferência de arquivos e quaisquer dados trocados entre as partes. A criptografia deve atender aos padrões de segurança mais rigorosos, garantindo a confidencialidade e a integridade das informações.

3 DAS OBRIGAÇÕES DA CONTRATADA

3.1 Iniciar a prestação dos serviços dentro dos prazos estabelecidos no Edital e seus anexos;

3.2 A implementação das soluções será realizada pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do CONTRATANTE;

3.3 A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

3.4 Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas para atendimento aos requisitos descritos neste Termo de Referência e em sua proposta;

3.5 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a CONTRATANTE autorizada a descontar da garantia, ou dos

pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

3.6 Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

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

3.8 Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique nos ativos da CONTRATANTE envolvidos nos serviços prestados;

3.9 Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços, indicando os chamados que foram atendidos dentro e fora do ANS estabelecido no Edital e seus anexos;

3.10 Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (ANS - SLA) do Edital e seus anexos;

3.11 Prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;

3.12 Paralisar, por determinação da CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

3.13 Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;

3.14 Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;

3.15 Submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações deste Termo de Referência;

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

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

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

3.19 Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE;

3.20 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

3.21 A contratada deverá prestar proteção dos dados a ela compartilhados durante toda a vigência contratual, desde o planejamento dos serviços objeto deste contrato;

3.22 Dentre as rotinas de execução dos trabalhos e etapas a serem executadas a contratada deverá realizar as seguintes atividades:

3.22.1 Executar a integração dos serviços da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega da CONTRATANTE;

3.22.2 Providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos serviços e detalhamento dos testes que serão executados para validar a solução implementada;

3.22.3 Executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do serviço, seguindo os procedimentos definidos no “Plano de Homologação e Testes;

3.22.4 Elaborar a “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

3.23 Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, análise de performance, tunning, resolução de problemas e implementação de segurança.

3.24 Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à implementação da solução.

3.25 A Contratada realizará adequação/configuração do serviço fornecido ao longo da etapa de migração e realização de novas configurações.

3.26 A CONTRATADA deve adotar um modelo de Centro de Operações de Segurança – SOC, prestado em período integral 24x7 (vinte e quatro horas, sete dias por semana) para o tratamento de eventos e incidentes de segurança da informação.

3.27 A medição do serviço será com base em indicadores e nível de serviço mínimo e deverá ser executado pela CONTRATADA, mensalmente, de modo a alcançar as respectivas metas exigidas, conforme INDICADORES DE NIVEL DE SERVIÇOS presente neste Termo de Referência.

3.28 A CONTRATADA deverá fornecer, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico e em português,

relatório detalhado sobre as atividades prestadas pela gestão de incidentes de segurança, geradas a partir do Serviço de Coleta e Correlação de Eventos de Segurança, contendo dados estatísticos pertinentes à gestão de incidentes de segurança, incluindo obrigatoriamente os campos abaixo:

3.28.1 Data/hora do início do evento ou incidente de segurança;
3.28.2 Nome do responsável pelo atendimento;
3.28.3 Descrição do evento ou incidente de segurança;
3.28.4 Severidade;
3.28.5 Número de identificação do chamado;
3.28.6 Descrição da solução realizada;
3.28.7 Tipo de evento ou incidente;
3.28.8 Data/hora de finalização do evento ou incidente de segurança;
3.28.9 Detalhamento do tempo em que o evento ou incidente ficou registrado na solução;
3.28.10 Consolidado dos chamados que não atenderem os prazos estabelecidos no item de INDICADORES DE NÍVEL DE SERVIÇOS, com suas devidas justificativas

3.29 Este relatório é uma obrigação contratual sujeita às sanções previstas no item de CÁLCULO DO NIVEL DE SERVIÇO, o qual deverá ser entregue por meio digital;

3.30 A CONTRATADA deverá fornecer, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico e em português, relatório detalhado sobre as atividades prestadas para atendimento da operação de segurança da informação, contendo dados estatísticos pertinentes às atividades, incluindo obrigatoriamente os campos abaixo:

3.30.1 Número de identificação do chamado;
3.30.2 Data/Hora início da execução
3.30.3 Nome do responsável pela execução
3.30.4 Descrição de todos os passos executados e suas devidas evidências
3.30.5 Severidade
3.30.6 Data/hora de fim da execução

3.31 Este relatório é uma obrigação contratual sujeita às sanções previstas no item de CÁLCULO DO NIVEL DE SERVIÇO, o qual deverá ser entregue no local de execução do contrato.

4 OBRIGAÇÕES DA CONTRATANTE

4.1 Prover acesso a rede física ou lógica sob demanda;
4.2 Ajustes na rede lógica da Prodam quando necessário;
4.3 Prover informações do ambiente de infraestrutura da Prodam para colaborar na solução de problemas;
4.4 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

4.5 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

4.6 As funções de gestão e fiscalização do contrato não recairão sobre o mesmo servidor, com as atribuições conforme a seguir especificadas:

4.6.1 Fiscal do Contrato: agirá de forma ativa e preventiva, observando o cumprimento, pela contratada, de todas as regras previstas contratualmente, além de buscar os resultados esperados do pacto com redução efetiva das inconsistências nos procedimentos de sua execução e, ainda, registrar todas as ocorrências relacionadas com a execução do contrato e encaminhar informações ao gestor do contrato.

4.6.2 Gestor do Contrato: irá controlar o processo referente ao contrato, zelando para que constem todos os documentos relativos à contratação, tais como: termo de referência/projeto básico, termo de contrato, ordem de serviço, portarias de nomeação/alteração de fiscal do contrato sempre que ocorrerem termos aditivos, termos de apostilamento, documentos fiscais, liquidações, obrigatoriedade de retenção na fonte dos tributos, entre outros.

4.7 Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

4.8 Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

4.9 Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da Contratada, no que couber;

4.10 Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

4.11 Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

4.12 Arquivar, entre outros documentos, projetos, as built, especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

5 INDICADORES DE NÍVEL DE SERVIÇOS

5.1 A execução dos serviços será gerenciada pela CONTRATADA, que fará o acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções de rumo.

5.2 Quaisquer problemas que venham a comprometer o bom andamento das atividades ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados à CONTRATANTE;

5.3 Tabela com a descrição da severidade de eventos de segurança da informação para atendimento de atividades de SOC e SIEM, não se limitando a isso, podendo a CONTRATANTE alterar, de acordo com a evolução tecnológica e sua necessidade:

Severidade	Descrição
1 – Crítica	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto médio ou alto em qualquer serviço crítico de TI; - Violação significativa de dados sensíveis; - Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente; - Vazamento de dados de acordo com a LGPD; - Evidências conclusivas de ataque cibernético.
2 – Alta	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em grande número de ativos ou ativos de alta criticidade; - Detecção de acesso não autorizado e/ou alterações em sistemas de informação; - Infecção persistente por código malicioso; - Intrusão persistente na rede; - Incidentes de segurança cibernética envolvendo dirigentes; - Ameaça significativa à disponibilidade e/ou integridade do ambiente; - Ameaça significativa à imagem da CONTRATANTE ou seus clientes.
3 – Média	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em poucos ativos ou um único ativo de média criticidade; - Detecção de varreduras em ativos ou tentativas mal-intencionadas de acesso não autorizado; - Intrusão na rede; - Infecção por código malicioso; - Alterações ou abuso de privilégios; - Ameaça à disponibilidade e/ou integridade do ambiente.
4 – Baixa	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em ativos pontuais ou ativos de baixa criticidade; - Violação das políticas de uso dos recursos tecnológicos; - Ocorrências não confirmadas, potencialmente mal-intencionadas; - Atividades anômalas detectadas na monitoração.

5.4 Os tempos corridos de atendimento máximos toleráveis para solução dos chamados constam nas tabelas a seguir em horas corridas:

Severidade	Descrição	Tempo de Resposta	Tempo de Solução
SEVERIDADE AGENDADA: O atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;	Esclarecimento de dúvidas ou similar.	8 horas	--
SEVERIDADE BAIXA: A Solução está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;	Sistemas operam sem impacto ao negócio.	4 horas	2 dias
SEVERIDADE MÉDIA: A Solução está operativa, mas suas funcionalidades são executadas com restrições;	Sistemas operam com degradação de desempenho.	40 minutos	24 horas
SEVERIDADE ALTA: A Solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;	Sistemas operam com paralisação parcial do ambiente.	20 minutos	12 horas
SEVERIDADE CRÍTICA: A Solução está totalmente parada ou inoperante;	Sistemas inoperantes ou paralisação total do ambiente.	10 minutos	6 horas

5.5 Os tempos de atendimento de Ordens de Serviços, Requisições de Mudanças e Incidentes demandados pelo serviço de ITSM da CONTRATANTE, terão os tempos de atendimento definidos pela própria ferramenta;

5.6 O não cumprimento dos prazos e dos critérios de qualidade determinados pelos controles definidos neste Termo de Referência sujeitará a

CONTRATADA às glosas e penalidades previstas neste Termo de Referência.

5.7 A frequência de aferição e de avaliação dos níveis de serviço será mensal, devendo a CONTRATADA elaborar relatório gerencial de serviços, contendo a mensuração dos indicadores constantes nas tabelas acima, indicando os demonstrativos e fontes de dados que embasaram tal medição, apresentando-os à CONTRATANTE em condições para que esta possa avaliar a devida aderência dos serviços prestados aos parâmetros de qualidade definidos neste Termo de Referência.

5.8 Devem constar desse relatório gerencial, entre outras informações, também registros de ocorrências relevantes (positivas ou negativas) do período em questão, recomendações técnicas, administrativas e gerenciais para os próximos períodos e quaisquer outras informações relevantes para que a CONTRATANTE tenha subsídios para realizar a devida gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes no primeiro mês de execução do contrato.

5.9 A entrega dos relatórios mensais será condição necessária à atestação dos serviços pela CONTRATANTE.

5.10 Caso algum nível de serviço ou parâmetro de qualidade for infringido, por razões fora da gerência da CONTRATADA, tais ocorrências não constarão do quadro de medições ou de registros negativos de qualidade de execução. No entanto, a CONTRATADA se obriga a descrever o ocorrido, contendo as devidas justificativas motivadoras do porquê não conseguiu contornar o ocorrido sem impacto nos níveis de serviço. Após, a CONTRATANTE avaliará, a cada ocorrência, a aplicabilidade desta cláusula.

5.11 As indisponibilidades programadas por mudanças autorizadas não serão computadas nos Indicadores de desempenho.

5.12 No caso dos indicadores de prazo de atendimento, não serão computados os tempos em que a solicitação aguarda retorno de informações do solicitante ou de equipe externa à gerência da CONTRATATADA, ou quando não existirem todos os pré-requisitos disponíveis de imediato.

5.13 Para fins de fiscalização contratual dos níveis de serviço, os primeiros 90 dias do contrato serão considerados período de estabilização e enfrentamento de curva de aprendizado inicial, sendo os níveis de serviços referentes a tal período aferidos, no entanto, no caso da infringência destes, não serão aplicadas as glosas correspondentes.

6 FISCALIZAÇÃO DOS SERVIÇOS

6.1 O acompanhamento dos serviços será executado de acordo com o Regulamento Interno da CONTRATANTE, bem como toda a legislação relacionada.

6.2 O faturamento e o ciclo de fiscalização contratual serão em base mensal.

6.3 A fiscalização requisitante procederá à análise da qualidade dos serviços com base nos parâmetros definidos no item 5 e subitens. Após, emitirá termo de recebimento definitivo, indicando, caso aplicável, se há indicação de descontos ou penalidades contratuais, e assinará aquele termo com o

6.4 Gestor do Contrato.

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

6.6 penalidades.

6.7 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

6.8 Após a apuração do valor devido no período em questão, a fiscalização requisitante informará a CONTRATADA o exato valor para o qual deverá ser emitida a nota fiscal de serviços.

6.9 Se existirem situações para as quais a CONTRATADA não concordar com o valor indicado pela CONTRATANTE como sendo o que deve ser faturado para o período em questão, aquela pode formalizar pedido de revisão, o qual será avaliado pela CONTRATANTE oportunamente e, caso acatado, a diferença será paga no período de faturamento subsequente à conclusão desta análise.

7 CONFIDENCIALIDADE

7.1 A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;

7.2 Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

8 PENALIDADES

8.1 Pela inexecução total ou parcial do objeto do Contrato, a CONTRATANTE poderá, garantida a prévia defesa, aplicar a CONTRATADA as seguintes sanções:

8.1.1 Advertência;

8.1.2 Multa de 1% (um por cento) por dia de atraso em qualquer uma das fases previstas no item 2.3 deste Termo de Referência - Serviço de Implementação e Ativação de SOC e SIEM, aplicável sobre o valor do faturamento do item em atraso;

8.1.2.1 Após o 30º (trigésimo) dia de atraso e, a critério da CONTRATANTE, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

8.1.3 Multa de 1% (um por cento) por ocorrência, aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento dos níveis de serviços relacionados às atividades descritas no item 5 - INDICADORES DE NÍVEIS DE SERVIÇOS e subitens 5.4 e 5.5;

8.1.4 Multa compensatória correspondente a 5% (cinco por cento), aplicável sobre o preço global do Contrato, caso não seja garantido absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados fornecidos pela CONTRATANTE, além das cominações previstas na legislação, podendo a CONTRATANTE rescindir o Contrato;

8.1.5 Multa de 10% (dez por cento), aplicável sobre o preço global contratado, nas demais violações ou descumprimentos de cláusula(s) ou condição(ões) estipulada(s) no Contrato;

8.1.6 Multa de 10% (dez por cento), aplicável sobre o preço global contratado, em caso de inexecução total do Contrato;

8.1.7 Suspensão temporária de participar em licitação e impedimento de contratar com a CONTRATANTE pelo prazo de até 2 (dois) anos.

8.1.8 Em caso de penalidades não previstas nos itens 8.1 a 8.7, será aplicada multa de 0,1% sobre o valor do contrato para cada termo de descumprimento ou cumprimento parcial.

9 QUALIFICAÇÃO TÉCNICA

9.1 A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) em papel timbrado por pessoa jurídica de direito público ou privado, que comprove(m) experiência prévia na prestação de serviço de fornecimento de serviços de mesma natureza do presente edital, ou seja, SOC, SIEM e Serviços Especializados de Segurança da Informação.

9.1.1 Para eventuais esclarecimentos, caso seja necessário durante a licitação, o(s) atestado(s) deverá(ão):

- **Estar devidamente datado(s) e assinado(s)**;
- Conter **identificação clara do atestante** (nome, cargo e empresa/instituição, telefone, e-mail etc.);
- Ser (em) emitido(s) por pessoa jurídica contratante dos serviços prestados.

9.1.2 Será aceita a apresentação de um único atestado ou a somatória de mais de um, desde que, em conjunto, comprovem a execução de serviços pertinentes, compatíveis com o objeto da contratação;

9.1.3 Para fins de comprovação de pertinência e compatibilidade, será considerado válido o(s) atestado(s) que comprove(m) a execução de, no mínimo, **50%** (cinquenta por cento) do total de EPS previsto no item 2 da Tabela de Composição de Itens constante deste Termo de Referência, correspondendo **a 72 (setenta e dois pacotes de 1000 EPS na execução total do contrato)**.

9.2 Para fins de julgamento das propostas a equipe de apoio técnico realizará a conferência técnica dos documentos exigidos, a saber:

9.2.1 Os atestados de capacidade técnica apresentados pelos licitantes em compatibilidade com os serviços realizados, com o objeto licitado, conforme especificado no Termo de Referência;

9.2.2 A verificação será conduzida por equipe de apoio técnico designada, com base nos critérios objetivos descritos no Termo de Referência.

9.3 Alocação de Profissionais, Item 2.1 - Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC):

9.3.1 A comprovação da capacitação técnica se dará mediante a apresentação de certificado de cada item acima.

10 ACEITE

10.1 O Termo de Aceite dos Serviços de SOC, SIEM e Atividades de Operação, será emitido mensalmente pela CONTRATANTE, no prazo de até 5 (cinco) dias úteis após a entrega do relatório mensal de atividades, emitido pela CONTRATADA, referente aos serviços prestados pelos itens “Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC)”, “Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)” e “Serviços Técnicos Especializados de Segurança da Informação”, itens1, 2 e 4 da Tabela de Composição de Itens.

10.2 O Termo de Aceite do Serviço de Implementação e Ativação de SOC e SIEM, será emitido pela CONTRATANTE, no prazo de até 5 (cinco) dias úteis após a entrega da formalização, por parte da CONTRATADA, do relatório de implementação contendo a comprovação do pleno funcionamento dos serviços previstos no item 3 da Tabela de Composição de Itens.

10.2.1 Entende-se por implementação e ativação a disponibilização de todas as funcionalidades exigidas neste Termo de Referência, inclusive e não se limitando a isso, com a entrega de evidências de registros de construção de automatização de regras de resposta a incidentes.

11 CONDIÇÕES DE FATURAMENTO

11.1 O valor dos itens 1, 2 e 4 da Tabela de Composição de Itens será faturado mensalmente em parcelas iguais, a partir da emissão do " Termo de Aceite dos Serviços de SOC, SIEM e Atividades de Operação";

11.2 O valor do item 3 da Tabela de Composição de Itens será faturado em parcela única, a partir da emissão do "Termo de Aceite do Serviço de Implementação e Ativação de SOC e SIEM";

12 CONDIÇÕES DE PAGAMENTO

12.1 A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do endereço eletrônico gfl@prodam.sp.gov.br

12.2 Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.

12.3 O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeiro (GFP), em 40 (quarenta) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.

12.4 Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.

12.5 Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica de caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% "pro rata tempore"), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

São Paulo, 15 de janeiro de 2026

gov.br Documento assinado digitalmente
WAGNER KANAGUSUKO
Data: 19/01/2026 15:34:51-0300
Verifique em https://validar.iti.gov.br

Wagner Kanagusuko
Gerente de Segurança da Informação – GIT

ANEXO I

CATEGORIA	TIPO	SUBCATEGORIA	FATOR DE PONDERAÇÃO		TEMPO DE EXECUÇÃO	FATOR DE CONVENÇÃO COLETIVA		(Ponderação x Tempo de Execução x Convenção SINDPD - formato horas)
			PERCENTUAL	COMPLEXIDADE		HORÁRIO DE EXECUÇÃO	Convenção Coletiva de Trabalho SINDPD/2023	
Incidente	Segurança da Informação	Ataque a Sites - Desconfiguração	1,35	Media	1	8-17h	1	01:21
Incidente	Segurança da Informação	Ataque a Sites - Negação de Serviço	1,83	Alta	1,5	8-17h	1	02:44
Incidente	Segurança da Informação	Ataque a Sites - Desconfiguração	1,35	Media	1	24h	1,3	01:45
Incidente	Segurança da Informação	Ataque a Sites - Negação de Serviço	1,83	Alta	1,5	24h	1,3	03:34
Incidente	Segurança da Informação	Firewall - Falha de HA - Indisponibilidade	1,35	Media	0,5	8-17h	1	00:40
Incidente	Segurança da Informação	Firewall - Alto Consumo de CPU / Memória	1,35	Media	0,5	8-17h	1	00:40
Incidente	Segurança da Informação	Firewall - Falha de HA - Indisponibilidade	1,35	Media	0,5	24h	1,3	00:52
Incidente	Segurança da Informação	Firewall - Alto Consumo de CPU / Memória	1,35	Media	0,5	24h	1,3	00:52
Incidente	Segurança da Informação	Incidente de Segurança	1	Baixa	1	8-17h	1	01:00
Incidente	Segurança da Informação	Incidente de Segurança	1	Baixa	1	24h	1,3	01:18
Incidente	Segurança da Informação	Proxy - Indisponibilidade	1,35	Media	0,25	8-17h	1	00:20
Incidente	Segurança da Informação	WAF - Falso Positivo	1	Baixa	0,25	8-17h	1	00:15
Incidente	Segurança da Informação	VPN Site-to-Site - Indisponibilidade	1,35	Media	0,5	8-17h	1	00:40
Incidente	Segurança da Informação	VPN Site-to-Site - Indisponibilidade	1,35	Media	0,5	24h	1,3	00:52
Incidente	Segurança da Informação	VPN Client-to-Site - Indisponibilidade	1	Baixa	0,15	8-17h	1	00:09
Incidente	Segurança da Informação	Atividade com avaliação e sem necessidade de atuação/execução	1	Baixa	0,15	8-17h	1	00:09
Incidente	Segurança da Informação	Atividade não relacionada à área ou informação incompleta	1	Baixa	0,15	8-17h	1	00:09

ANEXO I

CATEGORIA	TIPO	SUBCATEGORIA	FATOR DE PONDERAÇÃO		TEMPO DE EXECUÇÃO	FATOR DE CONVENÇÃO COLETIVA		(Ponderação x Tempo de Execução x Convenção SINDPD - formato horas)
			PERCENTUAL	COMPLEXIDADE		HORÁRIO DE EXECUÇÃO	Convenção Coletiva de Trabalho SINDPD/2023	
Ordem de Se	Antispam	Antispam - Relatório	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Antispam	Antispam - Rastreio de Mensagem	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Antispam	Antispam - Bloqueio / Liberação de Remetente	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Antispam	Antispam - Análise de Status de Mensagens	1	Baixa	0,25	8-17h	1	00:15
Ordem de Se	Antivírus	Antivírus - Relatório	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Antivírus	Antivírus - Suporte Instalação	1	Baixa	0,5	8-17h	1	00:30
Ordem de Se	Antivírus	Antivírus - Análise de Reputação (Bloqueio / Liberação)	1,35	Media	0,5	8-17h	1	00:40
Ordem de Se	Antivírus	Antivírus - Atualização de Versões	1,35	Media	0,25	8-17h	1	00:20
Ordem de Se	Antivírus	Antivírus - Bloqueio de USB (Device Control)	1,35	Media	0,5	8-17h	1	00:40
Ordem de Se	Antivírus	Antivírus - Análise de Relatório	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Antivírus	Antivírus - Manutenção de Host no EPO (adicionar / remover / mod	1,35	Media	0,5	8-17h	1	00:40
Ordem de Se	Projetos	Elaborar/Analisar	1,83	Alta	8	8-17h	1	14:38
Ordem de Se	Proxy/Firewall/IPS/Sites (	Liberar / Bloquear	1	Baixa	0,25	8-17h	1	00:15
Ordem de Se	Proxy/Firewall/IPS/Sites (	Relatórios / Log	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Proxy/Firewall/IPS/Sites (	Analisar Bloqueio	1,35	Media	0,5	8-17h	1	00:40
Ordem de Se	Reunião	Suporte, Análise e Consultoria	1	Baixa	2	8-17h	1	02:00
Ordem de Se	VPN Aruba	ClearPass OnGuard	1,35	Media	0,25	8-17h	1	00:20
Ordem de Se	VPN Aruba	Problemas de acesso	1,35	Media	0,25	8-17h	1	00:20
Ordem de Se	VPN Aruba	VIA - Virtual Intranet Access	1,35	Media	0,25	8-17h	1	00:20
Ordem de Se	WSUS	WSUS - Verificar/Sincronizar	1	Baixa	0,25	8-17h	1	00:15
Ordem de Se	WSUS	WSUS - Aprovar Novas Atualizações	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Segurança da Informação	Atividade com avaliação e sem necessidade de atuação/execução	1	Baixa	0,15	8-17h	1	00:09
Ordem de Se	Segurança da Informação	Atividade não relacionada à área ou informação incompleta	1	Baixa	0,15	8-17h	1	00:09

ANEXO I

CATEGORIA	TIPO	SUBCATEGORIA	FATOR DE PONDERAÇÃO		TEMPO DE EXECUÇÃO	FATOR DE CONVENÇÃO COLETIVA		(Ponderação x Tempo de Execução x Convenção SINDPD - formato horas)
			PERCENTUAL	COMPLEXIDADE		HORÁRIO DE EXECUÇÃO	Convenção Coletiva de Trabalho SINDPD/2023	
RDM	Segurança da Informação	Antivírus, Agente e MOVE - Alterar Regras/Instalar/Manutenção	1	Baixa	0,1	8-17h	1	00:06
RDM	Segurança da Informação	AVALIADOR - Antivírus, Agente e MOVE - Alterar Regras/Instalar/M	1	Baixa	0,1	8-17h	1	00:06
RDM	Segurança da Informação	AVALIADOR - Certificado Digital - Instalar em Servidor (SI-SB)	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	AVALIADOR - Firewall - Incluir/Alterar/Excluir Regra e ou NAT	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	AVALIADOR - Firewall - Rede Apartada	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	AVALIADOR - Firewall/IPS - Instalar/Manutenção,800	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	AVALIADOR - Instalar Novos Servidores de WSUS (NOC-SD-SI-SB)	1	Baixa	0,1	8-17h	1	00:06
RDM	Segurança da Informação	AVALIADOR - Proxy - Criar/Alterar/Excluir Regra	1	Baixa	0,1	8-17h	1	00:06
RDM	Segurança da Informação	AVALIADOR - Proxy - Instalar/Manutenção	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	AVALIADOR - Realizar Análise de Vulnerabilidade	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	Certificado Digital - Instalar em Servidor (SI-SB)	1	Baixa	0,5	8-17h	1	00:30
RDM	Segurança da Informação	Firewall - Incluir/Alterar/Excluir Regra e ou NAT	1	Baixa	0,5	8-17h	1	00:30
RDM	Segurança da Informação	Firewall - Configurar VPN Site-to-Site	1,35	Media	0,5	8-17h	1	00:40
RDM	Segurança da Informação	Firewall - Configurar rede WiFi	1,35	Media	0,5	8-17h	1	00:40
RDM	Segurança da Informação	Firewall - Configurar Rede Apartada	1,35	Media	0,5	8-17h	1	00:40
RDM	Segurança da Informação	Firewall - Manutenção (Corretiva / Preventiva)	1,35	Media	2	24h	1,3	03:30
RDM	Segurança da Informação	Firewall - Setup de Firewall	1,83	Alta	4	8-17h	1	07:19
RDM	Segurança da Informação	Firewall - Instalar / Desinstalar	1	Baixa	2	8-17h	1	02:00

ANEXO I

CATEGORIA	TIPO	SUBCATEGORIA	FATOR DE PONDERAÇÃO		TEMPO DE EXECUÇÃO	FATOR DE CONVENÇÃO COLETIVA		(Ponderação x Tempo de Execução x Convenção SINDPD - formato horas)
			PERCENTUAL	COMPLEXIDADE		HORÁRIO DE EXECUÇÃO	Convenção Coletiva de Trabalho SINDPD/2023	
RDM	Segurança da Informação	WAF - Incluir Aplicação	1,83	Alta	1,5	8-17h	1	02:44
RDM	Segurança da Informação	WAF - Ajustes de Configuração	1,83	Alta	1	8-17h	1	01:49
RDM	Segurança da Informação	WAF - Manutenção (Corretiva / Preventiva)	1,35	Media	2	24h	1,3	03:30
RDM	Segurança da Informação	Instalar Novos Servidores de WSUS (NOC-SD-SI-SB)	1,35	Media	1	8-17h	1	01:21
RDM	Segurança da Informação	Proxy - Liberar / Bloquear - Filtro de Conteúdo	1	Baixa	0,25	8-17h	1	00:15
RDM	Segurança da Informação	Proxy - Instalar / Desinstalar	1	Baixa	2	8-17h	1	02:00
RDM	Segurança da Informação	Proxy - Setup de Proxy	1,83	Alta	2	8-17h	1	03:39
RDM	Segurança da Informação	Proxy - Manutenção (Corretiva / Preventiva)	1,35	Media	2	24h	1,3	03:30
RDM	Segurança da Informação	Cloud - Incluir/Alterar/Excluir Regra de Firewall	1,83	Alta	0,25	8-17h	1	00:27
RDM	Segurança da Informação	Cloud - Configurar VPN Site-to-Site	1,83	Alta	0,5	8-17h	1	00:54
RDM	Segurança da Informação	Realizar Análise de Vulnerabilidade	1,35	Média	1	8-17h	1	01:21
RDM	Segurança da Informação	VPN - Client-to-Site - Instalar / Desinstalar	1	Baixa	2	8-17h	1	02:00
RDM	Segurança da Informação	VPN - Client-to-Site - Setup	1,83	Alta	2	8-17h	1	03:39
RDM	Segurança da Informação	VPN - Client-to-Site - Manutenção (Corretiva / Preventiva)	1,35	Media	2	24h	1,3	03:30
RDM	Segurança da Informação	VPN - Client-to-Site - Configuração de Regras	1,35	Media	0,25	8-17h	1	00:20
RDM	Segurança da Informação	Atividade com avaliação e sem necessidade de atuação/execução	1	Baixa	0,1	8-17h	1	00:06
RDM	Segurança da Informação	Atividade não relacionada à área ou informação incompleta	1	Baixa	0,1	8-17h	1	00:06