ESTUDO TÉCNICO PRELIMINAR

SIGA Nº CTEC-ETP-2025/00002

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A infraestrutura de tecnologia do município de Bento Gonçalves é atualmente protegida por soluções críticas de segurança cibernética da marca Sophos: o Next-Generation Firewall (NGFW) e a Proteção de Endpoints (Antivírus). Estas soluções integradas formam a espinha dorsal da defesa digital do município, garantindo a integridade, confidencialidade e disponibilidade dos dados e sistemas governamentais.

Com a aproximação do término da vigência das licenças previamente contratadas, torna-se imperativa a abertura de um processo licitatório para a renovação das licenças do NGFW. Esta renovação é de suma importância, pois, caso não seja realizada, todos os serviços essenciais de segurança deixarão de funcionar. Isso inclui o bloqueio a ataques de rede, o controle de acesso de usuários a sites, o AntiSpam do e-mail corporativo e diversos outros serviços que compõem nossa barreira de segurança contra ameaças cibernéticas.

A não renovação dessas licenças poderia resultar em consequências catastróficas para o município. Existe o risco real de comprometimento da infraestrutura de rede, potencial perda de dados armazenados nos servidores municipais e até mesmo danos permanentes aos equipamentos pertencentes ao município. Tais cenários não apenas comprometeriam a eficiência operacional, mas também poderiam resultar em violações de privacidade e perda de confiança pública.

Além da necessidade crítica de renovação das licenças, o município enfrenta um desafio adicional este ano. O fabricante Sophos anunciou recentemente o fim do ciclo de vida para sua linha de appliances XG, o que afeta diretamente os dois equipamentos Sophos XG Firewall modelo XG 330 atualmente em uso pelo município. Esta situação demanda não apenas a renovação das licenças, mas também a substituição dos equipamentos de hardware.

Baseado em uma análise minuciosa da carga atual e das projeções futuras de demanda, foi determinado que o novo equipamento Sophos XGS 4500 seria capaz de atender às necessidades do município. Este modelo foi escolhido por sua capacidade de suportar a carga atual com uma margem de crescimento de 50%, além de oferecer uma expectativa de vida útil de, no mínimo, 7 anos antes de necessitar de um novo upgrade.

Para fortalecer ainda mais a postura de segurança do município, faz-se necessária a implementação de uma plataforma de Gerenciamento e Correlação de Eventos de

Segurança da Informação (SIEM). Esta solução complementará a solução de NGFW e a Proteção de Endpoints (Antivírus) já existentes, proporcionando uma visão holística e em tempo real de toda a infraestrutura de segurança. A implementação do SIEM permitirá uma detecção mais rápida e eficaz de ameaças complexas, melhorando significativamente a capacidade de resposta a incidentes do município.

Considerando as especificidades técnicas e operacionais da solução de Next-Generation Firewall (NGFW) e da nova plataforma SIEM, o processo de contratação visa garantir a melhor estratégia de aquisição para o município de Bento Gonçalves. A escolha criteriosa do fabricante e do modelo de equipamento leva em conta não apenas o desempenho técnico, mas também a compatibilidade com a infraestrutura existente e a capacidade de atender às demandas de segurança cibernética do município.

Para garantir um alinhamento perfeito na estratégia de segurança cibernética do município e assegurar o máximo aproveitamento das soluções adquiridas, faz-se necessária também a contratação de uma empresa especializada. Esta empresa terá a missão de guiar a equipe técnica do município na condução da área de segurança da informação e segurança cibernética. As limitações técnicas e de recursos humanos, naturais dos tradicionais departamentos de TI, exigem serem supridas por profissionais especialistas, constantemente atualizados com as novidades deste segmento em rápida evolução.

Considerando o tamanho, a abrangência e a criticidade da infraestrutura de tecnologia do município de Bento Gonçalves, onde serviços públicos essenciais como saúde e segurança pública necessitam de disponibilidade total, é imprescindível que os appliances de Firewall e a plataforma SIEM que compõem a solução de segurança sejam monitorados continuamente. Além disso, o suporte técnico contratado deve estar disponível em tempo integral, 24 horas por dia, 7 dias por semana. Este serviço deve ser pautado por um Acordo de Nível de Serviço (ANS) que delimite prazos de atendimento rígidos, inclusive para atendimentos presenciais, caso o incidente assim exija.

Outro aspecto crucial desta contratação é a instalação e implantação dos novos equipamentos, uma vez que os atuais serão descontinuados pelo fabricante. Em virtude de uma série de razões, como novas funcionalidades, necessidade de revisão de regras de segurança e objetos obsoletos, e a adoção de melhores práticas de configurações de segurança, a equipe de TI do município optou por realizar uma implantação inteiramente nova, partindo do zero, ao invés de meramente importar as configurações do equipamento antigo para o novo. Esta abordagem garantirá que os novos equipamentos não herdem configurações excessivas e, na maioria das vezes, desnecessárias, que poderiam trazer lentidão, vulnerabilidades e insegurança ao ambiente.

Para garantir a máxima eficácia das novas soluções e a capacitação adequada da equipe de TI, é necessário incluir uma camada de treinamentos especializados. Estes treinamentos devem abranger as novas funcionalidades do NGFW, bem como a operação e gerenciamento da nova plataforma de SIEM. É crucial que estes treinamentos sejam ministrados por instrutores devidamente certificados pelos fabricantes das soluções, assegurando assim a qualidade e atualidade do conhecimento transmitido.

Em conclusão, a contratação para renovação de licenças e substituição dos equipamentos da solução de Next-Generation Firewall (NGFW), a implementação de uma plataforma SIEM, juntamente com a aquisição de serviços especializados de suporte, implantação e treinamento, é essencial para manter e aprimorar a segurança cibernética do município.

Esta abordagem abrangente não apenas garantirá a continuidade dos serviços de TI e atenderá às necessidades atuais e futuras de proteção da infraestrutura tecnológica, mas também otimizará recursos financeiros e operacionais.

Esta estratégia holística de segurança cibernética não é apenas uma medida preventiva, mas um investimento crucial no futuro digital seguro do município de Bento Gonçalves. Ao combinar tecnologia de ponta, expertise especializada, monitoramento contínuo e capacitação da equipe interna, o município estará bem posicionado para enfrentar os desafios de segurança digital em constante evolução, garantindo assim a integridade e eficiência dos serviços públicos essenciais para seus cidadãos.

2. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

Não se aplica

3. REQUISITOS DA CONTRATAÇÃO

3.1. REQUISITOS PARA A EXECUÇÃO DO SERVIÇO

3.1.1. REQUISITOS GERAIS

A CONTRATADA deverá executar a instalação física e a configuração lógica dos produtos, conforme especificado nos itens na tabela presente no Objeto deste Termo de Referência.

Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados, incluindo deslocamento e demais despesas de seus profissionais para as unidades onde as soluções serão instaladas;

Caberá a CONTRATANTE subsidiar toda infraestrutura necessária para implantação das soluções de firewall, exemplo: locais de instalação dos appliances de Firewalls (Racks, gavetas);

Os serviços de implantação deverão ser executados presencialmente nas instalações da CONTRATANTE por técnico(s) da CONTRATADA capacitado(s) para tal;

Após o recebimento dos equipamentos e das licenças, a CONTRATANTE deverá definir, juntamente com a CONTRATADA, o cronograma de instalação e configuração dos mesmos, enviando a CONTRATADA, documento contendo informações de Data, Hora, Local, e soluções a serem instaladas;

3.1.2. FASES DO SERVIÇO DE IMPLANTAÇÃO

As fases da implantação dos serviços devem contemplar:

Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento da solução a ser implementada, onde serão definidos os prazos por atividade, as pessoas, a estratégia de

implantação do serviço, o plano de testes, bem como quaisquer outros itens que sejam necessários para a implantação da respectiva solução. Deve-se considerar as janelas de manutenção da CONTRATANTE, plano de rollback e o escopo definido. Os responsáveis técnicos da CONTRATANTE acompanharão e aprovarão o planejamento;

Implantação: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

Etapa de Testes: todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço;

Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pela CONTRATANTE.

A CONTRATANTE terá o prazo de 02 (dois) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite);

O serviço será aceito se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos utilizados, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos itens deste Termo;

No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados;

O processo de instalação, implantação e configuração deverá ter início em no máximo 15 (quinze) dias após o recebimento dos equipamentos e das licenças. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

Após a conclusão dos serviços de instalação, o técnico da CONTRATADA deverá realizar o monitoramento da solução por pelo menos 04 (quatro) dias úteis, com acompanhamento da equipe da CONTRATANTE, a fim de identificar e sanar eventuais inconsistências;

Ao término da instalação, a CONTRATADA deverá entregar Caderno de Documentação "As Built" do Projeto, no qual conste todos os detalhes da instalação, tais como:

1. Descrição dos serviços implantados;
2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;
4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;
5. Definição de responsabilidades;
6. Recursos de alta disponibilidade;
7. Procedimentos para abertura e atendimento a chamados;
8. Procedimentos de recuperação de equipamentos;
9. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;
10. Documentação dos processos de trabalho associados ao item;
11. Desenho dos racks onde estão instalados os equipamentos (bayface);
12. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);

3.1.3. ESCOPO DO SERVIÇO DE IMPLANTAÇÃO

1. Instalação das Soluções de Firewall, conforme contratado;
2. Configurar as Soluções de Firewall conforme segmentação de rede definida pela CONTRATANTE;
3. Atualização e aplicação de correções nas soluções de Firewall;
4. Implementação/migração de regras de Filtragem;
5. Implementação/migração de regras de NAT;
6. Implementação/migração de regras de QoS;
7. Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Antimalware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
8. Implementação de alta disponibilidade, quando aplicável;
9. Implementação de monitoramento de links, quando aplicável;
10. Integração com o Active Directory;
11. Tunning de configuração e regras de filtragem, removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados;
12. Testes gerais, validando o funcionamento das aplicações após a implementação dos Firewalls;
13. Registrar e associar todos os dispositivos de firewall a solução de gerenciamento;
14. Configuração de comunicação para permitir o tráfego entre a solução de gerenciamento e dispositivos firewalls;
15. Importar configurações existentes, quando aplicável;
16. Configuração de alertas e notificações para eventos críticos de segurança;
17. Definição de grupos de administração;

Não faz parte do Escopo dos Serviços de Implantação da Solução de Firewall:

1. Passagens de cabo que não compreendam as necessárias para conectividade das soluções de firewall e proteção da rede;
2. Instalação de demais soluções e equipamentos que não compreendam os mencionados neste serviço de implantação;
3. Configuração de equipamentos de terceiros;

3.2 REQUISITOS PARA A EXECUÇÃO DOS SERVIÇOS DE CIBERSEGURANÇA PARA FIREWALL DE PRÓXIMA GERAÇÃO (NGFW), SIEM E SERVIÇOS ESPECIALIZADOS

3.2.1. REQUISITOS GERAIS

O propósito do gerenciamento executado pela CONTRATADA é manter a estabilidade, disponibilidade e integridade do ambiente computacional da CONTRATANTE, operando e sustentando todas as soluções de segurança contemplados nesse Termo de Referência, além de responder às solicitações dos usuários, resolver incidentes e realizar atividades proativas para reforçar a segurança.

Durante os primeiros 30 dias de prestação do serviço, a CONTRATADA deverá conduzir uma avaliação abrangente do ambiente do CONTRATANTE, visando identificar lacunas ou oportunidades de aprimoramento (Gap Analysis) dos controles de segurança do CONTRATANTE.

A CONTRATADA deverá ter processos estabelecidos que assegurem a proteção das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.

A CONTRATADA será responsável pela manutenção, ativação e gestão de licenciamento, bem como a atualização da solução durante a vigência do contrato.

Principais atividades a serem executadas de forma contínua pela CONTRATADA:

1. Acompanhar a execução dos serviços para garantir a conformidade com os níveis de serviço estabelecidos.
2. Realizar monitoramento contínuo e avaliações periódicas dos produtos e serviços de segurança do CONTRATANTE.
3. Adotar medidas proativas para prevenir e identificar incidentes de segurança antes que impactem os serviços.
4. Responder prontamente aos eventos de Segurança da Informação que possam comprometer a disponibilidade, integridade ou confidencialidade das informações.
5. Agir imediatamente em caso de falha nos controles de segurança ou situações que possam ameaçar os sistemas e serviços de TI.
6. Em caso de necessidade definida pelo CONTRATANTE o atendimento à resposta de incidentes deverá ser executado presencialmente nas instalações da CONTRATANTE pela CONTRADA.
7. Para a execução do atendimento presencial todos os custos atrelados como hospedagem, deslocamento e alimentação deverão ser arcados pela CONTRADA sem ônus para a CONTRATANTE.
8. Fornecer relatórios técnicos e gerenciais para evidenciar a execução dos serviços.
9. Exercer supervisão sobre a equipe na realização dos serviços de segurança da informação.
10. Elaborar planos de execução e treinamento para os profissionais envolvidos, além de orientar a equipe técnica em situações críticas.
11. Prestar atendimento em primeiro nível de solicitações, requisições e incidentes relacionados aos serviços de segurança;

12. Oferecer recomendações e colaborar na elaboração e atualização contínua, com o respaldo e concordância do CONTRATANTE, de procedimentos estruturados e do repositório de conhecimento, abrangendo todas as soluções para questões resolvidas com respostas padronizadas.
13. Receber as solicitações dos serviços referentes as soluções de segurança da informação contempladas nesse Termo de Referência e coordenar a realização e distribuição de recursos de trabalho.
14. Desenvolver e apresentar relatórios de atividades mensais (mês calendário), referente aos serviços gerenciados de segurança, provendo informações gerenciais ao CONTRATANTE
15. Propor novas tecnologias para atualizar o ambiente tecnológico, visando apoiar a equipe do CONTRATANTE na gestão da segurança da informação.

3.2.2. ACORDO DE NÍVEL DE SERVIÇO (ANS)

A prestação do serviço, objeto deste Termo de Referência, deverá estar disponível conforme os indicadores, níveis de prioridade e prazos detalhados abaixo.

NÍVEIS DE SERVIÇO

Tipo	Indicador	Nível de Serviço
Atendimento	Resolução de incidente dentro do prazo estipulado	95%
Atendimento	Atendimento de solicitação dentro do prazo estipulado	95%

NÍVEIS DE PRIORIDADE

Prioridade	Descrição
1. Emergencial	O serviço está inoperante ou há um impacto crítico nas operações para o negócio. ***O atendimento aos chamados com nível de prioridade Emergencial devem ser realizados obrigatoriamente de forma presencial (in loco) nas instalações físicas da CONTRATANTE***.
1. Alta	O serviço está comprometido ou aspectos significativos das operações foram negativamente afetados pelo desempenho insatisfatório

Média	O serviço está operacional, porém com problemas menores que não afetam diretamente as operações
Baixa	O desempenho operacional do serviço está comprometido, mas sem afetar sua funcionalidade ou operação
Planejada	Um incidente ou evento que não interrompe ou degrada os serviços ao cliente, mas requer ação planejada

PRAZOS DE ATENDIMENTO

Prioridade da solicitação	**Nível de Serviço (SLA) – Horas Corridas**
Emergencial	2 horas
Alta	6 horas
Média	12 horas
Baixa	48 horas
Planejada	60 horas

3.2.3. LOCAL DE EXECUÇÃO DO SERVIÇO

Os serviços acordados podem ser realizados à distância pela CONTRATADA, mas também podem ser executados in loco, mediante acordo entre as partes, nos casos em que o acesso remoto não seja viável ou quando a situação exija, cobrindo toda a infraestrutura de segurança e usuários da CONTRATANTE.

As atividades de implantação, descritas no item 1.6 da tabela presente no Objeto deste Termo de Referência, devem ser realizadas presencialmente (in loco) nas instalações físicas da CONTRATANTE.

Os serviços de Cibersegurança, descritos nos itens 1.7 da tabela presente no Objeto deste Termo de Referência, podem ser oferecidos a partir das instalações da CONTRADA ou de forma remota.

3.2.4. HORÁRIOS DE EXECUÇÃO DO SERVIÇO

Os Serviços de Cibersegurança para Firewall de Próxima Geração (NGFW), incluindo Plataforma SIEM, NOC e SOC, devem ser fornecidos remotamente em período integral, 24x7 (24 horas por 7 dias da semana), com a possibilidade de atendimento presencial nas instalações da CONTRATANTE em caso de incidentes graves de segurança que afetem a disponibilidade, integridade ou confidencialidade das informações.

3.3. REQUISITOS PARA A EXECUÇÃO DOS SERVIÇOS DE MONITORAMENTO CONTÍNUO E BACKUP (NOC - NETWORK OPERATIONS CENTER)

O serviço de monitoramento contínuo será prestado durante todo o período do contrato, abrangendo o monitoramento da disponibilidade de todos os appliances de firewall que compõem a solução;

Em casos de incidentes, a CONTRATADA deverá iniciar o procedimento de escalonamento previamente acordado com a CONTRATANTE em, no máximo, 15 (quinze) minutos, o que inclui, mas não se limita, a contatar a operadora de Internet responsável.

A CONTRATADA deverá disponibilizar acesso a um software web, protegida por login e senha, que permita a visualização em tempo real do desempenho e status dos equipamentos monitorados. Esta ferramenta deve possibilitar a personalização dos dashboards, de modo a apresentar as informações mais relevantes para a CONTRATANTE.

A CONTRATADA deverá emitir um relatório mensal detalhado contendo informações sobre:

1. Tempo de indisponibilidade de cada link.
2. Consumo de CPU e memória;
3. Conexões utilizadas e disponíveis;
4. Status da VPN e das interfaces;
5. Upload e Download dos links de Internet;
6. Número de série e versão do firmware dos equipamentos.
7. Uptime dos dispositivos.

A CONTRATADA deverá executar backups automáticos diariamente dos firewalls, garantindo que os dados estejam disponíveis para a CONTRATANTE em um servidor FTP seguro.

3.4. REQUISITOS PARA A EXECUÇÃO DO SERVIÇOS DE CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC - SECURITY OPERATION CENTER)

3.4.1. REQUISITOS GERAIS

O serviço de Centro de Operações de Segurança (Security Operation Center - SOC) deve ser prestado majoritariamente de forma remota.

O serviço deverá ser disponibilizado 24x7 (24 horas por 7 dias da semana), durante toda a vigência do contrato.

Além do serviço de SOC (Security Operation Center), a CONTRATADA deverá utilizar uma ferramenta de monitoramento que inclua uma console, podendo ser em nuvem. Esta ferramenta deve permitir o acesso a partir do ambiente da CONTRATANTE e possibilitar o controle do serviço de monitoramento da operação de segurança tanto do ambiente da CONTRATADA quanto da CONTRATANTE.

O SOC (Security Operation Center) deve atender aos seguintes requisitos mínimos:

1. Possuir um profissional dedicado à operação das soluções de detecção e resposta aos incidentes com ao menos uma certificação do fabricante do produto que será adotado, não sendo necessário a presença física no ambiente da CONTRATANTE.
2. Estar conectado aos Data Centers que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN, de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos.
3. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente.

3.4.2. REQUISITOS DO AMBIENTE DA FERRAMENTA DE SIEM

O ambiente da plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (Security Information and Event Management – SIEM), deve possuir as seguintes certificações: FedRAMP® Moderate Authorized, SOC2 Type 2, HIPAA, PCI DSS, ISO 27001

A comunicação entre o ambiente DATACENTER da CONTRATANTE e a ferramenta de SIEM deverá ocorrer somente via criptografia TLS

A solução deve:

1. Rodar em ambiente cloud listado no quadrante mágico do Gartner
2. Permitir acessos com MFA
3. Permitir segregação de acessos
4. Permitir opções de armazenamento customizável
5. Possuir registro de logs para fins de auditoria (definir prazo viável 90 dias)
6. Integrar com o Framework MITTRE ATT@CK
7. Possuir Machine learning em suas regras
8. Possuir Integração nativa com ferramenta de SOAR do mesmo fabricante

A solução deve operar de forma ininterrupta, 24x7 (24 horas por 7 dias da semana), garantindo monitoramento e resposta contínuos durante toda a vigência do contrato.

3.4.3. DETECÇÃO E RESPOSTA A INCIDENTES

3.4.3.1. Monitoração de Incidentes

Trata-se do monitoramento de aplicações web, servidores, virtualizadores e rede de forma proativa e reativa (com anuência do CONTRATANTE) no ambiente Internet e Intranet da instituição.

O ambiente a ser monitorado possui em seus ativos a quantidade de 1 GB de logs de dados brutos diários, incluindo servidores, roteadores, switchs, entre outros.

A ferramenta de SIEM deverá suportar a retenção dos logs coletados pelo período mínimo de 90 dias.

Nesse sentido, são papéis da CONTRATADA:

1. Monitorar o ambiente quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser gerenciada, bem como todo o escopo contratado quanto aos incidentes relacionados à segurança da informação;
2. Gerir os incidentes (criação de alertas, detecção e abertura de chamados);
3. Acompanhar do início ao fim os incidentes;
4. Realizar o acionamento por matriz de escalação hierárquica e funcional, para os incidentes;
5. Correlacionar o processo de eventos (gerenciar eventos durante todo o seu ciclo de vida) e o processo de incidentes de forma automatizada entre as ferramentas de ITSM e monitoramento;
6. Acompanhar os processos através de indicadores de desempenho.

3.4.3.2. Detecção e resposta

A CONTRATADA deve elaborar um Plano de Resposta aos Incidentes mais comuns. Tal plano deve conter, minimamente:

1. Tipo de incidente;
2. Ações a serem realizadas;
3. Responsáveis pela execução das ações, incluindo nome, telefone e e-mail.

O correlacionamento de logs deve ser realizado por meio de uma ferramenta apropriada de Gerenciamento e Correlação de Eventos de Segurança da Informação (Security Information and Event Management – SIEM) fornecida pela CONTRATADA. Esta solução de SIEM deve atender a critérios específicos de reconhecimento no mercado, estando listada no Quadrante Mágico do Gartner por, no mínimo, 2 (dois) anos, bem como figurar na listagem de produtos de SIEM do Quadrante da Forrester.

A detecção de atividades maliciosas em rede deve ser realizada por meio da coleta de syslogs e flow dos dispositivos de rede, tais como: Switches, NGFW, controladoras Wi-Fi, NAC, roteadores.

A CONTRATADA deverá reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE.

A CONTRATADA deve prover o controle de ações, notificações e escalonamento dos incidentes, bem como a articulação com as equipes da CONTRATANTE, atuando em conjunto com o time de especialistas da CONTRATANTE para a elaboração da proposta de contenção, erradicação e recuperação.

Em caso de ataque, devem ser elaborados alertas e estratégias de prevenção para todos os ambientes da CONTRATANTE.

A CONTRATADA deve criar, revisar e manter artigos de conhecimento (playbooks) de segurança com objetivo de simplificar e dar agilidade ao processo de resposta a incidentes.

Os referidos artigos de conhecimento devem ser transferidos para o CONTRATANTE. (Excluída qualquer transferência de propriedade intelectual)

A CONTRATADA deve ofertar um treinamento para as equipes de TI da CONTRATANTE, com duração mínima de 4 (quatro) horas. O conteúdo do treinamento deve abranger a operação da ferramenta de SIEM, incluindo instruções sobre como gerar relatórios e realizar pesquisas no sistema.

3.4.3.3. Relatórios e análise de causa raiz

Para cada incidente identificado deverá ser elaborado e entregue um relatório detalhando minimamente:

1. Os impactos observados;
2. Criticidade;
3. Componentes relacionados;
4. A(s) vulnerabilidade(s) explorada(s);
5. A origem do ataque;
6. O destino do ataque;
7. Descrição do evento.

4. ESTIMATIVAS DAS QUANTIDADES

Os quantitativos são indicados na Planilha de Pesquisa de Preços, anexa a este documento.

5. LEVANTAMENTO DE MERCADO

Após estudos e pesquisas de mercado, chegou-se a conclusão que a contratação descrita nesse Estudo Técnico é a solução que demonstra o resultado financeiro pretendido com ênfase na economicidade.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O valor da licitação será de aproximadamente R$ 949.068,89 para 36 meses, conforme pesquisa de mercado.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A presente contratação visa implementar uma solução abrangente de segurança cibernética para o Município de Bento Gonçalves, que compreende a aquisição e renovação de licenças de software de segurança cibernética, incluindo Next-Generation Firewall (NGFW), implementação de plataforma de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM) em modalidade SaaS, substituição dos equipamentos de hardware existentes, contratação de serviços especializados de suporte e implantação, e realização de treinamento especializado para a equipe técnica.

Para materializar esta estratégia de segurança cibernética, através da presente licitação, pretende-se alcançar os seguintes resultados:

1. Padronização da infraestrutura tecnológica do Município de Bento Gonçalves;
2. Manutenção da alta disponibilidade dos serviços de TI prestados pelo Município de Bento Gonçalves, bem como redução de riscos ocasionados pela interrupção destes serviços;
3. Reestabelecimento das atualizações de software necessárias ao correto funcionamento dos sistemas de segurança utilizados nos servidores de rede do Município de Bento Gonçalves;
4. Manter e ampliar o nível de proteção da rede, através da solução de Next-Generation Firewall (NGFW) e plataforma SIEM;
5. Aumentar a segurança dos sistemas informatizados, proporcionando eficiência às atividades administrativas, gerenciais e de suporte dos órgãos partícipes;
6. Garantir a continuidade dos serviços públicos essenciais ao cidadão, como atendimentos da saúde, segurança pública e educação.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

A adjudicação do objeto será realizada pelo critério de menor valor global, considerando todos os itens listados na tabela do objeto deste Termo de Referência.

Esta decisão se justifica pelos seguintes motivos:

1. **Integração das soluções**: As soluções de Firewall de Próxima Geração (NGFW) e Proteção de Endpoints (Antivírus) são complementares e fazem parte de uma estratégia unificada de Cibersegurança para o Município de Bento Gonçalves. A contratação de um único fornecedor para ambas as soluções garante uma melhor integração e eficácia na proteção do ambiente tecnológico.
2. **Continuidade e consistência dos serviços**: A empresa que fornecer os equipamentos e licenças (itens 1.1 a 1.5) será também responsável pelos serviços de

implantação (item 1.6), pelos serviços contínuos de Cibersegurança (item 1.7) e pelos serviços de Treinamento (item 1.8). Isso assegura uma abordagem coesa e consistente na implementação e manutenção das soluções.

3. **Otimização de recursos**: A contratação global permite uma melhor negociação de preços e condições, potencialmente resultando em economia para a Administração.
4. **Simplificação da gestão contratual**: Um único contrato para todos os itens simplifica os processos de gestão, fiscalização e acompanhamento por parte da Administração.
5. **Garantia de compatibilidade**: A adjudicação global assegura que todos os componentes da solução sejam plenamente compatíveis entre si, reduzindo riscos de incompatibilidades ou conflitos entre diferentes fornecedores.
6. **Responsabilidade unificada**: Um único fornecedor será responsável por todos os aspectos da solução, desde a entrega dos equipamentos até a prestação dos serviços continuados, facilitando a resolução de problemas e o cumprimento dos níveis de serviço estabelecidos.

Esta abordagem de adjudicação global está alinhada com os objetivos de padronização da infraestrutura tecnológica, manutenção da alta disponibilidade dos serviços de TI e garantia da continuidade dos serviços públicos essenciais ao cidadão, conforme estabelecido nos objetivos deste Termo de Referência.

9. DEMONSTRATIVO DOS RESULTADOS

Após estudos e pesquisas de mercado, chegou-se a conclusão que a contratação descrita nesse Estudo Técnico é a solução que demonstra o resultado financeiro pretendido com ênfase na economicidade.

10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

a) A fiscalização do contrato será exercida por representantes da Coordenadoria de Tecnologia de Informação e Comunicação - CTEC.

b) Não obstante a(s) CONTRATADA(s) seja(m) a(s) única(s) e exclusiva(s) e responsável (veis) pela execução de todos os serviços, à CONTRATANTE é reservado o direito de sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, diretamente ou por prepostos designados.

c) A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por quaisquer irregularidades e na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos.

d) Quaisquer exigências da fiscalização inerentes ao objeto do presente Termo de Referência deverão ser prontamente atendidas pela CONTRATADA, sem ônus para a CONTRATANTE.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

A CTEC será responsável pela fiscalização do Contrato, entretanto a prestação de serviço se dará unicamente pela empresa vencedora do certame.

12. DESCRIÇÃO DE IMPACTOS AMBIENTAIS E MEDIDAS MITIGADORAS

Não haverá impactos ambientais.

13. POSICIONAMENTO CONCLUSIVO DA CONTRATAÇÃO

A CTEC posiciona-se favorável a referida contratação.

14. JUSTIFICATIVA PELO NÃO-PREENCHIMENTO DOS ITENS NÃO OBRIGATÓRIOS

Foram preenchidos todos os campos.

Bento Gonçalves, 31 de janeiro de 2025.

- assinado eletronicamente -
Nataniel Breda Dendena
Diretor