O FUNDO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE SUMARÉ, em conformidade com o artigo 75, §3º da Lei Federal nº 14.133/2021, Nova Lei de Licitações e Contratos Administrativos e artigo 9º, do Decreto Municipal 12.066/23, torna público que este Fundo de Previdência realiza processo de DISPENSA DE LICITAÇÃO para:

Objeto: Sistema de cyber segurança

Regime de Execução: Indireta – Serviços cybersegurança

Tipo de Licitação: Dispensa de licitação – menor preço global

Eventuais Interessados podem apresentar propostas de preço no prazo de 03 (três) dias úteis, oportunidade em que o SUMPREV escolherá a mais vantajosa.

As propostas deverão ser encaminhadas ao Fundo de Previdência Social do Município de Sumaré até 16 de dezembro de 2025, até as 17h00 horas, através do e-mail compras.sumprev@sumare.sp.gov.br, conforme modelo de proposta anexo ao termo de referência.

Sumaré, 10 de dezembro de 2025.

Larissa Coelho de Morais Monção
Superintendente Previdenciária

Processo Administrativo nº 24.019/2025

Fundamentação da necessidade da contratação – art. 6º, XXIII, "b" da Lei 14.133/21 e Artigo 75, inciso II, e art. 72, ambos da lei 14.133/21.
Decreto Municipal nº 12.066/23

A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada neste Termo de Referência.

Termo de Referência – Contratação Direta

Do Objeto

Constitui objeto do presente contrato a aquisição de soluções, serviços de controle, proteção e segurança integrada dos produtos descritos abaixo.

Da Justificativa

Considerando o momento crítico que vivemos no quesito de segurança da informação, é necessário ressaltar a importância que as atividades desempenhadas seja como serviço de natureza contínua. Somente assim é possível auxiliar nas medidas de prevenção e combate a ataques cibernéticos, vírus, falhas de segurança, tentativas de invasão, roubo de dados, perda de dados e interrupções nas atividades operacionais e administrativas nas diversas instâncias dos órgãos municipais e estaduais.

A contratação é imprescindível à Administração para o desempenho de suas atribuições, onde a interrupção de qualquer um dos itens pode comprometer a continuidade das atividades da Administração Pública e cuja necessidade de contratação deve se estender por mais de um exercício financeiro, tendo vigência de 24 (vinte e quatro) meses. Tendo em vista que toda a infraestrutura de computadores, funciona de forma totalmente integrada, faz-se necessária a contratação de uma empresa que comercialize softwares de cibersegurança, de forma integrada e que ainda, o suporte a todas as soluções seja diretamente com o fabricante das soluções em regime irrestrito. E que possa garantir a prestação dos serviços previstos neste documento de forma a garantir um monitoramento e gerenciamento adequados de todo o ambiente sem prejuízo para os usuários.

As boas práticas de segurança da informação sempre relacionam que o investimento necessário seja proporcional ao risco e impacto de uma ocorrência danosa ao processo em questão.

Analisando o risco e o impacto, percebemos um cenário com uma probabilidade cada vez maior de ocorrência, dado o aumento vertiginoso da quantidade de ameaças a cada momento. Nestes últimos anos, vivenciamos situações altamente perigosas com até mesmo instituições, até então altamente protegidas com altos investimentos em segurança da informação, tiveram seus dados comprometidos e muitas vezes tornando-os públicos, o que infringe em muitos casos a LGPD (Lei Geral de Proteção de Dados - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018), em vigor desde 2018.

É de conhecimento de todos que o ataque mais popular atualmente é referente ao sequestro de informação, na imensa maioria das vezes sendo comprometido por meio de um malware denominado “ransomware”. Por ransomware, entende-se que é um tipo de malware que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate, em dinheiro ou criptomoedas para que o acesso possa ser restabelecido. Desde que se vivenciou um grande aumento de infecção por ransomware, foi natural o aumento do uso de sistemas de backup como uma alternativa para minimizar os danos, para que caso tenha os dados comprometidos, possa restaurar de maneira rápida reduzindo

chance de prejuízo. Porém, como podemos observar diante as informações publicadas na mídia, a tática adotada pelos criminosos tem sido que além do “sequestro de dados”, ameaçar com a divulgação de dados na mídia, acarretando pesadas consequências para a instituição que sofreu o ataque. Isso faz com que o backup não seja a única ação necessária para minimizar os dados de um ataque de ransomware, sendo necessário também proteção completa.

As ameaças não se limitam apenas ao ransomware, poderíamos listar pelo menos milhares de ameaças a mais que vão desde ataque direto para explorar alguma falha e vulnerabilidade com intuito de invasão direta aos servidores, desktops assim como também negação de serviço entre os mais explorados. Agora recentemente vivenciamos também uma indisponibilidade de serviços em várias intituições e empresas ao redor do mundo devido à uma atualização incorreta do sistema operacional Windows, ressaltando ainda mais a importância de ter processos e procedimentos reconhecidos e testados, tais como ISO 27001, NIST, entre outras, sempre visando alta disponibilidade e redução de riscos.

Muitos dos ataques são com objetivos financeiros, como tem ocorrido em diversos órgãos governamentais conforme reportagens a seguir:

Prefeitura de Barroso
https://www.barbacenamais.com.br/policia-mais/62-policia-militar/20138-conta-bancaria-da-prefeitura-de-barroso-e-invadida-por-hacker

Prefeitura de Taboão da Serra
https://g1.globo.com/sp/sao-paulo/noticia/2021/09/17/piratas-digitais-invadem-sistema-da-prefeitura-de-taboao-da-serra-na-grande-sp-e-deixam-populacao-sem-servicos-publicos.ghtml

Prefeitura de Candiota
https://g1.globo.com/rs/rio-grande-do-sul/noticia/2020/10/15/hackers-invadem-sistemas-da-prefeitura-de-candiota-e-prejudicam-funcionamento-de-servicos.ghtml

Prefeitura de Brumadinho
https://hojeemdia.com.br/minas/site-da-prefeitura-de-brumadinho-e-invadido-e-hackers-publicam-video-atacando-a-mineradora-vale-1.868906

Como pode-se verificar, os prejuízos somados chegam em altíssimas cifras de centenas de milhões de prejuízo.

O problema tornase ainda mais grave, quando o alvo são instituições consideradas críticas para população, assim como ocorreu com a invasão à usina de água no estado da florida nos Estados Unidos em que um hacker tentou manipular as misturas quimicas na água, podendo causar um grande desastre para a população.
https://g1.globo.com/economia/tecnologia/noticia/2021/02/08/hacker-tentou-contaminar-agua-com-aditivo-quimico-em-cidade-da-florida.ghtml

Segundo a CNN Brasil, somente no primeiro mês deste ano, já temos mais de 20 instituições públicas que sofreram ataques cibernéticos.

Infelizmente a tendência é que tais atos, sejam cada vez mais frequente. Recentemente o fórum econômico mundial (https://www.weforum.org/), em seu evento anual, classificou problemas de Cibersegurança entre as maiores ameaças mundiais nos próximos anos, apelidado pelo seu presidente

(Klaus Swab) como “Ciber pandemia”, reforçando ainda mais o grau de atenção à segurança da informação nos momentos atuais.

Dado estas informações listas, podemos considerar o risco como alto, justificando a abrangência de soluções conforme descrito neste termo.

Da Especificação Técnica

O fabricante do produto deverá ser uma empresa atuante na área de segurança da informação a fim de garantir eficácia das soluções de proteção, e possuir modelo de boas práticas baseado em padrões de mercado.

Quaisquer soluções que sejam escolhidas, deverão possuir em um único painel em nuvem que agregue em grande parte o gerenciamento e monitoramento das soluções listadas. As funções de gerenciamento e monitoramento que deverão ter no painel em nuvem estão listadas neste documento.

As soluções deverão ser entregues por um único fornecedor precisará deter a capacidade de fazer ajustes/correções, mesmo que no código fonte do sistema em nuvem, caso necessário.

A proponente deverá garantir que ao longo do presente contrato, nenhum produto, software, hardware ou peças necessárias, estejam em uma versão considerada não oficial, não comercializada, “end-of-life, end-of-sale ou end-of-support”. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte e vida. Devendo estar em linha de produção do fabricante, sempre em sua versão mais atualizada (seja software, sistema e hardware, caso o fabricante lance uma nova versão etc.) A proponente deverá garantir que estão cobertos por garantia ao longo do contrato pela proponente.

Todas as funcionalidades descritas, deverão ser comprovadas por meio de documento oficial do fabricante, a fim de garantir que as funcionalidades de grande importância para proteção estejam contempladas.

Apresentar carta emitida pelo próprio Fabricante, dirigida ao CONTRATANTE, referenciando ao edital em epígrafe, informando que a Proponente é revenda autorizada a comercializar seus produtos e serviços, e o Fabricante confirma que atende a todos os itens listados no referente edital.

Será feita a verificação da compatibilidade dos recursos e das capacidades, facilidades operacionais informadas na proposta para cada item ofertado com base nas informações dos catálogos, folhetos, manuais técnicos e semelhantes produzidos pelo fabricante. Documentos estes que deverão ser anexados a proposta comercial, referenciar o endereço web para consultas e diligências de todo material apresentado. Salienta-se que não serão aceitos materiais produzidos pela Proponente a não ser que ela seja fabricante.

Apresentar no mínimo 1 técnico certificado nas soluções contratadas. Este deverá ser comprovado através de documento emitido pelo fabricante da solução ou empresa devidamente autorizada para emissão de certificados, no caso de a certificação não ser realizada pelo fabricante da solução, deverá apresentar comprovação que a empresa fornecedora da certificação é devidamente credenciada para emitir tal documentação.

Apresentar no mínimo 1 técnico certificado com cursos voltados para segurança da informação, oferecidos por empresas cujo foco seja segurança da informação.

Apresentar no mínimo 1 técnico que possua atestado de capacidade técnica que já tenha executado projetos nas soluções mencionadas na proposta. O atestado deverá ser assinado pela empresa contratante ou pelo fabricante da solução.

A proponente deverá disponibilizar serviços de treinamento especializado em segurança da informação oficiais do fabricante da solução, com certificado do fabricante, de forma a atender aos seguintes requisitos: carga horária mínima de 06 horas, até 20 participantes na turma.

A proponente deverá efetuar visita técnica presencial antes da apresentação da proposta para verificar requisitos físicos a serem providos para a correta instalação e prestação de serviços.
As visitas somente poderão ocorrer de segunda a sexta, das 10hs às 12hs ou 14hs as 16hs.

Dos Produtos e Serviços

Descrição	Valor/mês
Solução de segurança de rede e controle e segurança de dispositivos	9.567,60
Implantação da UTM e Ativação do Recurso	3.000,00
Total	12.567,60

ITEM 01 – SOLUÇÃO DE SEGURANÇA DE REDE

A solução deverá possuir em um único painel em nuvem que agregue em grande parte o gerenciamento e monitoramento das soluções listadas. As funções de gerenciamento e monitoramento que deverão ter no painel em nuvem estão listadas neste documento.

A proponente deverá garantir que ao longo do presente contrato, nenhum produto, software, hardware ou peças necessárias, estejam em uma versão considerada não oficial, não comercializada, “end-of-life, end-of-sale ou end-of-support”. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte e vida. Devendo estar em linha de produção do fabricante, sempre em sua versão mais atualizada (seja software, sistema e hardware, caso o fabricante lance uma nova versão etc.) A proponente deverá garantir que estão cobertos por garantia ao longo do contrato pela proponente.

Sempre que o fabricante lançar uma versão nova, seja do hardware (appliance) ou do software, o mesmo ficará responsável por notificar o cliente e atualizar os mesmos.

A solução de segurança de redes, também chamado de Firewall UTM ou Firewall NGFW, deverá permitir acesso as informações do produto, em idioma Português (Brasil), não somente através de um acesso direto ao equipamento e ao seu painel, como também acesso à um servidor em Cloud (nuvem). Permitindo assim ser acessado de qualquer lugar, sem restrições de origem, através de login e senha com possibilidade de possuir dupla autenticação a fim de aumentar o nível de segurança de acesso.

O painel em Cloud (nuvem), permitirá visualizar informações essenciais dos produtos em tempo real, a fim de monitoramento, tais como:

- Informações do hardware: Processamento, memória, disco;
- Informações de qualidade do link: Disponibilidade, latência e perda de pacotes.

O servidor em nuvem, deverá efetuar backup das configurações dos produtos, no mínimo diariamente, dos últimos 5 dias, a fim de aumentar a segurança em caso de algum incidente que afete as configurações ou o hardware.

O servidor em nuvem, deverá avaliar o nível de risco do produto, no que se refere as melhores práticas de configuração de segurança de redes, sendo analisado pelo menos as regras de firewall, regras de NAT, qualidade da senha de acesso, configurações de VPN, entre outros. Tal análise tem que ser no mínimo diária.

Deverá possuir aprendizado de máquina (Machine Learning) trabalhando na prevenção de ataques em todas as camadas segundo o modelo OSI, referenciando arquivos.

Estabelecer comunicação contínua com mecanismos em nuvem para receber atualizações de informações de maneira contínua, visando aperfeiçoamento e reciclagem de conteúdo.

Possuir recurso para recomendação de boas práticas relacionadas a controle, gestão e segurança através de alertas, gráficos e análise de risco. Existir ainda a possibilidade de configurar as recomendações para reduzir as chances de falhas humanas, automatizando alertas.

Em caso de impossibilidade de configuração via interface gráfica, devido à algum incidente, a solução deverá permitir também o acesso via console de linha de comando, podendo ser acessível através de protocolo de acesso remoto. Tal como: SSH ou conexão direta via cabo console. As configurações mínimas permitidas por meio de linha de comando deverá ser:

- Configuração de interface de rede, configuração de senha de acesso à WEB, “resetar” equipamento para a configuração “padrão de fábrica”, reiniciar o sistema, parar o sistema, acesso ao sistema operacional, lista das atividades do firewall, visualizar filtro do firewall, reiniciar o serviço de acesso à WEB, acessar o sistema operacional como “desenvolver”, à fim de reparação de algum bug. Atualização do sistema, habilitar acesso via SSH, efetuar download de módulos, pacotes ou atualizações, logout e ping.

Com objetivo de ter uma instalação fácil, prática e rápida. A solução deverá permitir a utilização de um auxiliador de configuração (wizard) nos casos de primeira instalação do sistema.

A solução deverá suportar uso de VLANs 802.1Q.

A solução deverá suportar regras de Firewall tradicionais, permitindo filtrar por: origem e IP de destino, porta de origem do protocolo, e destino IP para o tráfego TCP e UDP, com limite de conexões simultâneas por regra, com possibilidade de alteração do gateway para cada regra, podendo fazer balanceamento de carga ou failover por regra. As regras de Firewall devem permitir também gestão da tabela de estado das conexões.

A solução deverá permitir efetuar regras de Firewall por Objetos. Por objetos considerasse um IP, Porta, URL, sub-redes, entre outros.

A solução deverá fazer bloqueios na camada de aplicação (considerando camada 7 no modelo de camadas OSI de comunicação), também chamado de Firewall por aplicação permitindo assim:
Reconhecer aplicações independente de porta e protocolo, tendo a capacidade de bloquear e liberar aplicações diretamente através de configuração por meio da interface gráfica com poucos cliques, podendo configurar regras por grupo e usuário.

Efetuar regras por usuário ou grupo através de integração com Microsoft Active Directory ou base local.
A solução deverá reconhecer pelo menos aplicações nas seguintes categorias: redes sociais, ameaças, pornografia, antivírus, portais.

A solução deve mostrar por meio de um painel o percentual do tráfego de cada rede social, tais como: facebook, twitter, instagram, whatsapp, linkedin, youtube e as

aplicações que estão sendo utilizadas no momento, com informações sobre a aplicação, data e hora, nome de usuário que está originando o tráfego e se o tráfego está liberado ou bloqueado.

A solução deverá prover relatório de acesso do uso das aplicações.

A solução deverá possuir proteção contra tráfego malicioso, ataques, independente de porta e protocolo, ou seja, proteção na camada 7 (camada de aplicação segundo modelo OSI), permitindo visualizar em um dashboard de maneira gráfica e georreferenciada de acordo com a origem dos ataques.

A proteção na camada 7 contra tráfego malicioso, deverá garantir bloqueio de no mínimo worms, trojans, malwares, além de protocolos de uso não recomendados como: UltraSurf, UltraVPN, CyberGhost, Express VPN etc.

Deverá ainda ter proteção em tempo real de forma distinta da proteção na camada de aplicação.

Uma vez que seja uma ferramenta de proteção de borda nativamente na interface WAN, deverá englobar todas as ferramentas de proteção como antivírus, antiphishing, antispyware, antiransomware e IDS/IPS.

Deve possuir dashboard exclusivo com gráficos de informações dos principais países de origem das tentativas de invasões.

Ter recurso para exibir um resumo das tentativas de invasão, infecções identificadas e nível de risco de cada uma delas.

Deverá possuir proteção integrada de IPs com assinaturas mantidas também pelo fabricante.

Deverá ter disponível uma ferramenta responsável por identificar e bloquear aplicações ou serviços independente de uso de um Proxy nos dispositivos. Com capacidade de bloquear até mesmo tráfego de dispositivos móveis.

Oferecer opção de separação de gráficos e as porcentagens de acesso por rede/interface.
Exibir consumo por aplicações e detalhes de pelo menos as 5 principais aplicações que mais consomem banda da internet.

As informações de navegação devem ser em tempo real, com a possibilidade de separar interface/rede.

Deverá ter gráfico com porcentagem de navegação separado por categoria.

Deverá possuir a seleção total ou parcial de bloqueios ou liberações de aplicativos ou websites.

A solução deve possuir a possibilidade de uso de regras separadas por redes (book de regras), e ainda ser possível configurar políticas de navegação distintas entre as redes.

Deve ainda possuir um modo simplificado de uso do recurso agindo na camada de aplicação, para uso em equipamentos com hardware com carga alta de consumo.

Deve possuir recurso de limpeza de log e data base de log de navegação, com recurso de limpeza automática, com possibilidade de personalização e alterações de configurações.

A solução deverá permitir efetuar bloqueio de conexões recebidas por determinado país ou continente, tendo como uma das funcionalidades, permitir visualizar países ou continentes líderes no ranking de tráfego malicioso e assim fazer bloqueios de entrada e saída.

A solução deverá permitir regras de redirecionamento de portas, atuando como um recurso para informar ao equipamento qual o destino a ser dado aos pacotes.

A solução deverá permitir regras de NAT (Network Address Translator), entre os hosts da rede interna e a internet, traduzindo os IPs com as seguintes características: Encaminhamento de portas, incluindo faixas de rede e o uso de múltiplos IPs públicos, NAT para IPs individuais ou sub-redes inteiras, NAT de saída, NAT de saída avançado, permitindo que seu comportamento padrão seja desativado e permitindo a criação de múltiplas flexões de regras de NAT, NAT Reflection, possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.

A solução deverá fazer proxy do protocolo IGMP entre segmentos de rede, bem como interface de upstream e downstream.

A solução deverá, através de funcionalidade, permitir suporte ao protocolo Universal Plug and Play (UPnP) e NAT Port Mapping Protocol (NAT-PMP), podendo configurar download e upload máximo caso necessário.

A solução deverá ter um endpoint integrado e gerenciado na mesma plataforma em nuvem, que deverá possuir suporte para ser configurado o serviço de Wake on LAN, através de suporte no hardware, com objetivo de ligar o computador através de um pacote específico de rede.

A solução deverá possuir suporte para atualização automática da base de seu sistema, sempre que existir alguma disponível.

A solução deverá permitir criação de tabela de horários para agendamento de regras, bem como vincular uma regra a uma agenda definida para que elas vigorem a partir de ou durante datas e horários previamente especificados.

A solução deverá fornecer recursos de gerência de tráfego de rede, sendo possível a criação de regras dos seguintes tipos: Priorização de tráfego, definindo quais protocolos possui prioridade, Limite de tráfego por protocolo, definindo qual limite

máximo de um protocolo, reserva de tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.

Permitir que o DHCP Relay encaminhe requisições para um servidor definido em outro segmento de rede.

A solução deverá dispor de servidor DHCP, que permita atribuir endereços IPs e configurações relacionadas aos dispositivos da rede, por meio de MACAddress.

A solução deverá permitir uso de DNS dinâmico para que seja registrado o endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usados para conectar-se à VPNs, Web Servers e também Mail Servers. Podendo ser usado conta em serviço de terceiros no mínimo as seguintes opções: DynDNS, No-IP, OpenDNS, ZoneEdit e DyNS.

A solução deverá permitir gravar logs separando por pelo menos as seguintes categorias: Firewall, DHCP, Autenticação, IPSec, PPP, VPN, Load Balance, OpenVPN, NTP.

A solução deverá permitir gravar logs em servidor externo podendo configurar até 3 servidores.

O sistema deverá permitir envio de informações pré-programadas referente ao status do link, permitindo selecionar o gráfico a ser enviado, bem como enviar e-mail informando quando houver queda de link.

O sistema deverá permitir gerenciar certificados através de modo gráfico, e criar e/ou revogar novos certificados através do painel web.

O sistema deverá permitir efetuar controle de permissão para acesso às funcionalidades da solução.

A solução deverá permitir load balancing e/ou failover no tráfego de saída para Internet, permitindo configurar de acordo com a qualidade do link ou queda do mesmo.

Possibilidade de sincronização de horário do equipamento utilizando protocolo NTP.

A solução deverá possuir suporte, através de um serviço do sistema operacional para OLSR (Optimized Link State Routing Protocol).

A solução deverá permitir utilização do protocolo Netflow versão 1, 5 ou 9 para envio de informações referente à tráfego/link, permitindo configurar no mínimo: IP de destino, porta, IP de origem e restrição de direção.

A solução deverá permitir configurar roteamento dinâmico, tal como: RIP versão 1 e 2, OSPF padrão RFC 1583 ou BGP.

A solução deverá suportar utilizar protocolo SNMP.

A solução deverá possuir no mínimo os seguintes gráficos: memória, throughput, links, VPN, qualidade dos links, processamento.

A solução deverá permitir configurar um servidor PPPoE Server no equipamento, podendo ter autenticação por: base local, RADIUS, ou acessar um servidor PPPoE para ativar algum link.

A solução deverá permitir no mínimo as seguintes opções de VPN (Site-to-Site ou Client-to-Site): IPSec, OpenVPN e o L2TP, podendo a solução ser o server ou o client e permitindo uso de VPN com outros equipamentos de outros fornecedores, sem limite de licenças.

A solução deverá permitir uso de um cliente OpenVPN do fabricante, com opção de autenticação em base AD (Active Directory) ou LDAP, podendo ser instalado em estações de trabalho Windows, MAC OS X, ou dispositivos móveis como IOS (IPhone/IPad), Android.

Deverá possuir a funcionalidade de enviar e-mail sempre que: algum usuário se conectar ou desconectar no túnel VPN. A solução deverá ainda gravar logs das conexões de VPN, permitindo visualizar relatórios.

Todos os equipamentos deverão suportar funcionamento em modo Cluster e todas licenças para seu uso deverão estar inclusas no fornecimento, permitindo a configuração de dois firewalls como um grupo de “failover”, se uma interface falhar no primário ou ficar “off-line” completamente, o secundário se torna ativo, sem qualquer prejuízo de parada, lentidão ou interrupções de atividade de operação, tendo o secundário mesma capacidade que o primário (quantidade de usuários, conexões simultâneas, troughput, etc.) especificadas no dimensionamento.

A solução deverá permitir também efetuar backup em servidor em nuvem (cloud) de maneira automática das configurações e deverá estar incluso no contrato o serviço em nuvem para manter ao menos 5 copias das configurações do equipamento.

A solução deverá possuir módulo de liberação e bloqueio de maneira fácil e rápida e atualizados diariamente comuns para liberação ou bloqueio em uma rede considerada comum, tais como: Windows Update, Java, Caixa/Conectividade Social, Bancos, Microsoft, Governo, Acesso remoto, Redes sociais.

A solução deverá permitir gerenciamento de visitantes para acesso à redes para visitantes, com possibilidade de autenticação para usuários, por meio de cadastro, facebook, AD / LDAP, RADIUS.

A solução deverá permitir bloqueio de acesso à sites, por meio de categoria (atualizado diariamente com no mínimo 48 categorias), com regras que permita a escolha de trabalhar com proxy transparente ou autenticado. No caso de autenticação, os usuários poderão se autenticar através de: base local, LDAP, Active Directory (AD), RADIUS, NTdomain e Single-Sign-on.

A solução deverá permitir a criação de categorias personalizadas sem limite de quantidades, bem como permitir criação de lista brancas/negras como exceções. A solução deverá também scanear arquivos que forem efetuados download para verificar de vírus/malwares (todas licenças inclusas).

A solução deverá ter módulo de diagnóstico de bloqueio ou liberação de URL por usuário, mostrando qual regra está permitindo ou bloqueando o acesso a fim de diagnóstico rápido de ajuste da regra. A solução deverá também permitir o usuário justificar o acesso à uma URL bloqueado, podendo assim acessar mediante somente a justificativa ou mediante aprovação após a justificativa por parte de usuário com acesso administrativo.

A solução deverá compor suíte de relatórios no mesmo equipamento ou em caso de necessidade de uso de outro equipamento ou software o fornecedor deverá incluir todas os valores e licenças bem como equipamentos para atender ao quesito “relatórios de gerenciamento”

A suíte de relatório deverá permitir a personalização da marca estampada no cabeçalho do relatório, e possuir ao menos as seguintes informações de acesso: usuários, consumo de link, acessos por IP, acessos por usuário, acesso por categoria, acesso por meio de VPN.

A solução deverá permitir visualizar estrutura de rede conectada entre unidades por meio do painel em Cloud, permitindo visualizar problemas de rotas de conexão entre unidades, e permitir fazer failover sobre conexões de VPN de maneira automática sem intervenção manual.

A solução deverá fornecer sistema de detecção e prevenção de intrusão com capacidade de inspecionar o “payload” do pacote, fazendo o registro dos pacotes, além de detectar as invasões. Capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades, além de permitir a configuração de avisos ao administrador do ambiente sobre o ataque.

A solução deverá ser fornecida em appliance, ou seja, integração do hardware com software do mesmo integrador. Não serão aceitos equipamentos de uso genérico.

Caso o fabricante tenha um novo modelo durante o período do contrato, a CONTRATADA deverá efetuar a substituição pelo modelo mais novo sem ônus adicional ao Fundo de Previdência Social do Município de Sumaré – SUMPREV..

Não serão aceitos modelos do tipo SOHO ou quaisquer appliances preparados para modelos do tipo “Home office”.

No caso de módulos opcionais, caso o equipamento não permita a substituição, deverá ser contemplado o equipamento considerando o opcional como permanente.

Enquanto o contrato estiver vigente, quaisquer anomalia identificada deverá ser substituído por um hardware em perfeitas condições com capacidade igual ou maior

O suporte deverá ser disponibilizado via e-mail, telefone ou chat direto com especialistas do fabricante das soluções, sem intermédio de distribuidores e sem automação (robô), sem limite de chamados e tempo.

Em caso de necessidade de substituição, seja por mal funcionamento de hardware ou software, o suporte deverá prover um equipamento reserva com SLA de no máximo 4hrs úteis disponível para envio do local da CONTRATADA ou outro local no Brasil ou retirada pelo Fundo de Previdência Social do Município de Sumaré – SUMPREV..

Todas as atualizações de hardware ou de software das soluções são por conta do fabricante.

Caso seja necessário mediante chamado técnico, o fabricante deve intervir remotamente, podendo acessar o equipamento remotamente sem restrições de configuração, para prestar o suporte ao Fundo de Previdência Social do Município de Sumaré – SUMPREV.

O suporte deverá manter um backup em nuvem atualizado, no caso de locação de Firewall UTM NGFW, com todas as configurações do equipamento para uso posterior.

A solução em nuvem deverá prover modulo de monitoramento no mesmo painel de gerenciamento com objetivo de facilitar a operação.

O módulo deverá prover painel próprio de monitoramento na plataforma web com atualização em tempo real do alerta bem como prover App para ser instalado em dispositivos móveis da família Android.e IOS

Permitir monitorar as interfaces da solução;

Permitir monitorar links, gerando alertas e caso de perda de pacotes, latência ou queda de link

A solução deverá permitir o monitoramento dos serviços de filtro de conteúdo web entre outros.

O hardware deverá ter a capacidade mínima de 50 (cinquenta) dispositivos e possuir no mínimo as seguintes configurações:

Especificações mínimas dos equipamentos:

2.128. O hardware deverá ter a capacidade mínima de 50 (cinquenta) dispositivos e possuir no mínimo as seguintes configurações:
2.129. Especificações mínimas dos equipamentos.

2.130. Item 02 - firewall Tipo 02:

- Memória mínima: 4Gb
- Interfaces de rede mínimo: 4 interfaces (Gbs)
    - Interfaces Bypass mínimo: 2

- Processador:
  - Número de núcleos: 2
  - Nº de threads 2
  - Frequência mínima em processador: 1.50 GHz
- Conector console RJ45
- Conector HDMI/VGA
- Porta USB 2
- Fonte de Alimentação Full Range.
- Disco 120GB SSD
- Quantidade dispositivos simultâneos: 50
- Thoughtput mínimo de Firewall: 3.9GB

ITEM 02 – SOLUÇÃO DE CONTROLE E SEGURANÇA DE DISPOSITIVOS

A solução deverá funcionar tanto de forma integrada, quanto de forma isolada (“stand alone”);

Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa, denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);

Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;

A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aquelas relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.

A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações CPU, MEMÓRIA, DISCO;

O acesso para ferramenta de configuração do gerenciamento em nuvem (Plataforma) deverá ser com acesso seguro via HTTPS, com possibilidade de uso de duplo fator de autenticação.

Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;

A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do Brasil e inglês;

A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.

A plataforma de gerenciamento em nuvem permitirá gerência granular de politicas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;

A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.

Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:

- Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows Server 2016/2019/2022
- Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silencio onde a ação é tomada e o usuário não é notificado;
- Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- O console de gerenciamento Web deverá prover na tela principal um Dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- A solução deverá prover dashboard detalhado do gerenciamento do antimaware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados SQLServer, MySQL, PostgreSQL, Oracle, monitoramento do serviço do Microsoft Active Directory e DNS, informações quanto aos sistema operacionais instalados, versão do sistema operacional, informações quanto ao numero de maquinas com licença ativa do Windows bem como licenças não validas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- A solução deverá prover relatórios referente as informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.

- A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes (“worms”), cavalos de tróia (“trojan”), códigos espiões (“spyware”, “keylogger”, “screenlogger”, etc), códigos de apoio à invasão e escalada de privilégio (“rootkit”, “backdoor”, etc), código e conteúdo indesejado (“dialer”, “adware”, “joke”,etc);
- Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- Permitir detecção de ameaças em arquivos compactados nos principais algoritmos (“ZIP”, “RAR”, “7zip”)
- A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em especifico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
- Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- Possuir camada de proteção de arquivos contra sequestro de informações;
- Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- Permitir gerar “kit de emergência” que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para analise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil.
- Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;
- Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como

definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto PUP do acrônico em inglês Possible Unintended Programs, ou seja, programas possivelmente indesejados como exemplos Adwares e Spywares;

- A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (PUP - Possible Unintended Programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que uma regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequencia;
- A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimaware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, MEMÓRIA e DISCO e tais informação deverão estar disponíveis em um painel ou dashboard especifico para monitoramento;
- O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: Status do Dispositivo, Data em que os dados foram coletados, O número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, Nome do Host, Versão do antivirus/antimalware, Versão do Sistema Operacional, Usuário logado no dispositivo, Tempo de Atividade, Consumo e total de CPU, Consumo e total de memória RAM, Consumo e total de memória Swap, Consumo e volume total de Disco, Interfaces de rede, Serviços que estão em execução, Serviços que estão parados, Processos que estão mais consumindo CPU, Processos que estão mais consumindo Memória, Informações de Hardware, tais como: Drivers de impressora, CD-ROM, Dispositivos gerais, IDE, USB, SOM, VÍDEO, Adaptador de Rede, Processaor, BIOS, MEMÓRIA, PLACA DE SOM, DISCO, MEMÓRIA, Informações dos softwares instalados, tais como: fabricantes, software e versão;
- O sistema deverá permitir monitoramento por meio de protocolo SNMP de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma

- A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na BIOS;
- O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;
- O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a Internet, geralmente por meio de uma rede sem fio (Wi-Fi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- O sistema deverá permitir o controle e gestão de patchs do Sistema Operacional e outros produtos Microsoft gerenciáveis pelo Windows Update;
- O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;
- O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam IP na mesma;
- O sistema terá um módulo de prevenção contra vazamento de dados (DLP – Data Loss Prevention), que permitirá identificar através de SCAN se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.

No caso de Smartphones Android, o sistema deverá prover as funcionalidades de:

- Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- Permitir bloqueio de determinados aplicativos por horário
- Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos
- Configuração remota de redes Wifi
- Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- Disponibilizar informações sobre o dispositivo como Sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas

No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:

- A solução deverá prover agente para monitoramento do sistemas operacional Linux prevendo ao menos o funcionamento nas versões CentOs 7 e 7, Debian 8, 9 e 10, Ubunto 14, 16 e 18;
- A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- Ativar ou desativar recebimento de alerta dos dispositivos;
- Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, MEMÓRIA e DISCO e tais informações deverão estar disponíveis em um painel ou Dash Board específico para monitoramento;
- Trazer as seguintes informações de cada dispositivo: Status do Dispositivo, Data em que os dados foram coletados, Nome do Host, Versão do Sistema Operacional, Usuário logado no dispositivo, Consumo e total de CPU, Consumo e total de memória RAM, Consumo e total de memória Swap, Consumo e volume total de Disco e suas partições, Interfaces de rede, Serviços que estão em execução, Serviços que estão parados, Processos que estão mais consumindo CPU, Processos que estão mais consumindo Memória, Histórico de comandos executados, Localização do dispositivo em mapa georreferenciado, A solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;
- A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;
- O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover App para ser instalado em dispositivos móveis da família Android;
- Deverá disponibilizar função modo TV para facilitar a análise das informações;
- Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: CPU, MEMÓRIA e DISCO;
- Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;
- Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo CPU, memória e carga média;
- Permitir monitorar as interfaces de rede;
- A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- Permitir emitir alertas de uptime de um determinado website através da configuração da URL, assim como certificado SSL, lista negra;
- Ficam nomeados os senhores Osark Adriano Prado Lunardi e Fabio Gonçalves Costa para atuarem, respectivamente, como Fiscal e Gestor do Contrato.

- Os recursos para a presente contratação são oriundos do orçamento do Fundo de Previdência Social do Município de Sumaré, com a seguinte dotação orçamentária: 09.272.0002.2028.3.3.90 – Serviços de Terceiros – Pessoa Jurídica (ficha 26)

Sumaré, 09 de dezembro de 2025

Maria Elisabete Antunes
Gerente Financeira

Larissa Coelho de Morais Monção
Superintendente Previdenciária