**EDITAL DE PREGÃO PRESENCIAL Nº 011/2025**
**PROCESSO Nº 946/2024 ( 414/2024 SEI)**
**DATA DA REALIZAÇÃO: 25 de julho de 2025.**
**HORÁRIO: 10h00minh.**
**LOCAL: RUA VIGÁRIO CORRÊA, 1345, CORREAS, PETRÓPOLIS–RJ, SALA DE LICITAÇÕES DO SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO.**

**O SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO - SEHAC**, através do setor de licitação, TORNA PÚBLICO, para conhecimento de quantos possam se interessar, que fará realizar licitação na modalidade de **PREGÃO PRESENCIAL**, do tipo menor preço, para **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO DE CYBER SEGURANÇA, PELO PERÍODO DE 60 (SESSENTA) MESES**, conforme especificado no Anexo I do Edital**.** O certame deverá ser processado e julgado em conformidade com o Regulamento de Licitações e Contratações do Serviço Social Autônomo do Hospital Alcides Carneiro – Portaria 009 de 04 de dezembro de 2008 e demais normas complementares e disposições deste instrumento.

## 1 - INFORMAÇÕES

1.1. O caderno de licitação, composto deste Edital e de seus Anexos, poderá ser obtido através do site: www.alcidescarneiro.com ou retirado no setor de licitações do SEHAC, situado na Rua Vigário Corrêa, 1345, Corrêas, Petrópolis–RJ;

1.2. As informações relativas a este **PREGÃO** poderão ser obtidas junto ao Setor de Compras e Procedimentos Competitivos através dos telefones (24) 2236-6674 ou pelo e-mail licitacao@alcidescarneiro.com.

1.3. Quaisquer questionamentos acerca do edital deverão ser encaminhados exclusivamente por meio eletrônico, dirigidos ao Pregoeiro, para o endereço licitacao@alcidescarneiro.com até 02 (dois) dias úteis antes da data designada para a abertura das propostas.

1.4. A modalidade Pregão Presencial foi escolhida, tendo em vista, que a única plataforma eletrônica utilizada pelo Setor de Compras é o Portal Bionexo, a qual não é adequada para contratações do objeto do certame, uma vez que é plataforma utilizada para a modalidade cotações e escolhas eletrônicas, prevista no Atg. 13, inciso VIII do RLC SEHAC- Portaria nº 009 de 04/12/2008, adstrita a aquisições de matérias e insumos médicos-hospitalares.

## 2 - OBJETO

2.1 Constitui objeto deste **PREGÃO PRESENCIAL**, do tipo menor preço, para **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO DE CYBER SEGURANÇA, PELO PERÍODO DE 60 (SESSENTA) MESES**, de acordo com as especificações contidas no Anexo I deste Edital.

2.2 O prazo da prestação de serviço é de 60 (sessenta) meses contados a partir da assinatura do contrato e poderá ser prorrogado por iguais e sucessivos períodos limitado ao máximo permitido em lei, respeitando as condições estabelecidas no

presente edital e valores de acordo com o praticado no mercado. Assim como poderá sofrer acréscimos ou supressões que forem necessárias, obedecendo para tanto o limite de 25% do valor contratado e a disponibilidade financeira;

## 3 - IMPUGNAÇÃO DO EDITAL

3.1 O presente Edital poderá ser impugnado no prazo de 03 (três) dias a contar da sua comunicação, conforme disposto no art.19, VI, § 3º do Regulamento de Licitações e Contratações do Serviço Social Autônomo do Hospital Alcides Carneiro – Portaria 009 de 04 de dezembro de 2008.

## 4 – CONDIÇÕES DE PARTICIPAÇÃO

4.1 Poderão participar deste pregão as empresas que atenderem a todas as exigências deste Edital;

4.2 Será vedada a participação de empresas declaradas inidôneas para licitar e contratar com o poder público; suspensas de participar de licitações realizadas pela Administração Pública. (As empresas participantes poderão ser analisadas através do Portal da Transparência - http://www.portaldatransparencia.gov.br;

4.3 É vedada a participação de licitantes cuja atividade fim não for compatível com o objeto desta licitação, que será comprovada por intermédio do ato constitutivo em vigor (documento consolidado ou acompanhado de todas as alterações), podendo ser acrescido a este documentação complementar que possibilite identificar a compatibilidade da atividade fim com o objeto da licitação

4.4 É vedada a participação de licitantes que tenham como sócios, acionistas ou empreguem funcionários ou familiar de funcionários da CONTRATADA, que exerça cargo de confiança, ou cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação. Considera-se familiar o cônjuge, o companheiro, ou o parente em linha reta ou colateral, por consangüinidade ou afinidade, até o terceiro grau;

4.5 É vedada a participação de empresas constituídas em consórcio qualquer que seja a sua formação.
Obs.: No caso em pauta a justificativa para a vedação da participação de empresas reunidas em consórcio baseia-se na discricionariedade dada pela Lei à Instituição. Para determinar tal vedação, a Instituição buscou primar pela qualidade dos serviços e pelo equilíbrio econômico e financeiro da empresa que, se vencedora do certame, prestará os serviços nesta localidade. Considerando as condições dos serviços exigidos conforme as “dimensões e complexidade do objeto”, o fornecimento de gases medicinais para as Unidades de Pronto Atendimento não requer tal complexidade para que seja necessária a atuação de duas ou mais empresas consorciadas, eis que apenas uma empresa poderá prestar o serviço com a qualidade adequada conforme já vem sendo praticado desde a assunção da Unidade pelo SEHAC em 2018, além do que não seria viável duas empresas com objetos similares reunirem-se em um consórcio para a prestação dos serviços licitados em virtude das dimensões do objeto, caracterizado pela demanda equivalente apresentado neste Edital, já que trata-se de serviços de natureza

comum e relativamente simples, sem grandes complexidades ou dificuldades que pudessem levar a restrição no mercado ou ao número de fornecedores capacitados.

4.6 Não será causa de inabilitação de licitante a anotação de distribuição de processo de recuperação judicial ou pedido de homologação de recuperação extrajudicial, caso haja comprovação de que o plano já tenha sido aprovado/homologado pelo juízo competente quando da entrega da documentação de habilitação;

## 5 – SESSÃO PÚBLICA DE PREGÃO

Os documentos referentes ao credenciamento, os envelopes contendo **as propostas comerciais** e os **documentos de habilitação** das empresas interessadas serão entregues ao pregoeiro no momento da abertura da sessão pública de pregão, que será no dia **25 de julho de 2025 às 10h00min,** no setor de licitações do SEHAC, situado na Rua Vigário Corrêa, 1345, Corrêas, Petrópolis–RJ, **não sendo admitida participação de licitante que se apresente após a abertura do primeiro envelope;**

5.1.1 Será admitida a participação de empresas que optarem pelo envio dos envelopes pelo correio;

5.1.2 Em caso de remessa dos envelopes pelo correio, esta deverá ser via SEDEX, com aviso de recebimento, desde que entregue até o dia e hora da competição, no SEHAC, na Rua Vigário Correa, nº 1.345, Correas, Petrópolis-RJ, CEP 25720-322, A/C Setor de Licitações SEHAC;

5.1.3 Todos os documentos deverão estar impreterivelmente rubricados pelo representante legal, além de numerados seqüencialmente;

5.1.4 O Setor de Licitações não terá qualquer responsabilidade com relação a envelopes enviados via correio que não chegarem até o horário acima estipulado.

5.1. Na hora e local indicado no subitem 5.1, serão observados os seguintes procedimentos pertinentes a este **PREGÃO**;

5.2. O credenciamento dos representantes legais das empresas interessadas em participar do certame, mediante apresentação da carta de credenciamento, fora **dos envelopes 01 e 02**, conforme modelo referencial constante no Anexo II;

5.3.1 Para o credenciamento deverão ser apresentados os seguintes documentos:

a) **Documento de Identificação com foto do credenciado**;

b) **Estatuto social, contrato social ou outro instrumento de registro comercial, registrado na Junta Comercial,** no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura;

c) **Tratando-se de procurador: a procuração por instrumento público ou particular**, da qual constem poderes específicos para formular lances verbais, negociar preço, oferecer descontos, interpor recursos e desistir de

sua interposição e praticar todos os demais atos pertinentes ao certame, acompanhado do correspondente documento, dentre os indicados no item acima, que comprove os poderes do mandante para a outorga; **OU** mediante apresentação da **carta de credenciamento**, conforme modelo referencial constante no Anexo II;
OBS: Se o credenciado for o próprio sócio (com poderes para assumir obrigações pela pessoa jurídica concedidos pelo próprio contrato/estatuto social), não será necessária a entrega da procuração no rol acima.

- Nenhuma pessoa, ainda que munida de procuração, poderá representar mais de uma empresa, sob pena de exclusão sumária das representadas;

- Somente poderão participar da fase de lances verbais os representantes devidamente credenciados, sendo que a ausência do representante legal da empresa no decurso da sessão pública implicará na decadência de todo e qualquer direito atribuído aos licitantes.

**5.4 – MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:**

5.4.1. As microempresas e empresas de pequeno porte, para utilizarem as prerrogativas estabelecidas na Lei Complementar nº 123/2006, deverão apresentar, **FORA DOS ENVELOPES**, declaração (ANEXO V) de que ostentam essa condição e de que não se enquadram em nenhum dos casos enumerados no § 4º do art. 3º da referida Lei;

5.5. Abertura dos envelopes **"PROPOSTA COMERCIAL"**;

5.6. Desclassificação das propostas que não atenderem às exigências essenciais deste Edital e classificação provisória das demais em ordem crescente de preços;

5.7. Caso duas ou mais propostas escritas apresentem preços iguais, será realizado sorteio para determinação da ordem de oferta dos lances

5.8. Oferecimento de lances verbais pelos representantes das empresas classificadas;

5.9. Condução de rodadas de lances verbais sempre a partir do representante da empresa com proposta de maior preço em ordem decrescente de valor, respeitadas as sucessivas ordens de classificação provisória, até o momento em que não haja lances menores aos já ofertados;

5.10. Na fase de lances verbais, não serão aceitos lances de valor igual ou maior ao do último, e os sucessivos lances deverão ser feitos em valores decrescentes. Caso seja conveniente, o pregoeiro poderá fixar o valor mínimo para os lances;

5.10.1. Durante a etapa de lances, quando na sua oportunidade de ofertar novo lance não puder cobrir o menor preço apresentado, o licitante poderá oferecer um último lance para melhorar o seu preço, mesmo que este seja superior ao menor preço registrado até aquele momento.

5.11. Não poderá haver desistência de lances ofertados, sujeitando-se o desistente às penalidades previstas neste Edital;

5.12. A desistência, por qualquer participante, quando convocado pelo pregoeiro, da apresentação de lance verbal, implicará a exclusão daquele, da etapa de lances verbais, e a manutenção do último preço apresentado, pelo desistente, para efeito de ordenação das propostas;

5.13. Caso não realizem lances verbais, será verificada a conformidade entre a proposta escrita de menor preço e o valor estimado para a contratação;

**5.14 - MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:**

5.14.1 - A microempresa ou a empresa de pequeno porte mais bem classificada, nos termos do art. 44 da Lei Complementar nº 123/2006, com preços iguais ou até 5% (cinco por cento) superiores à proposta de melhor preço, será convocada para apresentar nova proposta no prazo máximo de 05 (cinco) minutos após o encerramento dos lances, sob pena de preclusão, de acordo com o estabelecido no § 3º do art. 45 da Lei Complementar nº 123/06;

5.14.2 - Não ocorrendo a apresentação da proposta da microempresa ou empresa de pequeno porte, na forma do subitem anterior, serão convocadas, na ordem classificatória, as remanescentes que porventura se enquadrem na hipótese acima, para o exercício do mesmo direito;

5.15. Declarada encerrada a etapa competitiva e ordenadas as propostas, o pregoeiro examinará a aceitabilidade da(s) primeira(s) classificada(s), quanto ao objeto e valor, decidindo motivadamente a respeito;

5.16. Declarada encerrada a etapa competitiva, a comissão procederá à classificação definitiva das propostas, consignando-a em ata;

5.17. Abertura do(s) envelope(s) **"DOCUMENTOS DE HABILITAÇÃO"** apenas da(s) empresa(s) classificada(s) em primeiro lugar;

5.18. Admitir-se-á o saneamento de falhas na documentação de habilitação de acordo com o art. 32 do Regulamento de Licitações e Contratações do Serviço Social Autônomo do Hospital Alcides Carneiro – Portaria 009 de 04 de dezembro de 2008;

5.19. Sendo inabilitada(s) a(s) proponente(s) classificada(s) em primeiro lugar o pregoeiro prosseguirá com a abertura do envelope de documentação da proponente classificada em segundo lugar, e assim sucessivamente, se for o caso, até a habilitação de um dos licitantes;

5.20. Proclamação da(s) empresa(s) vencedora(s) do certame pelo critério de **MENOR PREÇO GLOBAL;**

5.20.1. Embora seja considerado o preço total global para efeito de lances e classificação, o licitante classificado em primeiro lugar deverá, no momento da Sessão Pública do Pregão, quando indagado pelo Pregoeiro, definir o preço global, sendo que este preço não poderá ultrapassar o preço máximo estabelecido para o item, bem como não poderá em hipótese alguma, ser superior ao preço apresentado na proposta inicial.

5.20.2. Caso não seja possível a imediata recomposição dos preços resultantes dos lances, o Pregoeiro estabelecerá um prazo de até 24 (vinte e quatro) horas para que o licitante apresente nova proposta à comissão de Licitação, que poderá ser entregue diretamente no Setor de Licitações do Hospital Alcides Carneiro - SEHAC, em original assinado, ou enviado para o e-mail: licitacao@alcidescarneiro.com assinada e digitalizada, sob pena de desclassificação.

5.21. Proclamada a(s) vencedora(s), qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de três dias úteis para apresentação das razões do recurso, ficando as demais licitantes desde logo intimadas para apresentar contra-razões em igual número de dias, que começarão a correr do término do prazo da recorrente, sendo-lhes assegurada imediata vista dos autos do processo;

5.22. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento;

5.23. A ausência de manifestação imediata e motivada da licitante implicará a decadência do direito de recurso e a adjudicação do objeto da licitação às vencedoras;

5.24. Encaminhamento dos autos do processo à autoridade competente para homologação do certame, na hipótese de não ter havido interposição de recursos;

5.25. É facultado à administração, quando a adjudicatária não formalizar a contratação no prazo e condições estabelecidos, convocar as demais licitantes, na ordem de classificação, para fazê-lo em igual prazo e, preferencialmente, nas mesmas condições ofertadas pela adjudicatária;

5.26. Os envelopes contendo a documentação relativa à habilitação das licitantes desclassificadas e das classificadas não declaradas vencedoras permanecerão sob custódia do pregoeiro, até a efetiva formalização da contratação.

## 6 – APRESENTAÇÃO DOS ENVELOPES E SEU CONTEÚDO

6.1. No ato de credenciamento, o representante de cada licitante deverá apresentar, simultaneamente, 2 (dois) envelopes, fechados e indevassáveis, sendo:

**ENVELOPE Nº 1 - PROPOSTA COMERCIAL**
SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO
**RUA VIGÁRIO CORRÊA, 1345, CORRÊAS, - PETRÓPOLIS/RJ**
PREGÃO PRESENCIAL **Nº ____/2025**
(RAZÃO SOCIAL DO CONCORRENTE)

**ENVELOPE Nº 2 - DOCUMENTOS DE HABILITAÇÃO**
SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO

**RUA VIGÁRIO CORRÊA, 1345, CORRÊAS, - PETRÓPOLIS/RJ**
PREGÃO PRESENCIAL **Nº ____/2025**
(RAZÃO SOCIAL DO CONCORRENTE)

6.1.1. Os envelopes deverão estar sobrescritos com a titulação de seu conteúdo, nome e endereço da empresa, número do **PREGÃO** e número do Processo Administrativo;

6.1.2. Após a entrega dos envelopes, não caberá desistência da proposta, salvo por motivo justo, decorrente de fato superveniente e aceito pelo pregoeiro e equipe de apoio;

6.1.3. Não caberá desistência da proposta em hipótese alguma, depois de aberto o respectivo envelope.

6.2. O **envelope nº 1** conterá a proposta comercial, que deverá ser apresentada em papel timbrado da empresa, sem rasuras ou emendas.

6.3. Os **envelopes nº 1** de proposta serão abertos diante dos presentes, que rubricarão o seu conteúdo;

6.4 O **envelope nº 1**, devidamente fechado, em papel timbrado, sem emendas ou rasuras, identificação social, número do CNPJ, assinatura do representante da proponente, referência a esta licitação, número de telefones, endereço, dados bancários, endereço eletrônico e descrição clara e detalhada dos produtos cotados;

6.4.1. A empresa licitante deverá apresentar comprovação ponto a ponto, contemplando os requisitos funcionais estabelecidos no termo de referência, para cada uma das tecnologias exigidas e utilizadas para a prestação do serviço contratado

6.5. O prazo de validade da proposta não poderá ser inferior a **60 (sessenta) dias**, contados da sua entrega;

6.6. O preço deve ser cotado em reais. Qualquer divergência de preços será corrigida pela comissão de procedimentos competitivos, prevalecendo sempre o **menor preço**. A não concordância com a correção acarretará a **desclassificação** da proposta do concorrente;

6.7. Quando forem constatados erros nas propostas dos competidores, estes deverão ser corrigidos pela comissão de procedimentos competitivos, desde que tal correção não acarrete modificação do conteúdo da mesma;

6.8. O procedimento competitivo objeto deste Edital é do tipo **MENOR PREÇO** e o critério de julgamento será **GLOBAL;**

**6.8.1.** O critério de menor preço global foi definido com base na economicidade e na eficiência administrativa.
A contratação de empresa especializada serviços de cibersegurança de forma global reduz custos operacionais, facilita a logística e garante a uniformidade na prestação do serviço, evitando fragmentações que poderiam comprometer a continuidade do serviço às unidades descritas no Termo De Referência.

6.9. Fica estabelecido como preço máximo a ser aceito o valor estimado, conforme Anexo I do Edital;

6.10. Ao pregoeiro cabe o direito de desclassificar qualquer proposta que esteja em desacordo com as disposições legais e com as deste Edital;

6.11. O **envelope nº 2** deverá conter a documentação relativa à habilitação em conformidade com o previsto a seguir:

**a)** Contrato Social e, se for o caso, suas alterações, registrados na Junta Comercial ou Estatuto e Ata de Alterações, e respectivas publicações, nos casos de Sociedade Anônima OU Certificado de Inscrição no Cadastro de Fornecedores e Prestadores de Serviços da PMP, compatível com o objeto do procedimento competitivo (original acompanhado da cópia ou cópia autenticada), exceto fax, OU SICAF – contendo toda a situação do fornecedor (Conforme modelo Anexo III) Sistema Unificado de Cadastramento de Fornecedores, válidos pelo menos até a data de realização do procedimento competitivo.

**OBS.:**

- **No caso de apresentação** do Certificado acima citado, o concorrente deverá trazer declaração de que após a retirada do mesmo não ocorreu nenhum fato que impeça a sua participação na competição;

- **No caso de apresentação apenas do SICAF,** as empresas deverão apresentar cópia dos documentos dos sócios.

**b)** Certidão Conjunta Negativa ou Positiva co m Efeito de Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União - CND;

**c)** Certificado de Regularidade de Situação junto ao FGTS;

**d)** Certidão Negativa ou Positiva com Efeito de Negativa de Débitos Trabalhistas – CNDT;

**e)** A empresa licitante deverá apresentar um ou mais atestado(s) de Capacidade Técnico-Operacional emitido(s) por pessoa jurídica de direito público ou privado, em nome da LICITANTE, que comprove(m) experiência na prestação, de forma satisfatória, de Serviços Gerenciados de Segurança da Informação similares aos especificados no Termo de Referência e seus anexos, sendo tais documentos avaliados pelo responsável técnico designado para essa contratação;

Serão considerados compatíveis os atestados que comprovem a prestação de Serviços Gerenciados de Segurança da Informação, das seguintes parcelas de maior relevância:

Serviço gerenciado de segurança da informação;

Será considerado serviço gerenciado de segurança da informação, aquele serviço que contemple, no mínimo, o suporte, operação e proatividade de ativos de segurança da informação, tais como firewall, antimalware, antispam, DLP, WAF, web gateway, entre outros.

Serviços de monitoramento, detecção e resposta de eventos e incidentes de segurança da informação contemplando no mínimo:

Dois Centros de Operações de Segurança (SOC) remotos e próprios;
Equipes de profissionais especializados em segurança da informação, operando em regime contínuo e ininterrupto 24/7/365;

Fornecimento e utilização de solução tecnológica especializada para gerenciamento, análise, automação e resposta de informações, eventos e incidentes de segurança, com recursos de aprendizado de máquina;

Capacidades de inteligência de ameaças (threat intelligence), caçada contínua de ameaças (threat hunting) e gerenciamento de crises.

Será admitido o somatório de atestados para obtenção dos quantitativos exigidos, desde que pelo menos 01 (um) dos atestados contemple pelo menos 50% (cinquenta por cento) do total dos quantitativos; desde que a soma dos atestados contemple no mínimo 50% (cinquenta por cento) do total pretendido;

O(s) atestado(s)/certidão(ões)/declaração(ões) deverá(ão) ser apresentado(s) em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato e deve(m) indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da CONTRATADA.

Os atestados de capacidade técnica apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela CONTRATADA e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a LICITANTE, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

**f)** A empresa licitante deverá apresentar seu certificado de adequação à Norma NBR ISO/IEC 27001, cujo escopo contemple, ao menos, as centrais de operação de segurança (SOC) utilizadas para a prestação do serviço;

**g)** Declaração da licitante de que não possui em seu quadro funcional nenhum menor de dezoito anos desempenhando trabalho noturno, perigoso ou insalubre ou qualquer trabalho pormenor de dezesseis anos, na forma do art.7°, inciso XXXIII, da Constituição Federal (conforme modelo do Anexo VI);

**h)** A empresa licitante deverá apresentar seu certificado de adequação à Norma NBR ISO/IEC 27001, cujo escopo contemple, ao menos, as centrais de operação de segurança (SOC) utilizadas para a prestação do serviço;

**i)** Declaração expressa de que não está incluído em nenhuma das vedações contidas no item 4 deste edital, sendo da sua total responsabilidade a veracidade das informações;

**j)** Declaração que está ciente das condições contidas no Edital e em seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;

**k)** Declaração de que, até a presente data, inexistem fatos impeditivos para a habilitação no presente processo de seleção, ciente da obrigatoriedade de declarar ocorrências posteriores

**l)** Declaração de que a empresa para assinatura do contrato irá apresentar todos as documento das solicitados no ANEXO VIII, sendo tais documentos avaliados pelo responsável técnico designado para essa contratação, esses documentos deverão ser entregues no prazo de 20 (vinte) dias a partir do chamamento.

**m)** Certidão Negativa de**Falência**,**Concordata**, do Cartório Distribuidor da Comarca sede da proponente, deverá<u>estar válida na data de CONVOCAÇÃO</u>. A certidão deverá conter expressamente o prazo de validade, ou quando ausente será considerada válida por um período de **90 (noventa) dias** corridos, a contar da data da sua emissão pelo órgão expedidor, salvo disposição legal em contrário comprovada pelo proponente.

**n) BALANÇOPATRIMONIALEDEMONSTRAÇÕESCONTÁBEISdoúltimo exercício social,**já exigíveis e apresentados na forma da lei, registrado no órgão competente, **SPED CONTABIL e para as empresas optantes pelo simples DEFIS**, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 03 (três) meses da data de apresentação da proposta, que permitam aferir a condição financeira da empresa licitante.

**<u>OBS.</u>:**No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

- Balanço Patrimonial e Demonstrações Contábeis deverão estar assinados por contabilista, devidamente registrado no Conselho Regional de Contabilidade e pelo proprietário da empresa licitante.

- Os Balanços patrimoniais relativos ao item b) acima deverão conter, no mínimo, Termo de abertura e encerramento, as contas do ativo e do passivo do último exercício fiscal e do anterior, indicação do Patrimônio Líquido, o resultado do exercício (DRE) e eventuais notas explicativas.

**o)** Comprovação de possuir Capital Mínimo ou Patrimônio Líquido Mínimo de até **5%(cinco por cento) do valor estimado da contratação**,devendo a comprovação ser feita relativamente à data de apresentação da proposta, na forma da Lei, admitida a atualização para esta data através de índices oficiais.

**p)** As MICROEMPRESAS ou EMPRESAS DE PEQUENO PORTE deverão

apresentar documento (declaração ou outro documento hábil) esclarecendo tal situação, para fins de aplicação da Lei Complementar nº 123, de 14.12.2006, Lei Complementar nº 147/2014 (que altera a Lei Complementar nº 123/2006) e Dec. 8538/15, ressaltando, ainda, que não se enquadram nos termos do § 4º, do artigo 3º da Lei Complementar 123/2006.

## 6.12 – MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:

6.12.1. Aos licitantes que se enquadrem como MPE, nos termos da LC 123/06, deverão comprovar essa condição, mediante a apresentação de Certidão expedida pela Junta Comercial de seu domicílio, conforme o Art. 8º da IN 103 do Departamento Nacional de Registro do Comércio, de 30/04/2007, a qual deverá ser encaminhada ao pregoeiro juntamente com os demais documentos de habilitação;

6.12.2. Regularidade fiscal tardia - deverão ser apresentados todos os documentos de regularidade fiscal, mesmo que apresentem alguma restrição, nos termos do art. 43 da Lei Complementar nº 123/2006;

6.12.3. Será assegurado à MPE que tenha exercido o direito de preferência, e que apresentar alguma restrição na sua documentação fiscal, o prazo de 05 (cinco) dias úteis contados a partir da notificação do pregoeiro, prorrogável por igual período, a pedido da interessada e a critério do pregoeiro, para a necessária regularização;

6.12.4. A não-regularização da documentação fiscal da MPE, no prazo previsto no subitem anterior, implicará a decadência do direito à contratação, sem prejuízo das sanções cabíveis.

## 7 – DISPOSIÇÕES GERAIS SOBRE OS DOCUMENTOS

7.1. Todos os documentos exigidos deverão ser apresentados no original ou por qualquer processo de cópia, exceto fax, ou em publicação de órgão da imprensa, na forma da lei, e serão retidos para oportuna juntada aos autos do processo administrativo;
**OBS: No caso de fundada dúvida sobre a autenticidade do documento, o Pregoeiro poderá solicitar documento original para confirmação da veracidade do mesmo (Súmula 11 do TCE/RJ);**

7.2. Todos os documentos expedidos pela licitante deverão estar subscritos por seu representante legal ou procurador, com identificação clara do subscritor;

7.3. Os documentos devem estar com seu prazo de validade em vigor. Se este prazo não constar de lei específica ou do próprio documento, será considerado o prazo de validade de 06 (seis) meses, a partir da data de sua expedição;

7.4. Os documentos emitidos via internet poderão ser conferidos pela comissão de licitação;

7.5. Os documentos apresentados para a habilitação deverão estar em nome da licitante e, preferencialmente, com número de CNPJ. Se a licitante for matriz, todos os documentos deverão estar em nome da matriz. Se for filial, todos os documentos deverão estar em nome da filial, exceto aqueles que, pela própria

natureza ou por determinação legal, forem comprovadamente emitidos apenas em nome da matriz ou cuja validade abranja todos os estabelecimentos da empresa;

7.6. Todos os documentos acima listados deverão ser apresentados sem exceção, mesmo que existam informações repetidas em documentos distintos. Em nenhuma situação um documento substituirá outro. Nos casos de inexigibilidade de documentação, a empresa deverá apresentar documento informativo oficial.

## 8 - DO PREÇO E DA DISPONIBILIDADE FINANCEIRA

8.1. Os preços ofertados deverão incluir todos os custos diretos e indiretos da proponente, inclusive encargos sociais, trabalhistas e fiscais que recaiam sobre o objeto licitado, bem como todos os custos decorrentes da prestação dos serviços, tais como viagens e estadias, locomoção e outras despesas não mencionadas;

8.2. O preço deve ser cotado em reais. Havendo divergência entre os preços unitários e o preço global, a correção será feita prevalecendo o menor preço. A não concordância com a correção acarretará a desclassificação da proposta do concorrente;

8.3. O preço da proposta é fixo e irreajustável pelo período de 12 (doze) meses. Ultrapassado tal prazo, caberá reajuste pelo IGPM; (Índice Geral de Preços do Mercado no mês de aniversario ou mais próximo), No caso de extinção deste, outro índice, será aplicado outro que vier a substituí-lo.

8.4. As hipóteses excepcionais de revisão de preços serão tratadas de acordo com a legislação vigente e exigirão detida análise econômica para avaliação de eventual desequilíbrio econômico-financeiro do contrato;

8.5 Os recursos financeiros para execução da presente competição são provenientes do Orçamento Anual do SEHAC aprovado por seu Conselho Diretor, conforme regulamento aprovado pelo Decreto Municipal nº 593 de 17 de dezembro de 2007.

## 9 – DO TERMO DE CONTRATO

**9.1 Para assinatura do contrato a empresa considerada habilitada deverá apresentar todos as documento das solicitados no item 11 do termo de referência, sendo tais documentos avaliados pelo responsável técnico designado para essa contratação.**

9.2. - Será adjudicado o objeto da competição à(s) vencedora(s), com a posterior homologação do resultado pela autoridade superior;

9.3. – Uma vez homologado o resultado da competição, a(s) vencedora(s) será(ão) convocada(s) **via e-mail** pelo Setor de Contratos da Instituição (email: contratos@alcidescarneiro.com) no qual será enviado o competente contrato de locação a ser firmado para assinatura, tendo as vencedoras o prazo de até 72 (setenta e duas) horas contados a partir do envio do termo para apresentar o documento em três vias assinado pelos representantes legais da empresa ao SEHAC.

9.4. A apresentação do documento assinado poderá se dar por via física, entregue pessoalmente na Instituição ou por Correios/Sedex, devendo, neste último caso, ser encaminhado ao referido Setor, o Código de Rastreio do documento, ou poderá ser apresentado assinado eletronicamente, por assinatura eletrônica com Certificação Digital.

9.5. A falta de respostas ao email enviado pelo Setor de Contratos no prazo informado ou a não entrega do documento assinado ou a recusa de assinatura da(s) vencedora(s) junto ao SEHAC, sem motivo justo, implicará na desistência da(s) mesma(s), sendo facultado ao SEHAC convocar os licitantes remanescentes, na ordem de classificação, para fazê-los nas mesmas condições propostas pela(s) primeira(s), conforme Art. 41, parágrafos 1º, 2º, 3º e 4º do RCL do SEHAC, sem prejuízo das sanções que poderão ser aplicadas a licitante vencedora que se recusou;

9.6. A empresa CONTRATADA deverá iniciar a prestação dos serviços no prazo máximo de até 30 (trinta) dias após a assinatura do contrato;

**10 – DA EXECUÇÃO:**

10.4 A empresa deverá realizar a prestação de serviço, conforme o termo de referencia em anexo no ANEXO VII

**11 - DAS CONDIÇÕES DE PAGAMENTO:**

11.1 **-** Os pagamentos serão efetuados por meio de crédito em conta corrente, cujo número e agência deverão ser informados pela adjudicatária;

11.2 – Os pagamentos serão realizados após 30 (trinta) dias da entrega e aceite do objeto contratado, mediante apresentação de nota fiscal;

11.3 - Os pagamentos serão efetuados mediante apresentação de nota fiscal, conforme segue**:**

a) Nota Fiscal;

b) A empresa deverá emitir uma nota fiscal específica para cada pedido e respectiva entrega efetuada, na forma abaixo:

***NOME: SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO.***
***ENDEREÇO: RUA VIGÁRIO CORRÊA 1345 – CORRÊAS – PETRÓPOLIS.***
***C.N.P.J.: 09.444.759/0001-38***
***INSC. ESTADUAL: Isento.***
***INSC. MUNICIPAL: 90.194.***

c) Na nota fiscal ou fatura deverá constar obrigatoriamente o nome do Banco, agência e conta corrente da EMPRESA, para realização do pagamento obrigatoriamente por crédito em conta corrente.

d) Caso as notas fiscais ou faturas tenham sido emitidas com incorreções ou em desacordo com a legislação vigente, as mesmas serão devolvidas e o prazo

para pagamento passará a ser contado a partir da reapresentação das mesmas.

e) Caso algum item constante na nota fiscal seja impugnado, o SEHAC liberará a parte não sujeita a contestação, retendo o restante do pagamento até que seja sanado o problema;

f) Caso seja devido, será feita uma retenção de 11% (onze por cento) sobre o valor da Nota Fiscal, referente ao INSS, de acordo com a IN n.º 971, de 13.11.2009.

g) Caso sejam devidas, serão feitas retenções sobre o valor da nota fiscal dos percentuais referentes à Contribuição Social sobre o Lucro Líquido (CSLL), COFINS e PIS/PASEP de acordo com a IN n.º 381 de 30/12/2003.

h) Caso seja devido, será feita retenção do Imposto sobre Serviços (ISS), de acordo com a Lei Complementar n.º 116 de 01/08/2003.

11.4 **-** Compensações Financeiras e Penalidades - sempre que ocorrer atrasos nos pagamentos, o SEHAC ficará sujeita a pagar 0,1% (zero vírgula hum por cento) pró-rata dia, limitada ao total de 2% (dois por cento);

11.5 **–** Critério de reajuste: O preço da proposta é fixo e irreajustável pelo período de 12 meses. Ultrapassado tal prazo, caberá reajuste pelo IGPM (Índice Geral de Preços do Mercado), ou em caso de extinção deste, outro índice que vier a substituí-lo.

**12 - PENALIDADES**

12.1 - A vencedora da competição que descumprir quaisquer das cláusulas ou condições do presente Edital ficará sujeita às penalidades previstas abaixo, observando-se o direito ao contraditório e à ampla defesa;

12.2 - Pela inexecução total ou parcial deste Contrato, a contratada, garantida a prévia defesa, ficará sujeita às sanções previstas no art. 61 do Regulamento de Licitações e Contratações do SEHAC;

12.3 - De conformidade com o art. 64 do Regulamento de Licitações e Contratações do SEHAC, a contratada, garantida a prévia defesa, poderá incorrer nas seguintes PENALIDADES:

a) Advertência;

b) Multas;

- Multa equivalente a 3% (três por cento) do valor total atualizado do contrato, no caso de inadimplemento;

- As multas aplicadas serão consideradas dívida líquida e certa, ficando o **SEHAC** autorizado a descontá-las dos pagamentos devidos à **EMPRESA**, ou das garantias oferecidas ou ainda, cobrá-las judicialmente, servindo, para tanto, o presente instrumento, como título executivo extrajudicial;

- A aplicação das multas aqui previstas não exime a empresa de responder perante o **SEHAC** por perdas e danos, conforme legislação em vigor;

c) Suspensão temporária de participação em competição e impedimento de contratar com o SEHAC pelo prazo de 01 (hum) ano;

d) Declaração de inidoneidade para licitar ou contratar com o SEHAC, até que seja movida reabilitação do concorrente perante o mesmo;

e) Contra a decisão de rescisão do contrato ou da aplicação de penalidades previstas neste Edital, cabe recurso conforme artigo 65 inciso IV e V, artigo 66 §§ 1º, 2º e 3º do Regulamento SEHAC;

## 13 - DISPOSIÇÕES GERAIS

13.1 A apresentação de proposta implica aceitação de todas as condições estabelecidas neste Edital; não podendo qualquer licitante invocar desconhecimento dos termos do ato convocatório ou das disposições legais aplicáveis à espécie para furtar-se ao cumprimento de suas obrigações;

13.2 O presente **PREGÃO** poderá ser anulado ou revogado, nas hipóteses previstas em lei, sem que tenham as licitantes direito a qualquer indenização, observado o disposto no Regulamento de Licitações e Contratações do SEHAC;

13.3 A CONTRATADA se compromete a manter, durante a execução do presente contrato, todas as condições de habilitação e qualificação exigidas na contratação;

13.4 Todas as despesas com a realização dos serviços deverão estar incluídas no preço proposto pelo competidor;

13.5 Manter a qualidade e a especificação do serviço fornecido durante todo o período de vigência do contrato;

13.6 A Contratada se obriga a cumprir o preço pactuado na proposta, durante todo o procedimento competitivo até efetiva conclusão do contrato.

13.7 Com fundamento no Regulamento de Licitações e Contratações do SEHAC é facultada à comissão julgadora, em qualquer fase de licitação, promover diligência destinada a esclarecer ou a complementar a instrução do processo;

13.8 Casos omissos e dúvidas serão resolvidos de acordo Regulamento de Licitações e Contratações do SEHAC;

13.9 As normas deste **PREGÃO** serão sempre interpretadas em favor da ampliação da disputa entre os interessados, e o desatendimento de exigências formais, desde que não comprometa a aferição da habilitação da licitante nem a exata compreensão de sua proposta, não implicará o afastamento de qualquer licitante.

## 14 - ANEXOS

Anexo I - Especificações técnicas;

Anexo II - Modelo referencial de credenciamento de representantes;

Anexo III - Modelo impressão SICAF;

Anexo IV - Minuta do contrato;

Anexo V - Modelo de Declaração ME ou EPP.

Anexo VI - Modelo de Declaração.

Anexo VII - Termo de Referência;

Petrópolis, 18 de junho de 2025

Gustavo Gonçalvez Carneiro
Diretor Presidente do SEHAC

## ANEXO I

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO DE CYBER SEGURANÇA, PELO PERÍODO DE 60 (SESSENTA) MESES,** conforme especificado abaixo:

| ITEM | MATERIAL / PRODUTO / SERVIÇO | UND | QTDE | VALOR MÁXIMO A SER ACEITO |
|---|---|---|---|---|
| 1 | Contratação de empresa de Cyber Segurança | MÊS | 60 | 26.813,00 |

**Valor Total Estimado: R$ 1.608.780,00 (um milhão seiscentos e oito mil setecentos e oitenta reais)**

O prazo de validade da proposta não poderá ser inferior a **60 (sessenta) dias**, contados da sua entrega

O procedimento competitivo objeto deste Edital é do tipo **MENOR PREÇO** e o critério de julgamento será **GLOBAL;**

Fica estabelecido como preço máximo a ser aceito o valor estimado, conforme Tabela acima.

A empresa deverá prestar o serviço conforme descrito no Termo de Referência no ANEXO VII

**ANEXO II**

MODELO de CREDENCIAMENTO

AO SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO
RUA VIGÁRIO CORREA, 1345, CORRÊAS, - PETRÓPOLIS - RJ

Prezados Senhores,

Pela presente, fica credenciado o Sr _____(nome)_____, portador da Carteira de Identidade nº _____ expedida pelo _____ para representar a empresa _____(nome e endereço do concorrente)_____ Inscrita no CNPJ sob o nº _____ na competição, modalidade de Procedimento de Pregão Presencial, a ser realizada em " DATA", no SEHAC, podendo para tanto praticar todos os atos necessários, inclusive prestar esclarecimentos, receber notificações, interpor recursos e manifestar-se quanto a sua desistência.

Atenciosamente,

---

OBSERVAÇÃO: Só serão aceitos os credenciamentos assinados pelo **Representante Legal** da concorrente identificado claramente e que tenha poderes para constituir mandatário, servindo o presente como orientação na formulação do mesmo. Apresentar junto com o credenciamento: Estatuto social, contrato social ou outro instrumento de registro comercial, registrado na Junta Comercial, em cópia autenticada ou cópia simples acompanhada do original para autenticação durante a sessão, no qual estejam expressos os poderes do **Representante Legal** para exercer direitos e assumir obrigações em decorrência de tal investidura.

# ANEXO III

Ministério do Planejamento, Orçamento e Gestão
Secretaria de Logística e Tecnologia da Informação

Sistema Integrado de Administração de Serviços Gerais - SIASG
Sistema de Cadastramento Unificado de Fornecedores - SICAF

## Declaração

Declaramos para os fins previstos na Lei nº 8.666, de 1993, conforme documentação apresentada para registro no SICAF e arquivada na UASG Cadastradora, que a situação do fornecedor no momento é a seguinte:

Validade do Cadastro: / /
CNPJ / CPF: 00.000.000/0000-00
Razão Social / Nome: XXXXX XXXXX
Domicílio Fiscal: 00000 - XXXXX XXXXX
Unidade Cadastradora: 000000 - XXXXX XXXXX
Código e Descrição da Atividade Econômica:
0000-0/00 - XXXXX XXXXX

Endereço:
XXXXX XXXXX XXXXX - XXXXX XXXXX
Ocorrência: XXXXX
Impedimento de Licitar: XXXXX

Níveis validados:
I - Credenciamento
II - Habilitação Jurídica
III - Regularidade Fiscal Federal
Receita Validade: / /
FGTS Validade: / /
INSS Validade: / /
IV – Regularidade Fiscal Estadual/Municipal:
Receita Estadual/Distrital Validade: / /
Receita Municipal Validade: / /
VI – Qualificação Econômico-Financeira – Validade: / /
Índices Calculados: SG = ; LG = ; LC =

**Esta declaração é uma simples consulta não tem efeito legal.**

Legenda: documento(s) assinalado(s) com "*" está(ão) com prazo(s) vencido(s).

Emitido em: / /
CPF:
Ass: _____

**ANEXO IV**

**SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO SEHAC**

**CONTRATO Nº /2024**

Contrato de Prestação de Serviços, que entre si fazem**, o SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO, MANTENEDOR DO HOSPITAL DE ENSINO ALCIDES CARNEIRO,** e a Empresa**_____ na forma abaixo:**

**SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO**, instituição de natureza paradministrativa, qualificada como ente de cooperação do Município de Petrópolis, na prestação de serviços de saúde e na manutenção do **HOSPITAL DE ENSINO ALCIDES CARNEIRO**, pessoa jurídica de direito privado e social, sem fins lucrativos, de utilidade pública e interesse coletivo, com sede na Rua Vigário Corrêa, 1345 – Corrêas – Petrópolis/RJ, inscrita no CNPJ sob o nº 09.444.759/0001-38, neste ato representado por seu Diretor Presidente, ..... e pelo seu Diretor de Administração, Finanças e Patrimônio, ...., como **CONTRATANTE**, e a Empresa _____ , inscrita no CNPJ nº , estabelecida na Rua _____, neste ato representado pelo , portador do CPF nº._____ e da C. I. nº_____ , como **CONTRATADA**, têm justo e acertado**,** tudo em conformidade com o processo SEHAC nº_____ , fundamentado na competição _____ e nas normas contidas na Portaria nº 09 de 06/12/08 do Regulamento de Licitações e Contratações do SEHAC, mediante as seguintes cláusulas:

**CLÁUSULA PRIMEIRA: DO OBJETO DO CONTRATO:** O objeto deste **CONTRATO** é a **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO DE CYBER SEGURANÇA, PELO PERÍODO DE 60 (SESSENTA) MESES**, conforme especificado e descrito na proposta vencedora e Anexo I do Edital, que fazem parte integrante do presente **CONTRATO**.

**CLÁUSULA SEGUNDA: DO PRAZO:** O prazo da prestação de serviço é de 60 (sessenta) meses contados a partir da assinatura do contrato e poderá ser prorrogado por iguais e sucessivos períodos limitado ao máximo permitido em lei, respeitando as condições estabelecidas no presente edital e valores de acordo com o praticado no mercado. Assim como poderá sofrer acréscimos ou supressões que forem necessárias, obedecendo para tanto o limite de 25% do valor contratado e a disponibilidade financeira

**CLÁUSULA TERCEIRA:** A **CONTRATADA** se compromete a manter, durante a execução do presente contrato, todas as condições de habilitação e qualificação exigidas na contratação.

**PARÁGRAFO ÚNICO:** A **CONTRATADA** obriga-se, nos termos deste Contrato, a dar irrestrita prioridade ao **CONTRATANTE**, no que diz respeito à entrega dos itens, em detrimento de qualquer compromisso futuro.

**CLÁUSULA QUARTA: DOS PREÇOS:** Para todos os efeitos legais, pela execução do objeto deste **CONTRATO**, a **CONTRATADA** receberá em moeda corrente o valor global de R$ (_____),que serão pagos conforme disposto na cláusula quinta do presente contrato.

**PARÁGRAFO PRIMEIRO:** Nos preços ajustados estão incluídos todos os custos tais como: materiais complementares, insumos, equipamentos, remuneração da CONTRATADA, encargos sociais, previdenciários e trabalhistas despesas financeiras e administrativas, contribuições, seguros, impostos, taxas, royalties, bem como quaisquer outros custos e despesas necessárias a completa execução do objeto deste **CONTRATO**;

**PARÁGRAFO SEGUNDO:** Também estão incluídos no preço toda e qualquer inflação, desvalorização cambial, aumento de juros, aumentos de custos em geral, reajustes de preços quaisquer, que atinjam ou venham a atingir a **CONTRATADA** ou sua atividade, direta ou indiretamente; inclusive, preços de insumos, matérias primas, produtos industrializados, energia, combustíveis, serviços, mão de obra, encargos sociais ou trabalhistas, tributos, contribuições, assumindo a **CONTRATADA**, de forma exclusiva, todos os riscos, ônus, gravames.

**PARÁGRAFO TERCEIRO:** O preço da proposta é fixo e irreajustável pelo período de 12 meses. Ultrapassado tal prazo, caberá reajuste pelo IPGM – Índice Geral de Preços do Mercado, ou em caso de extinção deste, outro índice que vier a substituí-lo.

**CLÁUSULA QUINTA**: **DO PAGAMENTO:** Os pagamentos serão realizados após 30 (trinta) dias da entrega e aceite do objeto contratado, mediante apresentação de nota fiscal;

**PARÁGRAFO PRIMEIRO:** Se ocorrer atraso injustificado no pagamento por parte do **CONTRATANTE**, de qualquer de uma das parcelas, esta ficará sujeita a pagar 0,1% (zero vírgula hum por cento) pró-rata dia, limitada ao total de 2% (dois por cento) do valor do **CONTRATO**;

**PARÁGRAFO SEGUNDO**: Os pagamentos serão efetuados mediante apresentação de nota fiscal, conforme segue:

a) A empresa deverá emitir uma nota fiscal específica para cada pedido e respectivo serviço efetuado, na forma abaixo:

NOME: SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO.
ENDEREÇO: RUA VIGÁRIO CORRÊA 1345 – CORRÊAS – PETRÓPOLIS.
C.N.P.J.: 09.444.759/0001-38
INSC. ESTADUAL: Isento.
INSC. MUNICIPAL: 90.194.

b) Na nota fiscal ou fatura deverá constar obrigatoriamente o nome do Banco, agência e conta corrente da EMPRESA, para realização do pagamento obrigatoriamente por crédito em conta corrente;

c) Caso as notas fiscais ou faturas tenham sido emitidas com incorreções ou em desacordo com a legislação vigente, as mesmas serão devolvidas e o prazo para pagamento passará a ser contado a partir da reapresentação das mesmas;

d) Caso algum item constante na nota fiscal seja impugnado, o SEHAC liberará a parte não sujeita a contestação, retendo o restante do pagamento até que seja sanado o problema;

e) Caso seja devido, será feita uma retenção de 11% (onze por cento) sobre o valor da Nota Fiscal, referente ao INSS, de acordo com a IN n.º 971, de 13.11.2009.

f) Caso sejam devidas, serão feitas retenções sobre o valor da nota fiscal dos percentuais referentes à Contribuição Social sobre o Lucro Líquido (CSLL), COFINS e PIS/PASEP de acordo com a IN n.º 381 de 30/12/2003.

g) Caso seja devido, será feita retenção do Imposto sobre Serviços (ISS), de acordo com a Lei Complementar n.º 116 de 01/08/2003.

**PARÁGRAFO TERCEIRO** - Compensações Financeiras e Penalidades - sempre que ocorrer atrasos nos pagamentos, o SEHAC ficará sujeita a pagar 0,1% (zero vírgula hum por cento) pró-rata dia, limitada ao total de 2% (dois por cento);

**PARÁGRAFO QUARTO** - Os pagamentos serão efetuados por meio de crédito em conta corrente, cujo número e agência deverão ser informados pela adjudicatária.

**CLÁUSULA SEXTA: TRIBUTOS:** Todos os tributos federais, estaduais e municipais, as contribuições fiscais, parafiscais, previdenciárias e trabalhistas, devidos ou que vierem a sê-lo em decorrência do presente **CONTRATO** correrão exclusivamente por conta da **CONTRATADA**, a qual também se responsabilizará pelo fiel cumprimento de todas as obrigações e formalidades legais, perante as autoridades competentes.

**PARÁGRAFO ÚNICO:** Fica convencionado que, se for o **CONTRATANTE** autuado, notificado ou intimado em virtude do não pagamento na época própria, de qualquer obrigação, atribuível à **CONTRATADA**, assistirá o **CONTRATANTE** o direito de reter pagamentos devidos a **CONTRATADA**, até o montante do débito, ou cobrar da **CONTRATADA** o valor das referidas obrigações, consideradas desde já dívida líquida e certa.

**CLÁUSULA SÉTIMA: CESSÃO, SUBCONTRATAÇÃO E RESPONSABILIDADE:** A **CONTRATADA** não poderá transferir nem conceder a cessão do cumprimento do presente **CONTRATO**, nem tampouco transferir, sub-rogar, caucionar, dar

garantias decorrentes deste **CONTRATO**, no todo ou em parte, salvo com prévia e expressa autorização do **CONTRATANTE**.

**CLÁUSULA OITAVA: DA EXECUÇÃO DOS SERVIÇOS:** A empresa deverá realizar a prestação de serviço, conforme o termo de referencia em anexo no **ANEXO II.**

**CLÁUSULA NONA: A CONTRATADA** ficará, pela inexecução total ou parcial deste Contrato, garantida a prévia defesa, sujeita às sanções previstas no art. 61 do Regulamento de Licitações e Contratações do SEHAC;

**PARÁGRAFO PRIMEIRO:** De conformidade com o art. 64 do Regulamento de Licitações e Contratações do SEHAC, a contratada, garantida a prévia defesa, poderá incorrer nas seguintes PENALIDADES:

a) Advertência;

b) Multas;

- Multa equivalente a 3% (três por cento) do valor total atualizado do contrato, no caso de inadimplemento;

c) Suspensão temporária de participação em competição e impedimento de contratar com o **SEHAC** pelo prazo de 01 (hum) ano;

d) Declaração de inidoneidade para licitar ou contratar com o **SEHAC**, até que seja movida reabilitação do concorrente perante o mesmo;

e) A rescisão do contrato operar-se-á nas hipóteses alinhadas no artigo 61 do Regulamento **SEHAC**

f) Contra a decisão de rescisão do contrato ou da aplicação de penalidades previstas neste Edital, cabe recurso conforme artigo 65 inciso IV e V, artigo 66 §§ 1º, 2º e 3º do Regulamento **SEHAC**;

**PARÁGRAFO SEGUNDO:** As multas aplicadas serão consideradas dívida líquida e certa, ficando o **CONTRATANTE** autorizado a descontá-las dos pagamentos devidos à **CONTRATADA**, ou das garantias oferecidas, ou ainda, cobrá-las judicialmente, servindo, para tanto, o presente instrumento, como título executivo extrajudicial.

**PARÁGRAFO TERCEIRO:** A aplicação das multas previstas nesta cláusula não exime a **CONTRATADA** de responder perante o **CONTRATANTE** por perdas e danos, conforme legislação em vigor.

**CLÁUSULA DÉCIMA**: O **CONTRATANTE** poderá rescindir administrativamente o presente **CONTRATO** nas hipóteses previstas no livro II, Título I, Artigos 48 e 49 e seus Incisos, alíneas e parágrafos do Regulamento de licitações e Contratações SEHAC;

**PARÁGRAFO PRIMEIRO**: Constitui motivo para rescisão do **CONTRATO** por parte da **CONTRATADA**, o atraso superior a 90 (noventa) dias dos pagamentos ou parcelas destes, devidos pela **CONTRATANTE**, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao **CONTRATADO** o direito de optar pela suspensão do cumprimento de suas

obrigações, até que seja normalizada a situação, consoante previsto no parágrafo primeiro, artigo 61 do Regulamento de Licitações e Contratações SEHAC.

**PARÁGRAFO SEGUNDO**: Os casos de rescisão contratual deverão ser formalmente motivados no processo administrativo que originou a contratação.

**CLÁUSULA DÉCIMA PRIMEIRA:** A **CONTRATADA** reconhece os direitos do **CONTRATANTE** nos casos de rescisão previstos no Art. 48 parágrafo 3º do Regulamento de licitações e Contratações SEHAC;

**CLÁUSULA DÉCIMA SEGUNDA: DA EXCLUSÃO DE RESPONSABILIDADE:** A **CONTRATADA** assume como exclusivamente seus, os riscos e as despesas decorrentes do fornecimento da mão de obra necessária à boa e perfeita execução do presente contrato e, pelo comportamento de seus empregados, prepostos ou subordinados e ainda, quaisquer prejuízos que sejam causados ao contratante ou a terceiros.

**PARÁGRAFO PRIMEIRO:** O **CONTRATANTE** não será responsável por quaisquer ônus, direito ou obrigações vinculadas à legislação tributária, trabalhista, previdenciária ou securitária decorrentes da execução do presente contrato, cujo cumprimento e responsabilidade caberão exclusivamente à **CONTRATADA;**

**PARÁGRAFO SEGUNDO:** O **CONTRATANTE** não será responsável por quaisquer compromissos assumidos pela Contratada com terceiros, ainda, que vinculados à execução do presente contrato, bem como, por seus empregados, propostos ou subordinados.

**CLÁUSULA DÉCIMA TERCEIRA:** Integram o presente **CONTRATO,** como se dele fizessem parte a proposta vencedora o Edital e seus Anexos. Indica a Administração como fiscal do presente contrato o _____.

**CLÁUSULA DÉCIMA QUARTA:** Aos casos omissos neste edital, aplicar-se-ão o disposto no artigo 32 do Regulamento de Licitações e Contratações do SEHAC;

**CLÁUSULA DÉCIMA QUINTA:** Os recursos para fazer face às despesas decorrentes deste **CONTRATO** são provenientes do orçamento anual do SEHAC, aprovado por seu Conselho Diretor, conforme em seu estatuto, aprovado pelo Decreto Municipal nº 593 de 17 de dezembro de 2007.

**CLÁUSULA DÉCIMA SEXTA**: É competente o foro da Comarca de Petrópolis, para nele serem dirimidas quaisquer controvérsias decorrentes do presente **CONTRATO**. E, por estarem justos e contratados, assinam o presente juntamente com as testemunhas abaixo.
**********

Petrópolis, .....

# ANEXO V

MODELO DE DECLARAÇÃO DE ME OU EPP

Ref.: .....

_____(razão social da empresa), com sede na _____ (endereço), inscrita no CNPJ nº _____, vem, por intermédio de seu representante legal o(a) Sr(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA, sob as penas da Lei, que é _____(MICROEMPRESA ou EMPRESA DE PEQUENO PORTE), que cumpre os requisitos legais para efeito de qualificação como ME-EPP e que não se enquadra em nenhuma das hipóteses elencadas no § 4º do art. 3º da Lei Complementar nº 123, estando apta a usufruir dos direitos de que tratam os artigos 42 a 45 da mencionada Lei, não havendo fato superveniente impeditivo da participação no presente certame.

.....

(data)

.....
(representante legal)

# ANEXO VI

(MODELO “A” – EMPREGADOR PESSOA JURÍDICA)

DECLARAÇÃO

Ref.: (identificação da licitação)

....., inscrito no CNPJ nº....., por intermédio de seu representante legal o (a) Sr. (a)....., portador (a) da Carteira de Identidade nº.....e do CPF nº....., DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº 8.666/93, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

.....
(data)

.....
(representante legal)

(Observação: em caso afirmativo, assinalar a ressalva acima)

# ANEXO VII



## TERMO DE REFERÊNCIA

### 1. Objeto

Contratação de empresa especializada para execução de serviços técnicos contínuos de Segurança da Informação para atender o complexo hospitalar do HAC em especial ao SEHAC e o próprio Hospital de Ensino Alcides Carneiro, pelo período de 60 (sessenta) meses, conforme condições estabelecidas no presente Termo de Referência.

### 2. Justificativa da contratação

Com o surgimento de novas tecnologias e com a utilização cada vez maior da Rede Mundial de Computadores (Internet), a nossa sociedade se tornou refém de toda essa inovação tecnológica, e com isso, novas práticas passaram a ser adotadas no dia a dia dos cidadãos pelo mundo inteiro. Muitos são os benefícios dessas tecnologias, elas com certeza abriram novos horizontes, permitindo que processos se tornassem mais eficientes, ágeis e confiáveis, entretanto, existe o outro lado que envolve a segurança.

Como todos os problemas que enfrentamos em sociedade são resultado de desvio de conduta e do próprio ser humano, o crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou hackers que querem ganhar dinheiro ou levar algum tipo de vantagem.

Com o propósito de proteger as Unidades geridas pelo SEHAC e tentar evitar o incidente ocorrido no Hospital Alcides Carneiro no dia 04/08/2024, onde tivemos nossos servidores e estações de trabalho invadidas por Hackers, acarretando sérios danos em nossa base de dados e em alguns arquivos da rede, comprometendo a privacidade e até mesmo a perda de informações sensíveis relacionadas aos nossos clientes.

Avaliamos que seria prudente e necessária a contratação de uma empresa especializada em segurança cibernética, pois, com a utilização de suas ferramentas e com a expertise de seus profissionais capacitados e treinados para esse tipo de situação, a mesma terá condições de monitorar qualquer movimentação suspeita ou indesejada em nossa rede de dados, trazendo desta forma a certeza e a sensação de que estamos cuidando de fato de nosso bem mais precioso, que é cuidar do nosso banco de dados e informações.

### 3. Detalhamento do objeto

Este processo tem como objetivo a contratação de uma solução para a proteção, detecção e resposta aos incidentes relacionados à segurança das informações da CONTRATANTE – SEHAC e aos próprios sistemas que atendem ao HAC, contemplando as diversas etapas evolutivas para uma correta e assertiva gestão dos processos de segurança da informação.

Busca-se empresa especializada na prestação de serviços, incluindo os softwares e hardwares necessários para sua execução, através de centrais de operação de segurança (SOC - Security Operations Center), que objetivam assegurar os mais altos níveis de serviço quanto a predição, identificação, contenção e resposta aos incidentes, reduzindo ou mesmo evitando os impactos aos serviços da CONTRATANTE.

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

**Para tal, o objeto a ser contratado abrangerá os seguintes processos:**

3.1.1. Proteção de estações de trabalho;

3.1.2. Proteção de servidores;

3.1.3. Gestão de incidentes;

**Informações Gerais**

3.1.4. Todos os pontos funcionais exigidos e especificados neste termo de referência são requerimentos obrigatórios, devendo ser considerados nas diferentes fases de implementação e, por conseguinte, na execução dos serviços;

3.1.5. Em caso de eventuais ocorrências que demonstrem que os serviços não estão sendo prestados a contento, a CONTRATANTE exigirá a imediata regularização de quaisquer desconformidades observadas, de modo que sejam preservados e mantidos os níveis de serviço contratados;

3.1.6. É vedada a subcontratação total do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência total ou parcial, bem como a fusão, cisão ou incorporação. Fica autorizada a contratação parcial do objeto, nas parcelas de menor relevância, desde que mediante prévia e expressa autorização do CONTRATANTE. É possível a subcontratação parcial de serviços de menor relevância, desde que autorizado expressamente pelo SEHAC.

## 4. Justificativa para o não parcelamento do objeto, modalidade a ser adotada e critério de julgamento

A divisão do objeto em múltiplos fornecedores não é viável devido à natureza indivisível do serviço prestado, pois, embora os serviços possam ser categorizados em disciplinas distintas, isoladamente não seriam capazes de atender plenamente às necessidades da CONTRATANTE.

Além disso, dividir a solução e contratar diversos fornecedores para serviços altamente dependentes entre si não seria vantajoso devido à perda de economia de escala. Os profissionais precisam trabalhar de forma coordenada, uma vez que as ferramentas, atividades e habilidades necessárias para a prestação do serviço devem abranger todas as disciplinas. Se o objeto fosse parcelado, seria muito difícil alcançar essa sinergia, enquanto ter um único responsável por todas as atividades permitirá uma gestão e supervisão mais eficientes, alcançando melhores resultados para a CONTRATANTE.

Além dos argumentos técnicos e do alto grau de dependência entre os serviços, essa contratação envolve serviços de segurança da informação, nos quais a preservação do sigilo das informações é de extrema importância para a CONTRATANTE. Contratar múltiplos fornecedores implicaria em um maior compartilhamento de informações e serviços, aumentando o risco de violação da segurança da informação. Isso contraria o objetivo principal de proteger as informações.

Considerando os aspectos técnicos e os requisitos envolvidos na contratação dos serviços, juntamente com a alta criticidade e complexidade do ambiente de TI, o parcelamento do objeto se torna tecnicamente inviável. Isso se deve aos pereceres técnicos, aos riscos elevados que isso acarretaria para a execução dos serviços, aos possíveis conflitos entre fornecedores e à ausência de ganhos de escala decorrentes da integração das equipes.

No mais, a contratação será realizada através de procedimento competitivo nos termos do Regulamento de Licitações e Contratações do SEHAC- Portaria n° 009 de 04/12/2008, através da modalidade PREGÃO, tendo como critério de julgamento pelo MENOR PREÇO GLOBAL.

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

## 5. Escopo do serviço

**Tabela quantitativo dos Itens**

| ItemObjeto | | Descrição | Qtd | Unidade |
|---|---|---|---|---|
| 1 | Proteção de estações de trabalho | Solução envolvendo serviço gerenciado e ferramentas de proteção de estações de trabalho | 220 | Ativos/mês |
| 2 | Proteção de servidores | Solução envolvendo serviço gerenciado e ferramentas de proteção de servidores | 16 | Ativos/mês |
| 3 | Gestão de Incidentes | Solução integrada envolvendo serviços e ferramentas para Análise de Incidentes Globais e a Detecção e Resposta aos Incidentes | 250 | Ativos/mês |

**Informações do ambiente atual:**

5.1.1. A CONTRATADA deverá dimensionar as soluções de segurança para suportar, sem perda de performance, 250 (duzentos e cinquenta) ativos (incluindo desktops, servidores, impressoras, switches roteadores e todo equipamento que tenha a ele atribuído, um endereço IP), podendo exceder até no máximo 10% desse número sem ocorrer alteração no preço;

5.1.2. A CONTRATANTE possui atualmente 220 (duzentos e vinte) estações de trabalho, 16 (dezesseis) servidores, 14(quatorze) ativos de rede como roteador e switches e dois pontos de coleta de tráfego de rede, a serem cobertos pela solução de Gestão de Incidentes.

5.1.3. Os quantitativos acima referem-se ao SEHAC e as unidades por este geridas, dentro do complexo hospitalar do Hospital Alcides Carneiro;

5.1.4. O prazo de instalação será de no máximo de 30(trinta) dias, eis que há expressa necessidade na prestação do serviço objeto do presente.

## 6. Características gerais do serviço

A fim de garantir a qualidade da entrega do objeto como um todo, os itens abaixo devem ser implantados:

**Considerações Iniciais**

6.1.1. A presente contratação deverá ser entregue na modalidade de prestação de serviços. A CONTRATADA é responsável por prover todos os softwares, hardwares e infraestrutura necessária para o funcionamento das soluções exigidas neste processo, salvo os equipamentos descritos explicitamente, que serão disponibilizados pela CONTRATANTE para hospedar os serviços inerentes ao atendimento do contrato.

6.1.2. Quaisquer informações coletadas durante a execução dos serviços, somente poderão ser divulgadas à terceiros após a aprovação formal da CONTRATANTE.

Serviço Social Autônomo
Hospital Alcides Carneiro



6.1.3. Todos os equipamentos e softwares utilizados pela CONTRATADA para a entrega deste serviço, quando for o caso e se necessário à consecução das atividades de segurança, devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

6.1.4. Todos os equipamentos e softwares utilizados pela CONTRATADA para a entrega deste serviço, devem ser declarados de forma clara e objetiva na proposta cadastrada para a fase de lances deste processo, incluindo, minimamente, fabricante, modelo, versão.

6.1.5. Durante a execução dos serviços, a CONTRATADA deverá disponibilizar o quantitativo de profissionais necessários para atender todos os perfis, buscando o normal desenvolvimento dos Serviços Gerenciados de Segurança.

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

**Modelo de atuação**

6.1.7. O serviço deve ser prestado majoritariamente de forma remota;

6.1.8. As seguintes atividades deverão ser realizadas mediante atendimento presencial:

6.1.8.1. Migração de versionamento dos equipamentos gerenciados;

6.1.8.2. Atuação em incidentes massivos ou desastres;

6.1.8.3. Atuação em casos de inacessibilidade dos equipamentos gerenciados.

**Centro de Operações de Segurança (SOC)**

6.1.9. Características Gerais:

6.1.9.1. O serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center - SOC), incluindo minimamente dois ambientes na CONTRATADA, redundantes entre si e distantes, com pelo menos, 50 km de distância geodésica um do outro.

6.1.9.1.1. Estes ambientes já devem estar em pleno funcionamento na data da diligência, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados;

6.1.9.1.2. Os Centros de Operação de Segurança utilizados para a prestação do serviço deverão possuir a certificação ISO/IEC 27001 vigente, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida;

6.1.9.1.3. Todos os SOC's utilizados para a prestação do serviço devem estar instalados no Brasil ou ter a plena capacidade de atendimento em língua portuguesa.

6.1.9.2. Além dos SOC's, a CONTRATADA deverá fazer uso de uma ferramenta de monitoramento que contemple uma console em nuvem, com a finalidade de que a mesma possa ser acessada, também, a partir do ambiente da CONTRATANTE e que seja possível se fazer o controle do serviço de monitoramento da operação de segurança a partir do ambiente da CONTRATADA e da CONTRATANTE;

6.1.9.3. Cada um dos SOC's devem atender aos seguintes requisitos mínimos:

6.1.9.3.1. Funcionar em regime 24/7/365;

Serviço Social Autônomo
Hospital Alcides Carneiro



6.1.9.3.2. 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;

6.1.9.3.3. 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;

6.1.9.3.4. 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;

6.1.9.3.5. No caso dos serviços de atualização do versionamento dos equipamentos gerenciados e Modernização dos equipamentos gerenciados será necessário a presença do profissional da CONTRATADA no ambiente da CONTRATANTE para acompanhamento dessas operações;

6.1.9.3.6. Possuir UPS que suporte todos os equipamentos essenciais ao funcionamento, por, pelo menos, 30 minutos;

6.1.9.3.7. Utilizar sistema de gerenciamento de CFTV, que viabiliza o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas por no mínimo 90 (noventa) dias;

6.1.9.3.8. Ter o acesso de entrada e saída dos visitantes registrado, com identificação individual, e constituído por pelo menos 02 (dois) fatores de autenticação;

6.1.9.3.9. Ter o perímetro equipado com sensores de intrusão e alarmes contra acesso indevido, além de ser vigiado de forma ininterrupta por segurança perimetral em regime de 24x7x365.

6.1.10. Ambiente da CONTRATADA

6.1.10.1. Os recursos físicos da CONTRATADA (prédio, salas, mesas e outros) poderão ser compartilhados com outros clientes, desde que:

6.1.10.1.1. Toda a infraestrutura lógica que atende a CONTRATANTE seja separada dos demais clientes;

6.1.10.1.2. Todos os funcionários possuam assinado um documento de termo de responsabilidade e sigilo conforme Termo de Ciência e Manutenção de Sigilo deste Termo de Referência;

**Gerência de Serviços**

6.1.11. A gestão deve conhecer os padrões internacionais do HDI seguindo todos os processos definidos pela CONTRATANTE, com comprovação desta aptidão;

6.1.12. Entregar mensalmente relatórios gerenciais, incluindo níveis de serviço, atualizações de versões, principais incidentes e vulnerabilidade, estatísticas sobre desempenho e melhorias propostas, entre outras recomendações;

6.1.13. Entregar relatórios mensais dos resultados dos serviços prestados, com análise crítica clara elaborada pelos times técnicos da CONTRATADA;

6.1.13.1. Tais relatórios deverão ser confeccionados por equipes independentes, utilizando dupla validação das áreas de Cibersegurança e SOC, devendo conter minimamente:

6.1.13.1.1. Descrição das ações realizadas;

6.1.13.1.2. Contatos da CONTRATANTE acionados;

6.1.13.1.3. Possíveis problemas aplicáveis;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

6.1.13.1.4. Apresentação das evidências apuradas;

6.1.13.1.5. Fontes de pesquisa;

6.1.13.1.6. Pontos positivos encontrados;

6.1.13.1.7. Referências;

6.1.13.1.8. Ferramentas utilizadas.

6.1.14. Agendar reunião mensal presencial para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE;

6.1.15. Realizar pesquisa de qualidade operacional trimestralmente, documentando e disponibilizando os resultados para a CONTRATANTE em reunião presencial;

6.1.16. Rever periodicamente as políticas e processos do SOC a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL;

6.1.17. Disponibilizar dashboards de acompanhamento em tempo real da operação do SOC que permitam a validação dos indicadores acordados;

6.1.18. Apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;

6.1.19. Confeccionar relatórios técnicos pontuais sob demanda.

**Canais de Comunicação**

6.1.20. Ferramenta de Service Desk

6.1.20.1. Disponibilizar uma Ferramenta de Service Desk para o registro das demandas e tickets que devem ser tratados pelo SOC;

6.1.20.2. Todas as solicitações deverão ocorrer, por meio da interface web site (portal do cliente) segura através de sistema próprio e que contenha as seguintes características:

6.1.20.2.1. Módulos de incidente/solicitação, requisição de mudança, eventos, problemas, ICs, Contratos, Clientes, Fornecedores, Empresas, SLA's, Criticidades, Analistas, Base de conhecimento, Usuários e Avisos;

6.1.20.2.2. Realizar notificações por e-mail;

6.1.20.2.3. Catálogo de Serviços;

6.1.20.2.4. Integração com a ferramenta de monitoramento;

6.1.20.3. A ferramenta de Service Desk da CONTRATADA permitirá o acompanhamento dos chamados em aberto bem como a consulta dos chamados já finalizados (BASE HISTÓRICA DE INCIDENTES) e validação do chamado antes do encerramento do mesmo;

6.1.20.4. As solicitações de serviço, sejam de suporte ou consultoria, só poderão ser realizadas pelos contatos cadastrados, através dos métodos abaixo, em qualquer horário:

6.1.20.4.1. Ferramenta de service desk web;

6.1.20.4.2. E-mail;

6.1.20.4.3. Telefone.

**Horário de atendimento**

6.1.21. O serviço deverá ser disponibilizado 24 horas por dia, 7 dias por semana e 365 dias do ano (24x7x365), durante toda a vigência do contrato.

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

**Acompanhamento do Contrato**

6.1.22. Os serviços executados pela CONTRATADA estarão sujeitos à aceitação pela CONTRATANTE, mediante aferição dos correspondentes entregáveis, visando garantir que os mesmos satisfizeram os prazos e condições o padrão de qualidade exigido, considerando as disposições contidas neste Termo de Referência;

6.1.23. Na ocasião da apresentação do prestador de serviço, os Fiscais designados para acompanhar o contrato deverão prover a verificação da conformidade da documentação apresentada às normas do CONTRATANTE e às exigências do Termo de Referência;

6.1.24. Na ocasião do recebimento dos entregáveis, os seguintes procedimentos serão realizados pelos Fiscais designados para acompanhar o contrato:

6.1.24.1. Recebimento dos entregáveis através do preenchimento do Termo de Recebimento Provisório e entrega ao preposto da CONTRATADA;

6.1.24.2. Verificação do cumprimento da qualidade esperada na prestação dos serviços no período de referência, em conformidade com os Níveis Mínimos de Serviço (NMS) definido neste Termo de Referência;

6.1.24.3. Preenchimento do Termo de Recebimento Definitivo e da Autorização para Emissão de Nota Fiscal/Fatura e entrega a CONTRATADA;

6.1.25. O Relatório Mensal de Execução de Serviços, emitido pela CONTRATADA, deverá conter informações completas sobre os serviços prestados, incluindo no mínimo:

6.1.25.1. A situação atualizada do projeto de implantação;

6.1.25.2. As atividades realizadas no período de referência juntamente com o acumulado de atividades já realizadas;

6.1.25.3. As atividades previstas, mas não realizadas no período de referência juntamente com a descrição detalhada sobre as causas do não cumprimento do cronograma previsto;

6.1.25.4. Dificuldades encontradas e o plano de ação utilizado para solução;

6.1.25.5. Cronograma atualizado contendo prazos estimados e realizados para cada uma das atividades;

6.1.25.6. A avaliação do nível mínimo de serviço atingido e plano de ação para melhoria da qualidade;

6.1.25.7. Informações detalhadas sobre o desempenho e os serviços executados para análise gerencial;

6.1.25.8. Informações dos projetos e contratações em que houve o seu apoio técnico;

6.1.26. A Equipe de Gestão da Contratação elaborará documento interno obrigatório de acompanhamento mensal do contrato para registro de ocorrências durante a execução de um contrato, onde será avaliado o desempenho da CONTRATADA no que tange aos serviços prestados;

6.1.27. O documento interno obrigatório de acompanhamento mensal do contrato deverá fazer parte do correspondente processo de pagamento das faturas;

6.1.28. A Equipe de Gestão da Contratação exercerá a fiscalização permanente sobre a qualidade dos serviços prestados e atuação da CONTRATADA, inclusive quanto ao cumprimento da legislação, apontando todas as irregularidades verificadas, sem prejuízo da obrigação da CONTRATADA de gerenciar, por meio de seu preposto, a execução prestada por seus subordinados, dentro do critério de

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

periodicidade que entender como necessário ao cumprimento de suas responsabilidades;

6.1.29. Os casos omissos serão resolvidos pela CONTRATANTE, com base no Regulamento de Licitações e Contratações do SEHAC (Portaria n° 009 de 04/12/2008 e suas posteriores alterações), e, subsidiariamente, em outras leis aplicáveis ao tema em questão.

**Níveis mínimos de serviço (NMS)**

6.1.30. Características Gerais

6.1.30.1. Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, como a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança;

~~6.1.30.2. Os serviços serão medidos e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela do item **Erro! Fonte de referência não encontrada.**;~~

6.1.30.3. Serão aplicadas glosas, sob forma de desconto, à CONTRATADA referentes a falhas nos serviços executados ou em sua infraestrutura, que afetem a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança dos serviços, quando a responsabilidade for da CONTRATADA;

6.1.30.4. A aplicação de glosa pelo não atendimento aos Índices de Mediação de Resultado (IMR), onde se aplicar, poderá ser objeto de contestação, por meio do oferecimento de elementos que visem comprovar a não responsabilidade, por parte da CONTRATADA;

6.1.30.5. O valor do desconto, decorrente das glosas descritas nesta seção, e detectadas, conforme disposto neste Termo de Referência, deverá ser concedido na fatura do mês de referência da prestação do serviço, em que foi identificado o não atendimento aos níveis de qualidade de serviço determinados neste Termo;

6.1.30.6. O faturamento somente poderá ser emitido pela CONTRATADA e atestado pelo fiscal do contrato, após a aferição dos descontos a serem concedidos, decorrentes das glosas aplicadas, os quais deverão ser lançados na fatura do mês de prestação do serviço onde foram detectadas as ocorrências que ensejaram o não atendimento aos níveis de qualidade de serviço determinados neste Termo;

6.1.30.7. A qualidade da execução do objeto contratado será avaliada por de Níveis Mínimos de Serviço (NMS), que indicarão a faixa de ajuste no pagamento, de modo que o CONTRATANTE pague apenas pelo que efetivamente lhe foi entregue;

~~6.1.30.8. O NMS é composto de indicadores objetivos indicados no item **Erro! Fonte de referência não encontrada.**;~~

6.1.30.9. As glosas decorrentes das faixas de ajustes oriundas dos indicadores aferidos que compõem Índice de Medição de Resultado (IMR) não configuram sanção;

6.1.30.10. As glosas não ultrapassarão 10% (dez por cento) do valor mensal do serviço;

6.1.30.11. Independentemente da glosa aplicada, poderá ser aberto procedimento apuratório para aplicação de sanção mediante justificativa fundada em prejuízos ou transtornos causados em decorrência da entrega imperfeita do objeto contratado.

6.1.31. Nível Mínimo de Serviço para início do atendimento

6.1.31.1. Criticidade Alta: Início de atendimento em até 02 (duas) horas.

6.1.31.2. Criticidade Média: Início de atendimento em até 04 (quatro) horas.

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

6.1.31.3. Criticidade Baixa: Início de atendimento em até 08 (oito) horas.

**Equipe técnica e Capacitação dos Profissionais**

6.1.32. A CONTRATADA é responsável por dimensionar e manter equipe técnica em quantitativo e capacitação compatíveis com a prestação de serviço, a fim de garantir que as atividades sejam executadas dentro dos NMS e sem qualquer interrupção, independentemente de ocorrências de férias, descansos semanais, licenças, greves, paralisações do transporte público, faltas ao serviço e desligamentos de empregados;

6.1.33. Recomenda-se que a equipe conte com profissionais com habilidade de comunicação na língua inglesa, para leitura, escrita e conversação, tendo em vista frequentemente ser o idioma padrão em manuais, fóruns de dúvidas, bases de conhecimento e canais de atendimento de fabricantes;

6.1.34. A CONTRATADA deve prever e substituir imediatamente qualquer profissional por outro de mesmo perfil no caso de falta, impedimentos, férias e outras questões trabalhistas;

6.1.35. A CONTRATADA deve retirar dos serviços qualquer colaborador que, a critério da CONTRATANTE, seja julgado inconveniente ao bom andamento dos trabalhos;

6.1.36. A fim de garantir a prestação do serviço em conformidade com o framework ITIL, a CONTRATADA deve possuir ao menos um profissional com a certificação ITIL Foundation;

6.1.37. A fim de garantir a condução do projeto de acordo com as melhores práticas do mercado, a CONTRATADA deve possuir ao menos um profissional pós-graduado em Gerência de Projetos ou com a certificação PMI PMP;

6.1.38. A fim de garantir o conhecimento generalista em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação CISSP. Alternativamente, será aceita a certificação CISM;

6.1.39. A fim de garantir o conhecimento técnico em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação Security+;

6.1.40. A fim de garantir a existência de profissional com experiência de hacker ético, fundamental em momentos de crise de segurança, a CONTRATADA deve possuir ao menos um profissional com a certificação CEH, OSCP ou equivalente.

6.1.41. A CONTRATADA deverá apresentar, na fase de HABILITAÇÃO, a lista dos profissionais com seus currículos e a comprovação da exigência de certificação acima, suas responsabilidades em cada etapa (exemplo: testes externos, testes internos, análise de aplicações web), e, por fim, a comprovação de seu vínculo empregatício com a CONTRATADA.

**Implantação, mudanças e adoção tecnológica**

6.1.42. A CONTRATADA deve executar no **prazo máximo de 60 dias**, a contar da data do memorando de início, as atividades de planejamento, instalação/adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, em conformidade com este Termo de Referência;

6.1.43. Todas as atividades e documentação apresentadas deverão ser previamente aprovadas pela CONTRATANTE.

6.1.44. É responsabilidade da CONTRATADA o levantamento, junto à CONTRATANTE, de todas as informações necessárias para implantação/adoção dos itens de

Serviço Social Autônomo
Hospital Alcides Carneiro



serviço, incluindo topologia e configuração atual, processos de trabalho em execução e locais de execução dos serviços.

6.1.45. É de responsabilidade da CONTRATANTE fornecer todas as informações necessárias do seu ambiente tecnológico.

6.1.46. Após a ativação dos serviços, deve ser entregue a CONTRATANTE documentação de as-built de cada serviço, contendo, no mínimo, as seguintes informações:

6.1.46.1. Descrição dos serviços implantados;

6.1.46.2. Descrição da topologia física, após a ativação dos serviços, dos ambientes onde estão hospedados os equipamentos, softwares e soluções entregues pela CONTRATADA;

6.1.46.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

6.1.46.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

6.1.46.5. Definição de responsabilidades;

6.1.46.6. Recursos de alta disponibilidade;

6.1.46.7. Procedimentos para abertura e atendimento a chamados;

6.1.46.8. Procedimentos de recuperação de equipamentos;

6.1.46.9. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

6.1.46.10. Rotinas periódicas configuradas;

6.1.46.11. Documentação dos processos de trabalho associados ao item;

6.1.46.12. Desenho dos racks onde estão instalados os equipamentos;

6.1.46.13. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos).

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

6.1.47.1. O Assessment de Segurança e o GAP Analysis deverá ser realizado utilizando como base um dos seguintes frameworks de segurança: NIST ou CIS, devendo o planejamento ser antecipadamente aprovado pela CONTRATANTE;

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

6.1.48. A CONTRATADA deverá seguir o processo de mudança estabelecido pela CONTRATANTE;

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

6.1.50. A CONTRATADA, sempre que solicitada, deverá estar disponível para participar das reuniões internas da CONTRATANTE para prestar informações sobre os ambientes e serviços por ela executados;

Serviço Social Autônomo
Hospital Alcides Carneiro



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

6.1.52. A CONTRATADA deverá apresentar ao CONTRATANTE o planejamento de quaisquer mudanças no ambiente, conforme níveis de controle estabelecidos, para todas as mudanças apresentadas;

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

6.1.54. Caso alguma solução ofertada utilize SGBD – Sistema Gerenciador de Bancos de Dados, este deverá ser informado detalhado e fornecido como bundle, ou seja, já embutido no custo da solução.

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

**Requisitos de Segurança da CONTRATADA.**

6.1.56. Respeitar os critérios de sigilo, aplicáveis aos dados, informações e às regras de negócios relacionados com a prestação do serviço contratado;

6.1.57. Todas as informações transmitidas pela CONTRATANTE para a CONTRATADA e aos seus funcionários são de caráter confidencial e não poderão ser transmitidas ou facilitadas a quem quer que seja, sem expressa autorização do CONTRATANTE;

6.1.58. Deverá ser mantida a confidencialidade das informações obtidas em razão da execução do contrato.

**Ferramentas fornecidas**

6.1.59. Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.

6.1.60. Todas as ferramentas fornecidas como parte das soluções devem contar com serviços plenos de sustentação, conforme a seguir.

6.1.61. A sustentação, administração, operação, suporte técnico e atualização das Soluções informatizadas fornecidas pela CONTRATADA, bem como qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos, serão serviços de natureza continuadade responsabilidade da CONTRATADA;

6.1.62. Todas as Soluções Informatizadas devem possuir os serviços de licenciamento ou subscrição, garantia, suporte técnico e atualização oficiais do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços envolvidos, que devem estar contratados e disponíveis a partir da implantação da respectiva solução e durante toda a vigência do contrato;

6.1.63. As Soluções Informatizadas devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato;

6.1.64. As Soluções Informatizadas não podem constar, no momento da apresentação da proposta comercial, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, e não podem ter previsão de descontinuidade de fornecimento, suporte ou vida pelo menos até o fim da vigência prevista para o contrato;

Serviço Social Autônomo
Hospital Alcides Carneiro



6.1.65. As Soluções Informatizadas devem ser instaladas em sua versão mais estável e atualizada;

6.1.66. A CONTRATADA deverá cumprir todos os termos e condições do contrato de licenciamento dos respectivos fabricantes das Soluções Informatizadas, cuidando do adequado dimensionamento quantitativo e qualitativo das licenças necessárias para a prestação dos serviços e aderência ao ambiente da CONTRATANTE, mantendo a conformidade com os direitos depropriedade intelectual;

6.1.67. A CONTRATADA deve comprovar, na contratação e durante toda a vigência do contrato, que tenha, junto ao fabricante de cada ferramenta das Soluções informatizadas, amplo e irrestrito acesso aos recursos e serviços de apoio técnico bem como à plenitude de capacidades e efetividade da ferramenta, prestados diretamente pelo fabricante, como centros elaboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis;

6.1.68. A CONTRATADA assegurará garantia integral e perfeito funcionamento das Soluções Informatizadas pelo período de vigência do contrato.

**Serviço gerenciado de segurança**

6.1.69. Monitoramento das Soluções Gerenciadas

6.1.69.1. Monitorar o ambiente 24x7x365, quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser gerenciada;

6.1.69.2. Fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);

6.1.69.3. Acompanhamento completo dos incidentes de segurança, performance e disponibilidade;

6.1.69.4. Realizar a monitoração de performance e disponibilidade dos ativos;

6.1.69.5. Realizar o acionamento por matriz de escalação hierárquica e funcional, para eventos de segurança, performance e disponibilidade.

6.1.70. Suporte especializado

6.1.70.1. Quanto ao suporte especializado a CONTRATADA deve:

6.1.70.1.1. Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente) e telefone (0800) no regime 24x7x365, com atendimento bilíngue (português e inglês);

6.1.70.1.2. Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;

6.1.70.1.3. Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;

6.1.70.1.4. Possuir análise técnica documentada pelo N3 do SOC antes do envolvimento dos fabricantes, a fim de garantir o processo de escalação funcional.

6.1.70.1.5. Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;

6.1.70.1.6. Os administradores de tecnologia do CONTRATANTE terão total acesso à plataforma para fins de auditoria, porém a responsabilidade pela operação diária da solução será da CONTRATADA.

6.1.71. Atuação preventiva

Serviço Social Autônomo
Hospital Alcides Carneiro



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

6.1.71.1.1. Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;

6.1.71.1.2. Propor ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, as mantendo documentadas;

6.1.71.1.3. Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste edital, as mantendo documentadas e acessíveis no portal do cliente;

6.1.71.1.4. Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE;

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

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

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

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

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

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

6.1.71.1.11. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

6.1.71.1.12. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

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

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

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

6.1.71.1.16. Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação.

6.1.72. Escopo

6.1.72.1. O serviço gerenciado de segurança deverá contemplar todas as tecnologias entregues pela contratada;

Serviço Social Autônomo
Hospital Alcides Carneiro



6.1.72.2. Seu custo deverá ser contemplado nas respectivas linhas de serviço.

## 7. Proteção de estações de trabalho

**A ferramenta utilizada para o serviço de proteção de estações de trabalho deverá possuir, no mínimo, as seguintes características:**

**Características gerais**

7.1.1. Características básicas do agente de proteção contra malwares:

7.1.2. Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

7.1.3. O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

7.1.4. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

7.1.5. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

7.1.6. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

7.1.7. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

7.1.8. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

7.1.9. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

7.1.10. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

7.1.11. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

7.1.12. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

7.1.13. Suportar máquinas com arquitetura 32-bit e 64-bit, (Exceto para Windows 11 que não há opção de 32bits;

7.1.14. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, 12 Monterey, 13 Ventura, 14 Sonoma, Microsoft Windows 7, 8.1, 10 e 11;

7.1.15. A solução deve ser compatível com a execução nativa em processadores Apple Silicon, não serão aceitas soluções que dependem de emulação via Rosetta2 da Apple.

7.1.16. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

7.1.17. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

**Firewall e detecção e proteção de intrusão (IDS\IPS)**

7.1.18. Deverá possui atualização periódica de novas assinaturas de ataque;

7.1.19. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

7.1.20. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

7.1.21. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

7.1.22. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

7.1.23. Deve possuir técnicas de proteção, que inclui:

7.1.24. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

7.1.25. Algorítimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

7.1.26. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

7.1.27. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

7.1.28. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

**Antivírus e antispyware**

7.1.29. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

7.1.30. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

7.1.31. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

7.1.32. Permitir a configuração de ações diferenciadas para programas potencialmente

Serviço Social Autônomo
Hospital Alcides Carneiro



indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

7.1.33. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

7.1.34. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

7.1.35. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

7.1.36. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

7.1.37. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

7.1.38. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

7.1.39. Antivírus de Web (verificação de sites e downloads contra vírus);

7.1.40. Controle de acesso a sites por categoria;

7.1.41. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

7.1.42. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

7.1.43. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

7.1.44. Capacidade de verificar somente arquivos novos e alterados;

7.1.45. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

**Detecção proativa de reconhecimento de novas ameaças**

7.1.46. Funcionalidade de detecção de ameaças via técnicas de machine learning;

7.1.47. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

7.1.48. Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

7.1.49. Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

7.1.50. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

**Proteção contra ransomwares**

7.1.51. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

7.1.52. Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

7.1.53. Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

7.1.54. A solução deverá prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

7.1.55. Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

7.1.56. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

7.1.56.1. DEP (Data Execution Prevention);

7.1.56.2. Address Space Layout Randomization (ASLR);

7.1.56.3. Bottom Up ASLR;

7.1.56.4. Null Page;

7.1.56.5. Anti-HeapSpraying;

7.1.56.6. Dynamic Heap Spray;

7.1.56.7. Import Address Table Filtering (IAF);

7.1.56.8. VTable Hijacking;

7.1.56.9. Stack Pivot and Stack Exec;

7.1.56.10. SEHOP;

7.1.56.11. Stack-based ROP (Return-Oriented Programming);

7.1.56.12. Control-Flow Integrity (CFI);

7.1.56.13. Syscall;

7.1.56.14. WOW64;

7.1.56.15. Load Library;

7.1.56.16. Shellcode;

7.1.56.17. VBScript God Mode;

7.1.56.18. Application Lockdown;

7.1.56.19. Process Protection;

7.1.56.20. Network Lockdown.

Serviço Social Autônomo
Hospital Alcides Carneiro



7.1.57. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

7.1.58. Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

7.1.59. A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

7.1.60. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

**Endpoint detection and response (EDR)**

7.1.61. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

7.1.62. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

7.1.63. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

7.1.64. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

7.1.64.1. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

7.1.64.2. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

7.1.64.3. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

7.1.64.4. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

7.1.65. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

7.1.66. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

7.1.67. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

7.1.68. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

7.1.69. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

Serviço Social Autônomo
Hospital Alcides Carneiro



7.1.70. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

7.1.71. Deve possibilizar o agendamento de consultas (queries);

7.1.72. Deve reter os dados no Data Lake por no mínimo 7 dias.

**Controle de aplicações e dispositivos**

7.1.73. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

7.1.74. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

7.1.75. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

7.1.76. Oferecer proteção para chaves de registro e controle de processos;

7.1.77. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

7.1.78. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

7.1.79. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

7.1.80. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

7.1.81. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

7.1.82. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

7.1.83. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

7.1.84. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

7.1.85. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

7.1.85.1. Permitir que todos os dispositivos do mesmo modelo;

7.1.85.2. Permitir que um único dispositivo com base em seu número de identificação único;

7.1.85.3. Permitir o acesso total;

7.1.85.4. Permitir acesso somente leitura;

7.1.85.5. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

**Proteção e prevenção a perda de dados**

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

7.1.86. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

7.1.87. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

7.1.88. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

7.1.89. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

7.1.89.1. Números de cartões de crédito;

7.1.89.2. Números de contas bancárias;

7.1.89.3. Números de Passaportes;

7.1.89.4. Endereços;

7.1.89.5. Números de telefone;

7.1.89.6. Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

7.1.89.7. Lista de e-mails;

7.1.89.8. Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

7.1.90. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

7.1.91. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

7.1.92. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

7.1.93. Permitir o controle de dados para no mínimo os seguintes meios:

7.1.93.1. Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

7.1.93.2. Anexado no navegador (ao menos IE, Firefox e Chrome);

7.1.93.3. Anexado no cliente de mensagens instantâneas (ao menos Skype);

7.1.93.4. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

## 8. Proteção de servidores

**A ferramenta utilizada para o serviço de proteção de servidores deverá possuir, no mínimo, as seguintes características:**

### Características Gerais

8.1.1. Características básicas do agente de proteção contra malwares:

8.1.1.1. A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

8.1.1.2. Deve realizar a pré-execução do agente para verificar o comportamento

Serviço Social Autônomo
Hospital Alcides Carneiro



malicioso e detectar malwares desconhecidos;

8.1.1.3. O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

8.1.1.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

8.1.1.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

8.1.1.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

8.1.1.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

8.1.1.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

8.1.1.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

8.1.1.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

8.1.1.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

8.1.1.12. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:

8.1.1.12.1. Windows Server 2016;

8.1.1.12.2. Windows Server 2012 R2 (64 bits);

8.1.1.12.3. Windows Server 2012 (64 bits);

8.1.1.12.4. Amazon Linux;

8.1.1.12.5. Amazon Linux 2;

8.1.1.12.6. CentOS 7;

8.1.1.12.7. Debian 10;

8.1.1.12.8. Oracle Linux 7;

8.1.1.12.9. Oracle Linux 8;

8.1.1.12.10. Red Hat Enterprise 7;

8.1.1.12.11. Red Hat Enterprise 8;

8.1.1.12.12. Red Hat Enterprise 9;

8.1.1.12.13. SUSE Linux Enterprise Server 12;

8.1.1.12.14. SUSE Linux Enterprise Server 15;

8.1.1.12.15. Ubuntu 20.04 LTS;

8.1.1.12.16. Ubuntu 22.04 LTS;

8.1.1.13. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

8.1.1.14. Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

Serviço Social Autônomo
Hospital Alcides Carneiro



8.1.1.15. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

8.1.1.16. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

8.1.1.17. Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Platform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

8.1.1.18. A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

8.1.1.18.1. Escalação de privilégios dentro de containers;

8.1.1.18.2. Programas utilizando técnicas de mineração de criptomoedas;

8.1.1.18.3. Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

8.1.1.18.4. Detecção de funções internas do kernel que estão sendo adulteradas em um host;

8.1.1.19. A solução deve também se integrar à tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas,

8.1.1.20. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

8.1.1.20.1. Possuir proteção contra exploração de buffer overflow;

8.1.1.20.2. Deverá possui atualização periódica de novas assinaturas de ataque;

8.1.1.20.3. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

8.1.1.20.4. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

8.1.1.20.5. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

8.1.1.20.6. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

8.1.1.20.7. Deve possuir técnicas de proteção, que inclui:

8.1.1.20.7.1. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

8.1.1.20.7.2. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

8.1.1.20.7.3. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

8.1.1.20.7.4. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt)

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

8.1.1.20.7.5. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

**Antivírus e AntiSpyware**

8.1.2. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

8.1.3. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

8.1.4. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

8.1.5. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

8.1.6. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

8.1.7. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

8.1.8. Capacidade de detectar arquivos através da reputação dos mesmos;

8.1.9. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

8.1.10. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

8.1.11. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

8.1.12. Deverá detectar tráfego de rede para comandar e controlar os servidores;

8.1.13. Proteger arquivos de documento contra ataques do tipo ransomwares;

8.1.14. Proteger que o ataque de ransomware seja executado remotamente;

8.1.15. Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

8.1.16. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

8.1.17. Antivírus de Web (verificação de sites e downloads contra vírus);

8.1.18. Controle de acesso a sites por categoria;

8.1.19. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

8.1.20. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

8.1.21. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

8.1.22. Capacidade de verificar somente arquivos novos e alterados;

8.1.23. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

8.1.24. Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

8.1.25. Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

**Proteção contra ransomwares**

8.1.26. Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

8.1.27. Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

8.1.28. Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

**Controle de aplicações e dispositivos**

8.1.29. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

8.1.30. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

8.1.31. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

8.1.32. Oferecer proteção para chaves de registro e controle de processos;

8.1.33. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

8.1.34. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

8.1.35. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

8.1.36. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

leitura/escrita/execução do conteúdo desses dispositivos;

8.1.37. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

8.1.38. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

8.1.39. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

8.1.40. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

8.1.41. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

8.1.41.1. Permitir que todos os dispositivos do mesmo modelo;

8.1.41.2. Permitir que um único dispositivo com base em seu número de identificação único;

8.1.41.3. Permitir o acesso total;

8.1.41.4. Permitir acesso somente leitura;

8.1.41.5. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

**Proteção e prevenção a perda de dados**

8.1.42. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

8.1.43. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

8.1.44. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

8.1.45. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

8.1.45.1. Números de cartões de crédito;

8.1.45.2. Números de contas bancárias;

8.1.45.3. Números de Passaportes;

8.1.45.4. Endereços;

8.1.45.5. Números de telefone;

8.1.45.6. Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

8.1.45.7. Lista de e-mails;

8.1.45.8. Informações pessoais, corporativas e financeiras referentes especificamente ao

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

8.1.46. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

8.1.47. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

8.1.48. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

8.1.49. Permitir o controle de dados para no mínimo os seguintes meios:

8.1.49.1. Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

8.1.49.2. Anexado no navegador (ao menos IE, Firefox e Chrome);

8.1.49.3. Anexado no cliente de mensagens instantâneas (ao menos Skype);

8.1.49.4. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

**Endpoint Detection and Response (EDR)**

8.1.50. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

8.1.51. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

8.1.52. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

8.1.53. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

8.1.53.1. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

8.1.53.2. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

8.1.53.3. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

8.1.53.4. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

8.1.54. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

8.1.55. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

8.1.56. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

8.1.57. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

8.1.58. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de

Serviço Social Autônomo
Hospital Alcides Carneiro



buscar por hash, nome, endereços IP, domínio ou linha de comando;

8.1.59. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

8.1.60. Deve possibilizar o agendamento de consultas;

8.1.61. Deve reter os dados no Data Lake por no mínimo 7 dias.

8.1.62. Deve dispor de proteção Adaptativa contra Ataques;

8.1.63. Deve prover aviso de ataque crítico;

8.1.64. Deve possuir de proteção no modo seguro do Windows.

8.1.65. Deve possuir a opção de bloqueio do protocolo QUIC

**Detecção e resposta estendida (XDR)**

8.1.66. Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

8.1.67. Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

8.1.68. Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

8.1.69. Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

8.1.70. Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

8.1.71. Deve possuir sensores que fornecem telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em toda o ambiente da organização;

8.1.72. Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

8.1.73. Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

8.1.74. Deve reter os dados no Data Lake por no mínimo 30 dias.

8.1.75. O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

8.1.76. A console do XDR deve correlacionar os dados recebidos e armazenados no DataLake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

8.1.77. Tais detecções e evidencias devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

8.1.78. Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do DataLake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade

SEHAC SUS
Serviço Social Autônomo
Hospital Alcides Carneiro


do ataque presente na console;

8.1.79. Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

8.1.80. A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação;

8.1.81. Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação;

8.1.82. Integrações

8.1.82.1. Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do próprio fabricante, podendo ser entregue via appliance virtual compatível com ESXI e Hyper-v minimamente ou Hardware próprio, não sendo aceito equipamentos do tipo PC;

8.1.82.2. Deve ser compatível com integrações de terceiros com as seguintes categorias com no mínimo os seguintes fabricantes:

8.1.82.2.1. Firewalls:

8.1.82.2.1.1. Check Point;

8.1.82.2.1.2. Palo Alto;

8.1.82.2.1.3. Fortinet;

8.1.82.2.1.4. Cisco;

8.1.82.2.1.5. SonicWall

8.1.82.2.2. Endpoints:

8.1.82.2.2.1. Microsoft;

8.1.82.2.2.2. Crowdstrike;

8.1.82.2.2.3. McAfee;

8.1.82.2.2.4. SentinelOne;

8.1.82.2.2.5. Check Point;

8.1.82.2.2.6. Trend Micro;

8.1.82.2.2.7. Malwarebytes;

8.1.82.2.2.8. BlackBerry

8.1.82.2.2.9. Palo Alto Cortex XDR

8.1.82.2.3. Provedores de identidade

8.1.82.2.3.1. Microsoft Azure IDP, ATA;

8.1.82.2.3.2. Okta;

8.1.82.2.3.3. Duo

8.1.82.2.4. Plataformas de e-mails

8.1.82.2.4.1. Microsoft 365;

8.1.82.2.4.2. Mimecast;

8.1.82.2.4.3. Proofpoint

8.1.82.2.5. Cloud SaaS

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

8.1.82.2.5.1. AWS;

8.1.82.2.5.2. Azure;

8.1.82.2.5.3. Google Cloud;

8.1.82.2.5.4. Orca Security;

8.1.82.2.5.5. Prisma Cloud

8.1.82.2.6. Network

8.1.82.2.6.1. Darktrace;

8.1.82.2.6.2. Forcepoint

8.1.82.3. As integrações de terceiros poderão ser via API ou envio de Syslogs

8.1.83. A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema do tipo .OVA para uso em virtualizador;

8.1.84. O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados, para eventuais consultas;

## 9. Gestão de incidentes

### 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.

9.1.1. Nesse sentido, são papéis da CONTRATADA:

9.1.1.1. 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;

9.1.1.2. O ambiente a ser monitorado possui até 250 (duzentos e cinquenta) ativos, incluindo servidores, roteadores, switches, entre outros.

9.1.1.3. Gerir os incidentes (criação de alertas, detecção e abertura de chamados);

9.1.1.4. Acompanhar do início ao fim os incidentes;

9.1.1.5. Realizar o acionamento por matriz de escalação hierárquica e funcional, para os incidentes;

9.1.1.6. 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;

9.1.1.7. Acompanhar os processos através de indicadores de desempenho.

### Detecção e resposta

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

9.1.2.1. Tipo de incidente;

9.1.2.2. Ações a serem realizadas;

9.1.2.3. Responsáveis pela execução das ações, incluindo nome, telefone e e-mail.

9.1.3. A solução ofertada deve contemplar, de forma integrada e nativa, minimamente os seguintes mecanismos de detecção de incidentes

9.1.3.1. Correlacionamento de eventos (SIEM);

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

9.1.3.2. Análise comportamental de usuários (UEBA);

9.1.3.3. Detecção e Reposta de Rede (NDR);

9.1.3.4. Detecção de intrusão (IDS);

9.1.3.5. Malware Sandbox;

9.1.4. A solução ofertada deve permitir o Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana;

9.1.5. 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;

9.1.6. A CONTRATADA deve prover a proposta de contenção, erradicação e recuperação, articulação com as equipes do CONTRATANTE, controle de ações, notificações e escalonamento dos incidentes.

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

9.1.8. 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.

9.1.9. Os referidos artigos de conhecimento devem ser transferidos para o CONTRATANTE.

9.1.10. Para tal, a CONTRATADA deverá fazer uso de uma plataforma unificada para Detecção e Resposta Estendida com as seguintes características e especificações:

9.1.10.1. Quanto às suas características gerais, a solução ofertada deverá:

9.1.10.1.1. Possuir diversas funcionalidades de segurança que irão prover a capacidade de detecção e resposta aos incidentes de segurança, através do modelo da Cadeia de Ataque (Kill Chain) automaticamente, contando com, pelo menos, os seguintes componentes:

9.1.10.1.1.1. Gerenciamento e correlação de eventos (SIEM);

9.1.10.1.1.2. Orquestração e automação de respostas aos incidentes (SOAR);

9.1.10.1.1.3. Análise do comportamento do usuário (UEBA);

9.1.10.1.1.4. Detecção e Resposta na Rede (NDR);

9.1.10.1.1.5. Sistema de detecção de intrusão (IDS);

9.1.10.1.1.6. Malware Sandbox;

9.1.10.1.1.7. Inteligência de Ameaças (Threat Intelligence).

9.1.10.1.2. Gerenciar todos os componentes solicitados através de uma única interface gráfica Web, permitindo o gerenciamento centralizado de toda a solução;

9.1.10.1.3. Ser hospedada na nuvem do fabricante, com leitura de dados próprios para

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

correlação de eventos de atividades maliciosas;

9.1.10.1.4. Ser implantada de forma transparente através de sensores para fazer a coleta de informações, logs e telemetria;

9.1.10.1.5. Rastrear e detectar ameaças em qualquer fonte ou local dentro da CONTRATANTE, incluindo, mas não se limitando a:

9.1.10.1.5.1. Redes;

9.1.10.1.5.2. Servidores (físicos e virtuais);

9.1.10.1.5.3. Aplicações;

9.1.10.1.5.4. Nuvens públicas e privadas.

9.1.10.1.6. Permitir o inventário dos ativos presentes na rede, por endereços IP e o nível de risco desses ativos, contando com detalhes e evidências disso sem a necessidade de executar varreduras de rede para este fim;

9.1.10.1.7. Possuirnativamente a capacidade de correlacionar vulnerabilidades relatadas por ferramentas de terceiros, com assinaturas de ataque identificadas e exibi-las em um painel de controle a partir dos quais os relatórios são gerados;

9.1.10.1.8. Possuir mecanismos de controle de acesso e autenticação, baseado em função, para que apenas as pessoas autorizadas pela CONTRATANTE tenham acesso às informações;

9.1.10.1.8.1. Ser capaz de se integrar com métodos de autenticação via Active Directory e LDAP.

9.1.10.1.9. Priorizar o risco e as atividades de operação de segurança;

9.1.10.1.10. Prover toda a comunicação entre os componentes de forma criptografada;

9.1.10.1.11. Incluir mecanismos de sincronização, como NTP (Network Time Protocol) e, assim, garantir a sincronização correta das informações;

9.1.10.1.12. Possibilitar a auditoria sobre o status das ações tomadas ou pendentes.

9.1.10.2. Quanto ao modelo de licenciamento, a solução ofertada deverá:

9.1.10.2.1. Permitir o recebimento ilimitado de eventos, tendo a capacidade de operar acima do estimado inicialmente sem perder qualquer funcionalidade/capacidade de indexação;

9.1.10.2.2. Permitir a análise do tráfego de rede completo da CONTRATADA.

9.1.10.3. Quanto ao armazenamento de logs e eventos, a solução ofertada deverá:

9.1.10.3.1. Armazenar, na própria solução, as informações do tráfego de rede e dos Logs durante o período, mínimo, de 30 dias, bem como o registro dos incidentes gerados pela plataforma durante o período de 365 dias;

9.1.10.3.2. Permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados:

9.1.10.3.2.1. Dados de eventos de segurança;

9.1.10.3.2.2. Dados das aplicações;

9.1.10.3.2.3. Dados dos sistemas operacionais;

9.1.10.3.2.4. Dados das nuvens públicas e privadas;

9.1.10.3.2.5. Dados do tráfego de rede;

9.1.10.3.2.6. Tráfego de registro (syslog).

9.1.10.4. Quanto à compatibilidade e integrações, a solução ofertada deverá:

Serviço Social Autônomo
Hospital Alcides Carneiro



9.1.10.4.1. Ser capaz de integrar-se às soluções de segurança terceiras presentes na rede, a fim de enriquecer a análise das informações coletadas e permitir ações adicionais de bloqueio contra-ataques cibernéticos;

9.1.10.4.2. Possuir uma API RESTful para integração com vários serviços para ingestão de logs, telemetria e tráfego para detecção e resposta a eventos de segurança;

9.1.10.4.3. Ser compatível com plataformas Windows e Linux;

9.1.10.4.4. Permitir a inspeção de plataformas como:

9.1.10.4.4.1. Amazon AWS;

9.1.10.4.4.2. Microsoft Azure;

9.1.10.4.4.3. Google G-Suite;

9.1.10.4.4.4. Microsoft Office 365;

9.1.10.4.4.5. Componentes virtuais (máquinas virtuais);

9.1.10.4.4.6. Box.

9.1.10.5. Quanto ao mecanismo degerenciamento e correlação de eventos (SIEM), a solução ofertada deverá:

9.1.10.5.1. Possuir a capacidade de realizar a coleta e a ingestão de logs de todos os componentes do ambiente tecnológico da CONTRATANTE, através do padrão syslog ou similar;

9.1.10.5.2. Correlacionar eventos, com o objetivo de identificar anomalias e incidentes automaticamente.

9.1.10.6. Quanto ao mecanismo dedetecção e resposta na rede (NDR), a solução deverá:

9.1.10.6.1. Analisar o tráfego TCP/UDP na rede da CONTRATANTE para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego;

9.1.10.6.2. Realizar o aprendizado do ambiente de rede e a inspeção do tráfego de forma off-line através de TAPs, providos pela CONTRATADA, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede;

9.1.10.6.3. Ter a capacidade de identificar ameaças no tráfego de rede e realizar o monitoramento proativo de forma automatizada de todo o tráfego passante na rede da CONTRATANTE, contemplando os seguintes critérios:

9.1.10.6.3.1. Utilização da largura de banda;

9.1.10.6.3.2. Tentativas de penetração e varreduras de IPs e portas;

9.1.10.6.3.3. Autenticações recusadas ou com falhas;

9.1.10.6.3.4. Ataques bem-sucedidos de autenticação de força bruta;

9.1.10.6.3.5. Presença de tráfego malicioso, como ransomware, movimentação lateral, cryptojacking, mimekatz, etc;

9.1.10.6.3.6. Análise de arquivos benignos e maliciosos e suas respectivas categorias;

9.1.10.6.3.7. Ataques de negação de serviço;

9.1.10.6.3.8. Conexões de comando e controle presentes, internamente ou de/para a Internet;

9.1.10.6.3.9. Dispositivos que representam o maior risco;

9.1.10.6.3.10. Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes);

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

9.1.10.6.3.11. Aplicações que consomem mais recursos de rede;

9.1.10.6.3.12. Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho);

9.1.10.6.3.13. Identificação das conexões e seu risco associado;

9.1.10.6.3.14. Uso dos servidores de banco de dados (Principais Queries, usuários, origem e destino e os detalhes de uso);

9.1.10.6.3.15. Identificação de aplicações da Camada 7;

9.1.10.6.3.16. Principais eventos críticos de segurança;

9.1.10.6.3.17. Tempo de resposta das aplicações;

9.1.10.6.3.18. Nos ambientes de virtualização cujo tráfego passa pela rede física monitorada, pelo menos as seguintes métricas devem ser obtidas:

- Eventos críticos de segurança identificados nos servidores virtualizados;
- As aplicações que são mais utilizados;
- Principais eventos de segurança entre máquinas virtuais;
- Risco associado entre máquinas virtuais.

9.1.10.6.3.19. A CONTRATANTE proverá os servidores necessários para a hospedagem desta tecnologia em seu ambiente.

9.1.10.7. Quanto a detecção dos incidentes, a solução ofertada deverá:

9.1.10.7.1. Ser capaz de detectar padrões de ataques sem a utilização de assinaturas, através da elaboração automatizada de um baseline comportamental dos usuários e entidades;

9.1.10.7.2. Possuir a capacidade de, via técnicas de Machine Learning, identificar anomalias nos comportamentos individuais dos usuários e entidades e de gerar alertas com relação, ao menos, aos seguintes casos de uso:

9.1.10.7.2.1. Horário atípico do acesso;

9.1.10.7.2.2. Número atípico de sessões de uso nos sistemas operacionais;

9.1.10.7.2.3. Volume de conexões atípico;

9.1.10.7.2.4. Volume de transferências de dados atípico;

9.1.10.7.2.5. Localização geográfica atípica da origem do acesso;

9.1.10.7.2.6. Endereço IP de origem atípico do acesso;

9.1.10.7.2.7. Acesso atípico a dados armazenados;

9.1.10.7.2.8. Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade;

9.1.10.7.2.9. Mudança na postura de risco do usuário/entidade.

9.1.10.7.3. Possuir mais de 150 modelos de detecção para casos de uso, como, no mínimo, Ransomware, Command & Control, DGA, Cryptojacking, phishing, scripts de power shell maliciosos, UBA e ataques de zero-day;

9.1.10.7.4. Permitir a criação de novas regras de detecção e alteração das regras existentes;

9.1.10.7.5. Emitir alertas quando eventos críticos de segurança forem detectados na rede e estes se desviarem de padrões estabelecidos (anomalias), por meio de análises detalhada de cada aplicativo em execução na rede de modo nativo, gerando chamados para a equipe do SOC, automaticamente, para a sua

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

atenção, atuação e documentação;

9.1.10.7.6. Permitir a geração de diagramas de conexões TCP mostrando como as ameaças estão associadas, bem como se movem no ambiente, baseado em capturas de tráfego, classificados e normalizadas automaticamente.

9.1.10.8. Quanto a resposta aos incidentes, a solução ofertada deverá:

9.1.10.8.1. Incluir uma solução integrada de gerenciamento de casos e incidentes;

9.1.10.8.2. Ter a capacidade de associar vários alertas recebidos a um único incidente que tem a capacidade de ser atribuído, ter uma linha do tempo, objetos associados, bem como as principais métricas MTTD e MTTR;

9.1.10.8.3. Ter a capacidade de enviar instruções de resposta através dos mesmos sensores de coleta;

9.1.10.8.4. Ter a capacidade de responder a todos os eventos de forma orquestrada e automatizada, integrando-se ao ambiente tecnológico da CONTRATANTE. As ações possíveis de resposta devem ser, pelo menos, as seguintes:

9.1.10.8.4.1. Enviar um e-mail;

9.1.10.8.4.2. Enviar mensagens para meios de comunicação do tipo SLACK;

9.1.10.8.4.3. Fazer um POST, GET ou um PUT para um servidor;

9.1.10.8.4.4. Criar regras de bloqueio no firewall;

9.1.10.8.4.5. Desabilitar usuários no Active Directory;

9.1.10.8.4.6. Executar scripts.

9.1.10.8.5. Contemplar uma ferramenta que permita a investigação e busca de ameaças, com o objetivo de identificar as ameaças presentes na rede e automatizar os eventos de segurança para responder a elas;

9.1.10.8.6. Ser capaz de realizar análise retrospectiva com base nos dados ingeridos e armazenados do tráfego TCP/UDP, apoiando uma análise forense.

9.1.10.9. Quanto aos relatórios e dashboards, a solução ofertada deverá:

9.1.10.9.1. Ter a capacidade de gerar relatórios executivo e operacionais, com base em modelos pré-configurados, personalizáveis, baseados em dashboards, incluindo, pelo menos, relatórios sobre o status atual dos dispositivos, seu risco associado e tendências;

9.1.10.9.2. Gerar informações detalhadas sobre os eventos detectados, incluindo ameaças, anomalias, comportamentos e tendências de rede associadas ao risco de rede;

9.1.10.9.3. Detalhar os gráficos para aprofundar as informações apresentadas (mecanismo conhecido como Drill Down);

9.1.10.9.4. Gerar KRI (Principais Indicadores de Risco), como o número de eventos gerados em um dia, semana ou meses e compará-los com um período semelhante, o mesmo com a criticidade média dos eventos;

9.1.10.9.5. Permitir ao pessoal designado a geração de relatórios explorando todas as variáveis e funcionalidades da ferramenta, com a opção de parametrizar esses relatórios e consultá-los via Web, bem como a criação de filtros personalizados para pesquisas de eventos específicos;

9.1.10.9.6. Fornecer painéis configuráveis que possam conter diferentes gráficos com informações de, pelo menos:

9.1.10.9.6.1. Eventos anômalos e críticos, incluindo:

- Detecções de segurança;

SEHAC SUS
Serviço Social Autônomo
Hospital Alcides Carneiro
Tecnologia da Informação

- IPs de Origem e Destino;
- Visão geral da atividade dos dispositivos (servidores e infraestrutura, física e virtualizada);
- Táticas e técnicas do MITRE ATT&CK;
- Fases do Kill Chain e os alertas associados.

9.1.10.9.6.2. Aplicações utilizadas e seus dados históricos, discriminada por:

- Risco associado;
- IP de Origem e Destino;
- Anomalias detectadas;
- Classificação de risco;
- Tráfego entre hosts.

9.1.10.9.6.3. Informações de em um Host:

- Aplicações utilizadas;
- Tráfego de e para o Host com base em detecções de segurança e anomalias.

9.1.10.9.6.4. Informações e o status das aplicações e serviços que estão sendo executados no data center, tais como:

- Quantidade e a gravidade das anomalias;
- Possíveis problemas de segurança no data center.

9.1.10.9.7. Permitir a criação de relatórios por período (hora, dia, semana, mês, ano, e personalizado por datas específicas);

9.1.10.9.8. Possuir filtros pós-captura, pelo menos para:

9.1.10.9.8.1. Filtro de erro;

9.1.10.9.8.2. Filtros por tráfego entre duas estações através da seleção do nome ou endereço IP;

9.1.10.9.8.3. Filtros por protocolos;

9.1.10.9.8.4. Geolocalização;

9.1.10.9.8.5. Gravidade;

9.1.10.9.8.6. Endereço IP.

9.1.10.9.9. Suportar diagnósticos nas diferentes camadas do modelo OSI, incluindo:

9.1.10.9.9.1. Análise das anomalias da rede da camada 2 à camada 7;

9.1.10.9.9.2. Endereços IP;

9.1.10.9.9.3. Aplicações e/ou portas (TCP/UDP);

9.1.10.9.9.4. Serviços associados;

9.1.10.9.9.5. Servidores mais lentos;

9.1.10.9.9.6. Origem e destino.

9.1.10.9.10. Ser capaz de gerar um gráfico das anomalias das aplicações dentro da rede, fornecendo resultados com pelo menos as seguintes variáveis:

9.1.10.9.10.1. Movimentos laterais;

9.1.10.9.10.2. Histórico de eventos;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

9.1.10.9.10.3. Anomalias de tráfego maliciosos;

9.1.10.9.10.4. Anomalias de políticas e negações de firewalls de infraestrutura;

9.1.10.9.10.5. Principais Aplicações;

9.1.10.9.10.6. Top Servidores;

9.1.10.9.10.7. Top Clientes;

9.1.10.9.10.8. Status das sessões atuais;

9.1.10.9.10.9. Origens e destinos de países com má reputação.

9.1.10.9.11. Exportar as informações dos pacotes capturados em metadados para análise posterior.

**Análise de causa raiz**

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

9.1.11.1. Os impactos observados;

9.1.11.2. A(s) vulnerabilidade(s) explorada(s);

9.1.11.3. O método de ataque;

9.1.11.4. A origem do ataque.

## 10. Deveres e responsabilidades

**Da CONTRATADA**

10.1.1. Responder pela frequência dos seus profissionais, exercendo o devido controle sobre a assiduidade e a pontualidade destes, garantindo a presença de pessoal suficiente para o cumprimento dos serviços;

10.1.2. Prestar os serviços nos locais, horários e de acordo com os parâmetros de qualidade estabelecidos neste Termo de Referência, de forma a assegurar plena eficácia na execução;

10.1.3. Observar rigorosamente todos os itens do Termo de Referência, inclusive seus anexos, executando os serviços de acordo com as especificações e normas aplicáveis, utilizando ferramental apropriado e dispondo de infraestrutura e equipe técnica, exigidas para a perfeita execução do objeto desta contratação;

10.1.4. Arcar com todos os encargos sociais previstos na legislação vigente e com quaisquer ônus, despesas, obrigações trabalhistas, previdenciárias, fiscais, de acidentes de trabalho, bem como de alimentação, transporte ou qualquer outro benefício referente à contratação dos serviços, preservando o CONTRATANTE de quaisquer demandas, reivindicações, queixas e representações de qualquer natureza, resultantes da execução do contrato;

10.1.5. Indicar, formalmente, preposto, com capacidade gerencial para representá-la perante o CONTRATANTE, com disponibilidade e pronto atendimento, estando autorizado a tratar a respeito de todos os aspectos que envolvam a execução do contrato, bem como para prestar atendimento aos seus profissionais em serviço. O documento emitido pela CONTRATADA indicando o preposto deverá ser entregue ao Gestor do Contrato, no prazo máximo de 5 (cinco) dias contados do início da execução dos serviços, e conterá as seguintes informações: nome, endereço eletrônico, telefones fixo e celular;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

10.1.6. Reparar, corrigir, substituir, total ou parcialmente, a suas expensas, serviços, objeto do contrato, em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular de emprego de material ou equipamentos inadequados;

10.1.7. Atender com presteza às reclamações sobre a qualidade dos serviços executados, providenciando a sua imediata correção sem ônus para a CONTRATANTE;

10.1.8. Assumir como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução das obrigações contratadas, ainda que adote todas as diligências possíveis para evitar o dano;

10.1.9. Prestar todos os esclarecimentos que forem solicitados pela CONTRATANTE, sempre por escrito, assim como quaisquer entendimentos com o Fiscal ou o Gestor do Contrato, não sendo consideradas alegações, solicitações ou quaisquer declarações verbais;

10.1.10. Se responsabilizar pela idoneidade e pelo comportamento de seus profissionais, prepostos ou subordinados, e, ainda, arcará com o ônus de indenizar todo e qualquer dano que, os seus profissionais causarem ao CONTRATANTE ou a terceiros, inclusive pela má utilização dos bens (materiais, utensílios e equipamentos) disponibilizados pela Administração Pública, para a realização dos serviços, obrigando-se a repor desvios, desperdícios, perdas ou quaisquer outros prejuízos que venham a ocorrer;

10.1.11. Respeitar, na execução dos serviços, as indicações de locais, horários e parâmetros de qualidade estabelecidos neste Termo de Referência, de forma a assegurar a plena eficácia da execução, assumindo todos os ônus decorrentes da inobservância de tais indicações;

10.1.12. Apresentar-se, quando convocada, para reunião inaugural na data e hora previstas;

10.1.13. Obedecer aos critérios de gestão ambiental estabelecidos na legislação, normas e regulamentos específicos do serviço, visando à melhoria dos processos de trabalho quanto aos aspectos ambientais, sociais e econômicos;

10.1.14. Disponibilizar canais de comunicação, sem ônus para o CONTRATANTE, para tratar de quaisquer assuntos referentes ao objeto do contrato;

10.1.15. Manter quadro de pessoal suficiente para atendimento dos serviços, nos moldes previstos neste documento, que não terão, em hipótese alguma, qualquer vínculo de emprego com a CONTRATANTE, sendo de exclusiva responsabilidade da empresa as despesas com todos os encargos e obrigações sociais, trabalhistas, previdenciárias e fiscais, preservando a CONTRATANTE de toda e qualquer demanda, reivindicação, queixa e representação resultante da execução do contrato;

10.1.16. Recrutar, selecionar, treinar e reciclar os profissionais que irão prestar os serviços, objeto deste contrato;

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

10.1.18. Todos os custos decorrentes da execução dos serviços, dentro ou fora do horário de expediente do CONTRATANTE, tais como deslocamentos, alimentação da equipe e pagamento de horas extras, correrão por conta da CONTRATADA;

10.1.19. Independentemente da atuação do Equipe de Gestão da Contratação, não se eximir de suas responsabilidades quanto à execução dos serviços, responsabilizando-se pelo fiel cumprimento das obrigações constantes no Termo de Referência;

10.1.20. Se responsabilizar pela permanente manutenção de validade da documentação: Jurídica, Fiscal, Técnica e Econômico-financeira da empresa, assim como pela atualização de formação de seus profissionais;

10.1.21. Não se valer do contrato para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem previa autorização do CONTRATANTE;

10.1.22. Apresentar a Nota Fiscal do período correspondente à prestação dos serviços, acompanhada da documentação necessária, para pagamento após a data de sua autuação no Protocolo do CONTRATANTE, conforme previsto na cláusula relativa ao pagamento;

10.1.23. Fornecer crachá de identificação, em que constem o nome da empresa, o do profissional, o número da matrícula, o registro geral e a fotografia, devendo manter os profissionais, quando em horário de trabalho, identificados, mediante o uso permanente de crachá, podendo este ser recusado pelo fiscal do contrato, se não atendidas às especificações estabelecidas neste Termo de Referência.

**Da CONTRATANTE**

10.1.24. Permitir o livre acesso dos profissionais da CONTRATADA às dependências da CONTRATANTE, com a finalidade única de exercer atividades relacionadas à execução do contrato e desde que estejam devidamente cadastrados e identificados;

10.1.25. Efetuar o pagamento devido à CONTRATADA pela execução dos serviços prestados nos termos e prazos contratualmente previstos, após terem sido devidamente atestados e visados, de acordo com as normas vigentes;

10.1.26. Comunicar à CONTRATADA, com antecedência mínima de 24 horas, o planejamento estratégico de mudanças e inovações no ambiente tecnológico que estejam relacionados à execução do contrato;

10.1.27. Exercer a efetiva fiscalização sobre os serviços executados e sobre o cumprimento das leis, normas e regulamentos ambientais, sanitários, trabalhistas, previdenciário, tributário, fiscais e de defesa do consumidor, que se apliquem ao objeto deste contrato;

10.1.28. Nomear a Equipe de Gestão da Contratação para acompanhar e fiscalizar a execução do contrato;

10.1.29. Receber o objeto do contrato fornecido pela CONTRATADA desde que esteja em conformidade com este Termo de Referência;

10.1.30. A Equipe de Gestão da Contratação e os Órgãos Fiscalizadores, cada um na sua esfera de atribuição, terão competência para dirimir dúvidas e decidir acerca de questões relacionadas à interpretação do conteúdo deste Termo de Referência, bem como, quaisquer questões técnicas de TI não abordadas;

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

## 11. Requisitos de habilitação

### Qualificação Técnica

11.1.1. A empresa licitante deverá apresentar seu certificado de adequação à Norma NBR ISO/IEC 27001, cujo escopo contemple, ao menos, as centrais de operação de segurança (SOC) utilizadas para a prestação do serviço;

11.1.2. A empresa licitante deverá comprovar possuir em seu quadro de funcionários, pelo menos, os seguintes títulos/certificações:

11.1.2.1. Certificação ITIL Foundation;

11.1.2.2. Pós-graduação em Gerência de Projetos ou certificação PMI PMP

11.1.2.3. Certificação CISSP ou CISM;

11.1.2.4. Certificação Security+ ou equivalente;

11.1.2.5. Certificação CEH, OSCP ou equivalente.

11.1.3. A empresa licitante deverá apresentar pelo menos um Atestado(s) de Capacidade Técnico-Operacional emitido(s) por pessoa jurídica de direito público ou privado, em nome da LICITANTE, que comprove(m) experiência na prestação, de forma satisfatória, de Serviços Gerenciados de Segurança da Informação similares aos especificados no Termo de Referência e seus anexos.

Serão considerados compatíveis os atestados que comprovem a prestação de Serviços Gerenciados de Segurança da Informação, das seguintes parcelas de maior relevância:

11.1.3.1. Serviço gerenciado de segurança da informação;

11.1.3.1.1. Será considerado serviço gerenciado de segurança da informação, aquele serviço que contemple, no mínimo, o suporte, operação e proatividade de ativos de segurança da informação, tais como firewall, antimalware, antispam, DLP, WAF, web gateway, entre outros.

11.1.3.2. Serviços de monitoramento, detecção e resposta de eventos e incidentes de segurança da informação contemplando no mínimo:

11.1.3.2.1. Dois Centros de Operações de Segurança (SOC) remotos e próprios;

11.1.3.2.2. Equipes de profissionais especializados em segurança da informação, operando em regime contínuo e ininterrupto 24/7/365;

11.1.3.2.3. Fornecimento e utilização de solução tecnológica especializada para gerenciamento, análise, automação e resposta de informações, eventos e incidentes de segurança, com recursosde aprendizado de máquina;

11.1.3.2.4. Capacidades de inteligência de ameaças (threat intelligence), caçada contínua de ameaças (threat hunting) e gerenciamento de crises.

11.1.3.3. Será admitido o somatório de atestados para obtenção dos quantitativos exigidos, desde que pelo menos 01 (um) dos atestados contemple pelo menos 50% (cinquenta por cento) do total dos quantitativos; desde que a soma dos atestados comtemple no mínimo 50% (cinquenta por cento) do total pretendido;

11.1.3.4. O(s) atestado(s)/certidão(ões)/declaração(ões) deverá(ão) ser apresentado(s) em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato e deve(m) indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

11.1.3.5. Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da CONTRATADA.

11.1.3.6. Os atestados de capacidade técnica apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela CONTRATADA e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a LICITANTE, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

11.1.4. A empresa licitante deverá apresentar comprovação ponto a ponto, contemplando os requisitos funcionais estabelecidos neste termo de referência, para cada uma das tecnologias exigidas e utilizadas para a prestação do serviço contratado.

## 12. Forma de pagamento

Após a observância dos itens 6.7. e 6.8. elencados no Termo de Referência, os pagamentos serão realizados após 30 (trinta) dias, a contar da entrega e aceite de cada parcela do objeto contratado pelo fiscal do contrato mediante emissão e ateste de Nota Fiscal.

Se ocorrer atraso injustificado no pagamento por parte do **CONTRATANTE**, de qualquer de uma das parcelas, este ficará sujeito a pagar 0,1% (zero vírgula um por cento) ao mês pró-rata dia, limitada ao total de 2% (dois por cento) do valor do **CONTRATO**.

Os pagamentos serão efetuados mediante apresentação de nota fiscal, conforme segue:

*NOME: SERVIÇO SOCIAL AUTÔNOMO HOSPITAL ALCIDES CARNEIRO*
*ENDEREÇO: RUA VIGÁRIO CORRÊA 1345 – CORRÊAS – PETRÓPOLIS*
*C.N.P.J.: 09.444.759/0001-38*
*INSC. ESTADUAL: Isento. INSC.MUNICIPAL: 90.194.*

a- Na nota fiscal ou fatura deverá constar obrigatoriamente o nome do Banco, agência e conta corrente da EMPRESA, para realização do pagamento obrigatoriamente por crédito em conta corrente.

b- Caso as notas fiscais ou faturas tenham sido emitidas com incorreções ou em desacordo com a legislação vigente, as mesmas serão devolvidas e o prazo para pagamento passará a ser contado a partir da reapresentação das mesmas.

c- Caso algum item constante na nota fiscal seja impugnado, o SEHAC liberará a parte não sujeita a contestação, retendo o restante do pagamento até que seja sanado o problema.

d- Caso seja devido, será feita uma retenção de 11% (onze por cento) sobre o valor da Nota Fiscal, referente ao INSS, de acordo com a IN n.º 971, de 13.11.2009.

e- Caso sejam devidas, serão feitas retenções sobre o valor da nota fiscal dos percentuais referentes à Contribuição Social sobre o Lucro Líquido (CSLL), COFINS e PIS/PASEP de acordo com a IN n.º 381 de 30/12/2003.

SEHAC SUS
Serviço Social Autônomo
Hospital Alcides Carneiro
Tecnologia da Informação

f- Caso seja devido, será feita retenção do Imposto sobre Serviços (ISS), de acordo com a Lei Complementar n.º 116 de 01/08/2003.

g- Caso seja devido, será feita retenção sobre o valor da Nota Fiscal, referente ao I.R., de acordo com o disposto no Decreto Municipal nº 290 de 27 de outubro de 2022 e Portaria nº 013 de 01 de novembro de 2022. As alíquotas seguirão os critérios contidos no Anexo Único do referido Decreto Municipal.

## 13. Prazos e condições

### Informações Gerais

O prazo do contrato a ser formalizado é de 60 (sessenta) meses, contados da Ordem de Início dos serviços. O mesmo poderá sofrer acréscimos e supressões que se façam necessários no percentual de até 25% (vinte e cinco) por cento do valor contratado, mediante disponibilidade financeira.

Diego Oliveira 6537

Ricardo Pancich Retamal

João José de Paula

Serviço Social Autônomo
Hospital Alcides Carneiro

Tecnologia da Informação

Data: 22/05/2025
Origem: Setor T.I.
Destino: Setor Jurídico

Memorando: Nº 020/2025
Assunto: Avaliação Técnica

Conforme solicitado pelo setor Jurídico, seguem abaixo os ajustes referentes à análise realizada no Termo Técnico do processo Nº 0946/2024:

- No item 11. Requisitos de habilitação, todos os itens referentes à qualificação técnica e demais certificações, tanto da empresa quanto dos colaboradores, estão em conformidade com as exigências solicitadas neste termo. Lembrando que os subitens do item 11.1.2 aplicam-se apenas à empresa vencedora.

- No Item 5. Escopo do serviço, referente a Informações do ambiente atual, deverá ser incluído, o subitem 5.1.5 com o seguinte conteúdo: A empresa vencedora deverá oferecer sua solução tecnológica compatível com os requisitos de configuração mínima para equipamentos que possuam Memória RAM 8GB DDR3, Processador Core I3 - 2º geração, SSD 120GB e Sistema Operacional Windows 10 (22H2)

- O Item 6.30.2. Níveis mínimos de serviço (NMS), onde se lê: "A solução Os serviços serão medidos e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela do item "Erro! Fonte de referência não encontrada" deverá ser retirado deste Termo de Referência.

- O Item 6.30.8. Níveis mínimos de serviço (NMS), onde se lê: "O NMS é composto de indicadores objetivos indicados no item "Erro! Fonte de referência não encontrada" deverá ser retirado deste Termo de Referência.

- O Item 11.3 do Edital deverá ser removido do referido documento.

- A Tabela "Quantitativo de itens" no item 5. Escopo do serviço do Anexo VII encontra-se ilegível,necessita ser revisada..

Atenciosamente,

Marcelo Antão Golstorff
Assessor de TI - SEHAC
Mat. 3731
CRA-RJ 03.00165

# ANEXO VIII

Documentações exigidas á empresa considerada habilitada, para formalizazção da contratação que deverá ser apresentado 20 (vinte) dias antes da assinatura do contrato, a contar a partir do chamamento, conforme solicitação do Termo de Referência.

- A empresa licitante deverá comprovar que possuem em seu quadro de funcionários, pelo menos, os seguintes títulos/certificações:

1- Certificação ITIL Foundation;
2- Pós-graduação em Gerência de Projetos ou certificação PMI PMP;
3- Certificação CISSP ou CISM;
4- Certificação Security+ ou equivalente;
5- Certificação CEH, OSCP ou equivalente.