CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº 057/2023
Processo n° 057/2023

EMENTA: Contratação de empresa especializada para prestação de serviços de licença de antivírus para estações de trabalho e servidores Windows, com ferramenta de administração e console de gerenciamento, incluindo instalação, treinamento e suporte técnico remoto, para o Complexo de Saúde São Bernardo do Campo.
CONTRATADA: Brasoftware Informática Ltda.

Por este instrumento de aditamento contratual, as partes, de um lado a **FUABC - COMPLEXO DE SAÚDE SÃO BERNARDO DO CAMPO**, inscrita no CNPJ/MF sob nº 57.571.275/0025-70, estabelecida à Estrada dos Alvarengas, Nº 1001, Bairro Alvarenga, São Bernardo do Campo / São Paulo, neste ato representada por sua Diretora Geral, Dra. Agnes Mello Farias Ferrari, brasileira, casada, médica, portadora do RG/UF nº 11.801.246-0 e inscrita no CPF/MF sob o nº 083.923.878-99 e do CPF/MF nº 083.923.878-99 e por seu Diretor Financeiro, José Ramde Uchôa Jardim, brasileiro, casado, economista, portador do RG nº 11.673.268 e do CPF nº 012.149.808-56, doravante denominado apenas **CONTRATANTE e,** de outro, a empresa **BRASOFTWARE INFORMÁTICA LTDA.,** com sede a Rua Marina La Regina, nº 227, 3° andar, Salas 11 a 15, Poá, São Paulo/SP, CEP 08550-210, inscrita no CNPJ/MF sob o nº 57.142.978/0001-05, representada neste ato por seu procurador Sr.Eduardo Fouad Sukarie, brasileiro, casado, diretor comercial, portador do RG/UF nº 21.963.165-7 SSP/SP e inscrita no CPF/MF sob o nº140.728.638-23, doravante denominada **CONTRATADA**, tendo em vista o constante e decidido no Processo nº 057/2023, têm como justo e acordado o que segue:

1. DO OBJETO

1.1. Contratação de empresa especializada para prestação de serviços de licença de antivírus para estações de trabalho e servidores Windows, com ferramenta de administração e console de gerenciamento, incluindo instalação, treinamento e suporte técnico remoto, para o Complexo de Saúde São Bernardo do Campo, conforme especificações técnicas exigidas no presente instrumento e seus anexos, pelo período de 24 (vinte e quatro) meses.

1.1.1. A Proposta Comercial da CONTRATADA, no que não for contrária ao estabelecido no presente instrumento, é parte integrante deste Contrato.

2. DA EXECUÇÃO DOS SERVIÇOS

2.1. A CONTRATADA prestará os serviços nas seguintes unidades e endereços:

Unidade	Endereço
HC	Rua Paulo Coppini, nº 35, Alvarenga - São Bernardo do Campo/SP.
HA	Rua Silva Jardim, nº 470, Centro - São Bernardo do Campo/SP.
HPSC	Rua Secondo Modolin, n° 499, Centro - São Bernardo do Campo/SP.
HU	Rua Joaquim Nabuco, n° 380, Centro - São Bernardo do Campo/SP.

2.2. A CONTRATADA deverá fornecer as licenças em quantidades e características abaixo:

S.O	Versão	QTDE
Windows Pro	7,8, 10 e 11	1.700
Windows Server	2012 R2 / Superior	60

2.3. A CONTRATADA deverá fornecer licenças que atendam na íntegra as características de especificações constantes no anexo I.

2.4. A Contratada deverá prestar suporte técnico às licenças adquiridas durante todo o período de vigência contratual.

2.5. Durante a vigência do contrato e da garantia, deverá ser fornecido suporte técnico pela CONTRATADA. A Contratada deverá fornecer serviços de suporte técnico em horário comercial para correção de erros da solução, resolução de dúvidas técnicas pelo telefone; O horário comercial compreende o horário de 08h00min as 18h00min, de 2ª a 6ª feira, em dias úteis.

2.6. A CONTRATADA, após a assinatura do contrato, deve disponibilizar material ou meio de consulta para a Contratante sobre como instalar, configurar e utilizar o objeto adquirido, capacitando o(s) administrador(es) e operador(es) a executar essas atividades com o console central de gerenciamento da solução adquirida.

2.7. É de responsabilidade da CONTRATADA realizar análise técnica in loco da utilização da solução proposta no que tange: instalação, configuração e política no servidor e estações de trabalho, geração de indicadores, melhores práticas, etc., ao menos 2 vezes ao ano, bem como sugerir melhorias, treinamentos, novas funcionalidades ou indicar correções que sejam necessárias para a melhor aplicação da ferramenta de segurança, sem custos adicionais.

2.8. Quaisquer dúvidas técnicas na execução dessas atividades, bem como na instalação, configuração e utilização do Console de Gerenciamento Central deverão ser sanadas por meio do suporte técnico

2.9. A CONTRATADA deverá informar à Contratante toda e qualquer atualização lançada pelo Fabricante, com detalhamento técnico.

3. DAS OBRIGAÇÕES DA CONTRATADA

3.1. A CONTRATADA deverá substituir ou sanar às suas expensas, no total ou em parte, os serviços em que se verificarem vícios, defeitos, ou incorreções resultantes da fabricação, manutenção ou de materiais empregados, no prazo de 24 (vinte e quatro) horas, a contar da informação a ser realizada preferencialmente por escrito.

3.2. A CONTRATADA deverá informar imediatamente ao gestor do contrato eventual suspensão da prestação do serviço, alteração de horário de atendimento, supressão de agenda, remarcações ou qualquer anormalidade verificada na execução do contrato, devendo do mesmo modo, prestar todos os esclarecimentos que lhe forem solicitados pela CONTRATANTE.

3.3. A CONTRATADA deverá garantir todo o apoio técnico por profissional especializado nos serviços, referente a treinamento de pessoal junto às unidades usuárias, caso seja solicitado pela CONTRATANTE.

3.4. A CONTRATADA deverá atribuir no momento da assinatura do Contrato, o responsável para o atendimento a CONTRATANTE, fornecendo o contato telefônico e e-mail do mesmo.

3.4.1. Eventual alteração do responsável técnico deverá ser imediatamente informada a CONTRATANTE, encaminhando imediatamente o novo contato.

3.5. A CONTRATADA é responsável por garantir a execução plena do objeto deste Contrato, sem qualquer interrupção, independentemente de suas eventuais necessidades de adaptação, desde a assinatura do presente Contrato, salvo caso fortuito ou força maior.

3.6. Durante a execução do contrato a CONTRATADA obriga-se a adotar todas as preocupações e cuidados tendentes a evitar danos materiais e pessoais a seus funcionários, seus prepostos e a terceiros, pelos quais será integralmente responsável.

3.7. A CONTRATADA deverá indicar um profissional, na condição de preposto contratual, responsável pelo atendimento à CONTRATANTE em todos os assuntos pertinentes à execução do Contrato.

3.8. A CONTRATADA deverá exigir que seus profissionais, quando no ambiente da CONTRATANTE, apresentem-se de forma adequada, identificados com crachá da empresa com foto recente, que obedeçam aos regulamentos internos do local de trabalho, normas técnicas e protocolos recomendados para os procedimentos realizados.

3.8.1. A CONTRATADA deverá manter disciplina nos locais dos serviços substituindo, após notificação, qualquer mão-de-obra cujo comportamento seja considerado inconveniente pela CONTRATANTE.

3.8.2. A CONTRATADA deverá informar previamente, com no mínimo 48 (quarenta e oito) horas de antecedência ao procedimento, o nome completo e o número do documento do profissional que prestará os serviços esporadicamente nas instalações ou então encaminhar mensalmente relatório dos funcionários que prestarão os serviços nas unidades.

3.9. A CONTRATADA deve cumprir, além das normas vigentes de âmbito Federal, Estadual ou Municipal, as Normas de Segurança e Medicina do Trabalho.

3.10. A CONTRATADA não reproduzirá, divulgará ou utilizará em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços discriminados, sem o consentimento prévio e por escrito da CONTRATANTE.

3.11. A CONTRATADA não utilizará o nome da CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos, sem o consentimento prévio e por escrito da CONTRATANTE.

3.12. A CONTRATADA instruirá sua mão-de-obra, quanto à prevenção de acidente no trabalho de acordo com as normas vigentes instituídas pela Engenharia de Segurança do Trabalho da CONTRATANTE, provendo-os dos equipamentos de proteção individual (EPI), com exceção aos itens constantes no item 5.6 do anexo II, bem como fiscalizando o seu uso.

3.13. A CONTRATADA prestará os serviços dentro dos parâmetros de rotinas estabelecidas, fornecendo todos os materiais e equipamentos em quantidade, qualidade e tecnologia adequadas, com a observância das normas técnicas e legislações vigentes.

3.14. A CONTRATADA garantirá livre acesso a informações, dos procedimentos e à documentação referente aos serviços prestados, aos gestores indicados pela CONTRATANTE, para o acompanhamento da gestão contratual.

3.15. A CONTRATADA responsabiliza-se pelos danos causados diretamente à CONTRATANTE ou a terceiros, em decorrência de suas ações, tendo direito a CONTRATANTE ao ressarcimento da CONTRATADA, por força contratual, em eventual responsabilidade da CONTRATANTE em decorrência de defeitos nos serviços da CONTRATADA, podendo inclusive denunciá-la à lide para evitar o ajuizamento de ação de regresso.

3.16. Ao final da vigência deste Contrato, toda a documentação, históricos, processos estabelecidos e arquivos gerados, deverão ser entregues pela CONTRATADA à CONTRATANTE.

3.17. A CONTRATADA se responsabilizará por todas as despesas com encargos e obrigações sociais, trabalhistas, fiscais e comerciais decorrentes da execução contratual, sendo que os empregados da CONTRATADA não terão, em hipótese alguma, qualquer relação de emprego com a CONTRATANTE.

3.17.1. Caberá a CONTRATADA requerer a exclusão da CONTRATANTE do polo passivo de eventuais ações demandadas por seus funcionários em face CONTRATANTE, visando minimizar prejuízos judiciais e econômicos para esta Instituição.

3.18. A CONTRATADA terá seu desempenho submetido a acompanhamentos sistemáticos de acordo com os critérios de avaliação e controle da CONTRATANTE, através de formulários próprios.

3.19. A fiscalização ou acompanhamento da execução deste Contrato, por parte dos órgãos competentes da CONTRATANTE, não exclui nem reduz a responsabilidade da CONTRATADA.

3.20. A CONTRATADA cumprirá o Regimento Interno e as demais Normas Internas do CONTRATANTE, assim como outras normas relativas à engenharia de segurança do trabalho com base na lei 6.514, de 22/09/1977, portaria 3.214, (NR) e demais disposições legais e às regulamentações da Agência Nacional de Vigilância Sanitária (ANVISA) e do Ministério da Saúde.

3.21. A CONTRATADA manterá completo e absoluto sigilo sobre quaisquer dados, materiais, pormenores, informações, documentos, especificações técnicas ou comerciais, inovações que venha a ter conhecimento ou acesso, ou que venha a ser confiado em razão deste contrato, inclusive os dados protegidos pela Lei Geral de Proteção de Dados Pessoais nº 13.709/2018, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, utilizar, tratar, ou deles dar conhecimentos a terceiros a esta contratação, sob pena da lei.

3.22. A CONTRATADA será responsável por todos os ônus e tributos, emolumentos, honorários ou despesas incidentais sobre os serviços contratados, bem como cumprir rigorosamente, todas as obrigações trabalhistas, previdenciárias e acidentárias relativas ao pessoal que empregar para a execução dos serviços, inclusive as decorrentes de convenções, acordos ou dissídios coletivos, mantendo a disposição do CONTRATANTE toda e qualquer documentação pertinente (ficha de registro, guias de recolhimento dos encargos trabalhistas e previdenciários, exames admissionais e periódicos).

3.23. A CONTRATADA assume a defesa contra quaisquer reclamações ou demandas ambientais, administrativas e judiciais, arcando com os respectivos ônus, decorrentes de quaisquer falhas na prestação dos serviços ora contratados ou danos que venham a ser causados durante o período de execução dos serviços, seja na atuação direta, seja por seus empregados ou prepostos.

3.24. A CONTRATADA não terá como sócios, gerentes, diretores ou administradores, os cônjuges, companheiros (as) ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de funcionários, ocupantes dos cargos de direção, chefia, assessoramento da CONTRATANTE, sob pena de rescisão contratual.

3.25. A CONTRATADA não utilizará na execução do objeto do presente contrato, quaisquer funcionários, administradores ou ocupantes de cargos de direção da Fundação do ABC e de suas mantidas.

3.26. Fica vetado à CONTRATADA utilizar na prestação dos serviços, profissionais que sejam funcionários da CONTRATANTE, bem como ex colaboradores que tenham trabalhado para a CONTRATANTE nos últimos 18 (dezoito) meses que anteceder a prestação de serviços objeto do presente contrato, conforme artigo 5º-D da Lei 6.019/74.

4. DAS OBRIGAÇÕES DA CONTRATANTE

4.1. A CONTRATANTE gerenciará o Contrato, por intermédio de sua Gerência de Tecnologia da Informação.

4.2. A CONTRATANTE exercerá a fiscalização, examinando quanto ao cumprimento deste Contrato.

4.3. A CONTRATANTE efetuará os pagamentos, referentes aos serviços prestados, deduzindo-se das faturas as eventuais glosas determinadas pelo Gestor do Contrato, sendo assegurado à CONTRATADA o direito à ampla defesa.

4.4. Não obstante a CONTRATADA seja a única responsável pela prestação do serviço, a CONTRATANTE reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a fiscalização mais ampla e completa sobre os serviços prestados e aceitos pela CONTRATANTE.

4.5. A CONTRATANTE assegurar-se-á que o número de empregados alocados ao serviço por parte da CONTRATADA seja o suficiente para o adequado desempenho dos serviços.

4.6. A CONTRATANTE solicitará à CONTRATADA e seus prepostos, tempestivamente, todas as providências necessárias ao adequado desempenho dos serviços.

4.7. A CONTRATANTE emitirá pareceres em todos os atos relativos à execução deste Contrato, em especial, a aplicação de sanções, alterações e repactuações contratuais.

4.8. A CONTRATANTE permitirá o livre acesso dos empregados da CONTRATADA para execução dos serviços, quando autorizados.

4.9. A CONTRATANTE exigirá, após ter advertido a CONTRATADA por escrito, o imediato afastamento de qualquer empregado ou preposto da mesma, que não mereça a sua confiança ou embarace a fiscalização ou, ainda, que se conduza de modo inconveniente ou incompatível com o exercício das funções que lhe forem atribuídas.

4.10. É vedada à CONTRATANTE, e seus representantes, exercer poder de mando sobre os empregados da CONTRATADA, reportando-se somente aos prepostos e responsáveis por ela indicados.

4.11. A CONTRATANTE assegurará as condições mínimas para a realização dos procedimentos com segurança, garantindo a guarda e conservação dos serviços, após sua conferência e entrada em seu estabelecimento.

4.12. A CONTRATANTE fiscalizará por intermédio do gestor/fiscal do contrato os serviços objeto do Contrato.

4.13. A CONTRATANTE prestará informações e esclarecimentos que eventualmente venham a ser solicitadas pela CONTRATADA e que digam respeito à natureza dos serviços que tenham de executar.

5. DAS SANÇÕES ADMINISTRATIVAS E DEMAIS PENALIDADES

5.1. A CONTRATANTE poderá aplicar advertência quando ocorrer prestação insatisfatória dos serviços ou pequenos transtornos ao desenvolvimento dos serviços, desde que sua gravidade não recomende as sanções posteriormente descritas.

5.2. Em caso de infrações, o CSSBC poderá aplicar à CONTRATADA a seguinte sanção de multa:

5.2.1. Multa de 10% (dez por cento), por inexecução parcial do contrato, calculada sobre o valor mensal do Contrato. Na hipótese de reincidência por parte da CONTRATADA, a CONTRATANTE poderá rescindir o contrato, nos termos da cláusula 8.2 da Minuta de Contrato;

5.2.2. Multa de 20% (vinte por cento), por inexecução total do contrato, calculada sobre o valor total do Contrato

5.2.3. Faculta-se ao CSSBC, no caso da CONTRATADA não cumprir o serviço contratado, adquirir o serviço de outra empresa, devendo a CONTRATADA arcar com os custos que eventualmente forem acrescidos para a aquisição.

5.3. A CONTRATANTE poderá, em decorrência da gravidade dos atos praticados pela CONTRATADA, suspender temporariamente sua participação em coleta de preços a ser realizada pelo Complexo de Saúde São Bernardo do Campo, pelo prazo de até 02 (dois) anos.

5.3.1. A CONTRATADA possui plena ciência que a CONTRATANTE encaminhará relato do ocorrido a municipalidade e a Fundação do ABC, mantenedora da CONTRATANTE, para que caso assim desejem, também suspendam o direito de participar em processos de compras/contratação por eles iniciados.

5.4. A sanção de multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança não isentará a CONTRATADA de indenizar a CONTRATANTE por eventuais perdas e danos.

5.5. Constatado o descumprimento de quaisquer obrigações decorrentes do ajuste, a CONTRATANTE notificará a CONTRATADA acerca de sua intenção de aplicar-lhe eventuais penas, sendo-lhe facultada apresentação de defesa escrita, se assim entender, no prazo de 05 (cinco) dias úteis, contados do recebimento da referida notificação.

5.6. Uma vez apresentada a defesa, a CONTRATANTE poderá, após análise, deferir a pretensão, restando afastada, então, a possibilidade da penalização, ou indeferir a pretensão, dando prosseguimento aos trâmites administrativos visando à efetiva aplicação da pena.

5.6.1. Na hipótese de indeferimento, será a CONTRATADA notificada da referida decisão, podendo a CONTRATANTE realizar o abatimento da multa calculada na nota fiscal emitida para o pagamento dos serviços contratados.

6. DAS CONDIÇÕES DE PAGAMENTO E CRITÉRIOS DE FATURAMENTO

6.1. A CONTRATANTE deverá pagar à CONTRATADA o valor dos produtos fornecidos, exclusivamente através de depósito em conta corrente.

6.1.1. A CONTRATADA deverá indicar na documentação fiscal original o número de sua conta corrente, agência e banco no qual deverá ser efetuado o pagamento.

6.1.2. Em nenhuma hipótese serão aceitos títulos via cobrança bancária.

6.2. O pagamento dos serviços será realizado no dia 28 (vinte e oito) do mês, subsequente ao mês da prestação dos serviços, desde que a nota fiscal seja entregue à CONTRATANTE com, no mínimo, 10 (dez) dias de antecedência à data do vencimento, com a apresentação junto a Nota Fiscal / Fatura das certidões de regularidade fornecidas pela Secretaria da Receita Federal do Brasil e pela Procuradoria Geral da Fazenda Nacional referente a débitos relativos aos tributos federais e à dívida ativa da União (CND), FGTS (CRF) e Justiça do Trabalho (CNDT), por parte da CONTRATADA.

6.2.1. Caso se faça necessária a reapresentação de qualquer fatura por culpa da CONTRATADA, o prazo previsto na presente Cláusula será reiniciado.

6.2.2. Dos pagamentos, será retido na fonte, quando for o caso, o valor correspondente ao Imposto Sobre Serviços de Qualquer Natureza (ISSqn), nos termos da legislação específica e demais tributos que recaiam sobre o valor faturado.

6.2.3. A liberação para pagamento da nota fiscal/fatura ficará condicionada ao ateste do Gestor do Contrato e à entrega dos documentos mencionados no item 6.2.

6.2.4. Todas as notas fiscais em seu conteúdo original devem ser emitidas com os seguintes dizeres: **"Despesa custeada com recursos do Contrato de Gestão SS nº 001/2022 firmado com o Município de São Bernardo do Campo".**

6.3. A CONTRATADA deverá encaminhar a nota fiscal desmembrada para cada unidade, e estas deverão ser emitidas para a Fundação do ABC – Complexo de Saúde São Bernardo do Campo, CNPJ n° 57.571.275/0025-70.

Endereço de Fatura e Cobrança: Estrada dos Alvarengas, 1001 – Bairro Alvarenga – São Bernardo do Campo/SP.

6.3.1. Fica facultado a CONTRATADA o envio da nota fiscal eletronicamente.

6.4. A CONTRATADA, neste ato, declara estar ciente de que os recursos utilizados para o pagamento dos serviços ora contratados serão aqueles repassados pela Prefeitura Municipal de São Bernardo do Campo, em razão do Contrato de Gestão SS n° 001/2022, firmado entre a CONTRATANTE e a Prefeitura Municipal de São Bernardo do Campo, para a gestão do Complexo de Saúde São Bernardo do Campo.

6.5. A CONTRATANTE informa que, a única fonte de receita a ser utilizado para pagamento dos serviços ora contratados é aquela prevista no contrato de gestão 001/2022, sendo vedada a utilização de qualquer outra fonte de recurso para pagamento, nos termos do §7° do artigo 51 do regulamento de compras.

6.6. A CONTRATANTE compromete-se em pagar o preço irreajustável constante da proposta da CONTRATADA, desde que não ocorram atrasos e/ou paralisação dos repasses pela Prefeitura Municipal de São Bernardo do Campo para a CONTRATANTE, relativo ao custeio do objeto do Contrato de Gestão SS n° 001/2022.

6.7. No caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente, salvo quando não decorram de atrasos e/ou paralisação dos repasses pela Prefeitura Municipal de São Bernardo do Campo para a CONTRATANTE, em consonância com o disposto nas cláusulas 6.4, 6.5 e 6.6 deste CONTRATO.

7. DAS ALTERAÇÕES DO CONTRATO

7.1. O presente contrato poderá ser alterado, desde que, de forma fundamentada e em consenso, sempre através de termo aditivo.

7.2. As partes poderão realizar acréscimos ou supressões ao objeto do presente contrato desde que previamente acordadas e formalizadas por meio de termo aditivo.

7.2.1. Os acréscimos e supressões poderão ser solicitados pela CONTRATANTE, cabendo à CONTRATADA, em caso de discordância, notificar o interesse no distrato observando o prazo mínimo estipulado neste instrumento.

8. DA RESCISÃO/RESILIÇÃO

8.1. As partes poderão resilir, imotivadamente, o presente Contrato, desde que comunicado por escrito à outra com antecedência mínima de 30 (trinta) dias, ou celebrar, amigavelmente, o seu distrato na forma da lei, em qualquer caso, nenhuma indenização será devida.

8.2. A rescisão, por inadimplemento das obrigações prevista no presente Contrato poderá ser declarada unilateralmente pela CONTRATANTE, mediante decisão motivada.

8.3. Dar-se-á automaticamente a rescisão dos contratos decorrentes de obrigações contraídas por meio de Convênios Administrativos ou Contratos de Gestão, no caso de rescisão das respectivas avenças administrativas, sendo que nesta hipótese nenhuma indenização será devida, facultando-se a resilição unilateral sem aviso prévio.

8.4. Na hipótese de rescisão por inadimplemento, além das sanções cabíveis, ficará a CONTRATADA sujeita à multa de 10% (dez por cento) calculada sobre o saldo do serviço não executado, sem prejuízo da retenção de créditos, reposição de importâncias indevidamente recebidas e das perdas e danos que forem apurados.

9. DA CESSÃO E TRANSFERÊNCIA

9.1. O presente contrato não poderá ser objeto de cessão, transferência ou subcontratação no todo ou em parte, a não ser com prévio e expresso consentimento da CONTRATANTE e sempre mediante instrumento próprio.

9.1.1. O cessionário fica sub-rogado em todos os direitos e obrigações do cedente e deverá atender a todos os requisitos de habilitação previamente estabelecidos.

10. DO RECURSO AO JUDICIÁRIO

10.1. Caso as partes tenham que ingressar em juízo para haver o que lhe for devido, ficarão sujeitas ao pagamento do principal, despesas processuais e honorários, conforme determinação judicial arbitrada em sentença.

11. DA VIGÊNCIA

11.1. O prazo de vigência deste Contrato será de 24 (vinte e quatro) meses, contados a partir da data de sua assinatura.

11.1.1. O prazo contratual poderá ser prorrogado por iguais ou menores períodos e sucessivos, até o limite de 48 (quarenta e oito) meses.

11.1.2. O valor permanecerá inalterado durante a vigência do presente Contrato podendo ser reajustado com base no índice IGP-M a cada período de 12 (doze) meses, desde que seja previamente discutido e acordado entre as partes.

12. DO VALOR

12.1. Dá-se ao presente Contrato o valor total estimado de R$ 153.982,40 (cento e cinquenta e três mil e novecentos e oitenta e dois reais e quarenta centavos), sendo:

Licença	Quantidade	Valor unitário	Valor Total
Licenças	1.760	R$ 87,49	R$ 153.982,40

12.1.1. O valor acima descrito se trata de mera estimativa, não se obrigando a CONTRATANTE, de forma alguma, a atingi-lo.

13. DA EXCEÇÃO DO CONTRATO NÃO CUMPRIDO

13.1. A CONTRATADA não poderá opor a CONTRATANTE a exceção do Contrato não cumprido como fundamento para a interrupção unilateral do serviço, nos termos de art. 476 do Código Civil.

14. DO FORO DE ELEIÇÃO

14.1. Fica eleito o Foro do município de São Bernardo do Campo, para dirimir qualquer dúvida ou litígio decorrente do presente contrato, com expressa renúncia a outro por mais privilegiado que seja.

15. DAS DISPOSIÇÕES GERAIS

15.1. Fica a CONTRATADA obrigada a manter durante a execução deste Contrato todas as condições de qualificação e habilitação exigidas no respectivo procedimento de Coleta de Preços.

15.2. Considerando a possibilidade de as partes negociarem os termos deste contrato, fica desde já afastada, na presente contratação, a aplicabilidade do artigo 423 do Código Civil vigente.

15.3. Os termos deste Contrato são confidenciais e, salvo disposição legal em contrário, a CONTRATANTE não poderá divulgar esses termos a nenhum terceiro sem o consentimento por escrito da CONTRATADA.

15.4. A tolerância por qualquer das Partes quanto ao cumprimento das cláusulas e condições contratuais ora firmadas não implicará renúncia, novação, transação ou precedente, devendo ser havida como mera liberalidade.

15.5. Se uma disposição contratual for considerada inválida, ilegal ou inexequível a qualquer título, tal disposição será considerada em separado e não invalidará as disposições restantes, as quais não serão afetadas por esse fato.

E, por estarem as partes de comum acordo sobre as Cláusulas, termos e condições deste instrumento, firmam-no em 02 (duas) vias de igual teor e conteúdo, na presença de 02 (duas) testemunhas.

São Bernardo do Campo, 01 de agosto de 2023.

AGNES MELLO FARIAS FERRARI
Diretora Geral

JOSÉ RAMDE UCHÔA JARDIM
Diretor Financeiro

FUNDAÇÃO DO ABC – COMPLEXO DE SAÚDE SÃO BERNARDO DO CAMPO

EDUARDO FOUAD SUKARIE
Diretor
BRASOFTWARE INFORMÁTICA LTDA

Testemunhas:

1- Nome: _____CPF.: _____Ass.: _____

2- Nome:_____CPF.:_____Ass.: _____

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

1. Servidor de Administração e Console Gerenciamento

1.1. Compatibilidade:

1.1.1. Microsoft Storage Server 2012 e Server R2 x64;
1.1.2. Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64;
1.1.3. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
1.1.4. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
1.1.5. Microsoft Windows Server 2022 Standard / Core / Datacenter x64;
1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.7. Microsoft Windows 8 Professional / Enterprise x64;
1.1.8. Microsoft Windows 8.1 Professional / Enterprise x32/x64;
1.1.9. Microsoft Windows 10 x32/x64;
1.1.10. Windows 11 Home / Pro / Enterprise / Education x64;

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;
1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64;
1.2.5. Parallels Desktop 17;
1.2.7. Citrix XenServer 7.1, 8.x;
1.2.8. Oracle VM VirtualBox 6;

1.3. Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. A console deve suportar arquitetura on-premise e arquitetura cloud-based;
1.3.3. Console deve ser baseada no modelo cliente/servidor;
1.3.4. A console deve suportar autenticação de dois fatores;
1.3.5. Deve possuir compatibilidade com Windows Failover Clustering;
1.3.6. O servidor de administração deve possui modelo de cluster ativo-passivo;
1.3.7. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;
1.3.8. Deve permitir incluir usuários do AD para logarem na console de administração
1.3.9. Console deve ser totalmente integrada com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;
1.3.10. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.3.11. Deverá ser possível buscar novos produtos e soluções a partir da console;
1.3.12. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.3.13. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.
1.3.14. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.15. Deve armazenar histórico das alterações feitas em políticas;

1.3.16. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

1.3.17. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

1.3.18. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

1.3.19. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

1.3.19. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

1.3.20. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

1.3.21. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.3.22. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

1.3.23. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

1.3.24. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

1.3.25. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.3.26. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.3.27. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

1.3.28. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.29. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

1.3.30. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.3.31. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

1.3.31.1. Pesquisa de rede (Windows pooling);

1.3.31.2. Pesquisa ativa do AD (AD pooling);

1.3.31.3. Pesquisa de IP (IP pooling);

1.3.31.4. Pesquisa de rede (Zeroconf pooling);

1.3.32. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

1.3.33. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.34. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.3.35. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.3.36. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

1.3.37. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.3.38. Deve fornecer as seguintes informações dos computadores:

1.3.38.1. Se o antivírus está instalado;

1.3.38.2. Se o antivírus está iniciado;

1.3.38.3. Se o antivírus está atualizado;

1.3.38.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

1.3.38.5. Minutos/horas desde a última atualização de vacinas;

1.3.38.6. Data e horário da última verificação executada na máquina;

1.3.38.7. Versão do antivírus instalado na máquina;

1.3.38.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.3.38.9. Quantidade de vírus encontrados (contador) na máquina;

1.3.38.10. Nome do computador;

1.3.38.11. Domínio ou grupo de trabalho do computador;

1.3.38.12. Data e horário da última atualização de vacinas;

1.3.38.13. Sistema operacional com Service Pack;

1.3.38.14. Quantidade de processadores;

1.3.38.15. Quantidade de memória RAM;

1.3.38.16. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

1.3.38.17. Endereço IP;

1.3.38.18. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

1.3.38.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

1.3.39. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.3.40. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

1.3.40.1. Alteração de Gateway Padrão;

1.3.40.2. Alteração de subrede;

1.3.40.3. Alteração de domínio;

1.3.40.4. Alteração de servidor DHCP;

1.3.40.5. Alteração de servidor DNS;

1.3.40.6. Alteração de servidor WINS;

1.3.40.7. Resolução de Nome;

1.3.40.8. Disponibilidade de endereço de conexão SSL;

1.3.41. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.3.42. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.3.43. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.3.44. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

1.3.45. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.3.46. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

1.3.47. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.3.48. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

1.3.49. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

1.3.50. Capacidade de monitoramento do sistema através de um SNMP client;

1.3.51. Capacidade enviar eventos através de protocolo de syslog;

1.3.52. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

1.3.53. Listar em um único local, todos os computadores não gerenciados na rede;

1.3.54. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

1.3.55. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

1.3.56. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.3.57. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.3.58. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

1.3.59. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

1.3.59. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

1.3.60. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.61. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

1.3.62. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.63. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

1.3.64. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

1.3.65. Capacidade de realizar resumo de hardware de cada máquina cliente;

1.3.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

1.3.67. Permitir a instalação automática em máquinas novas na rede via software de gerenciamento remoto.

1.3.68. Atualizar a partir de um servidor web externo ou servidor web interno os repositórios locais em momentos específicos e estratégicos, objetivando a garantia de disponibilidade da rede.

1.3.69. O antivírus deverá promover mecanismos de customização dos pacotes de instalação em clientes e servidores, com possibilidade de uso de pacotes de instalação auto executáveis (.exe e .msi), instalação silenciosa, pastas de instalação no destino, configurações avançadas das tecnologias a serem instaladas.

2. Sistemas operacionais Windows

2.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;
2.1.2. Microsoft Windows 8 Professional/Enterprise;
2.1.3. Microsoft Windows 8.1 Professional / Enterprise;
2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;
2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.2. Deve ser compatível com os seguintes sistemas servidores:

2.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit)
2.2.2. Windows MultiPoint Server 2011 (64-bit);
2.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;
2.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;
2.2.5. Windows Server 2016 Essentials / Standard / Datacenter;
2.2.6. Windows Server 2019 Essentials / Standard / Datacenter;
2.2.7. Windows Server 2022.

2.3. Suporta as seguintes plataformas virtuais:

2.3.1. Vmware Workstation 16.2.3;
2.3.2. Vmware ESXi 7.0 Update 3d;
2.3.3. Microsoft Hyper-V Server 2019;
2.3.4. Citrix Virtual Apps and Desktops 7 2203;
2.3.5. Critrix Provisioning 2203;
2.3.6. Citrix Hypervisor 8.2

2.4. Características:

2.4.1. Deve prover as seguintes proteções:
2.4.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2.4.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
2.4.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
2.4.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
2.4.1.5. Deve possui modulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;
2.4.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
2.4.1.7. Controle de dispositivos externos;
2.4.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
2.4.1.9. Controle de acesso a sites por horário;
2.4.1.10. Controle de acesso a sites por usuários;
2.4.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
2.4.1.12. Controle de execução de aplicativos;
2.4.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
2.4.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
2.4.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.4.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.4.6. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.4.7. Deverá possuir módulo dedicado para proteção contra port scanning;

2.4.8. Deverá possuir módulo dedicado para proteção contra network flooding;

2.4.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.4.10. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.4.11. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.4.12. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.4.13. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

2.4.14. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

2.4.15. Deverá realizar scanner de firmware em busca de rootkits.

2.4.16. Ao detectar uma ameaça, a solução deve exibir informações:

2.4.16.1. Do objeto SHA256;

2.4.16.2. Do objeto MD5.

2.4.17. Capacidade de verificar somente arquivos novos e alterados;

2.4.18. Capacidade de verificar objetos usando heurística;

2.4.19. Capacidade de agendar uma pausa na verificação;

2.4.20. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.4.21. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.4.22. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.4.22.1. Perguntar o que fazer, ou;

2.4.22.2. Bloquear acesso ao objeto;

2.4.22.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.22.2.2. Caso positivo de desinfecção:

2.4.22.2.2.1. Restaurar o objeto para uso;

2.4.22.2.3. Caso negativo de desinfecção:

2.4.22.2.3.1. Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.23. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.4.24. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

2.4.25. Capacidade de verificar links inseridos em e-mails contra phishings;

2.4.26. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e analise de heurística bloqueado arquivos, sites de phishing e URL maliciosas;

2.4.27. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.4.28. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.4.28.1. Perguntar o que fazer, ou;

2.4.28.2. Bloquear o e-mail;
2.4.28.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.4.28.2.2. Caso positivo de desinfecção:
2.4.28.2.2.1. Restaurar o e-mail para o usuário;
2.4.28.2.3. Caso negativo de desinfecção:
2.4.28.2.3.1. Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.27. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.4.28. Capacidade de filtrar anexos de e-mail, apagando-os ou os renomeando de acordo com a configuração feita pelo administrador;

2.4.29. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);

2.4.30. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Trafego de rede por aplicativo.

2.4.31. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

2.4.32. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
2.4.32.1. Perguntar o que fazer, ou;
2.4.32.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
2.4.32.3. Permitir acesso ao objeto;

2.4.33. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.4.33.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2.4.33.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

2.4.34. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.4.35. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.4.37. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.4.38. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);

2.4.39. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.4.40. Deve possuir módulo para proteção contra *port scans, network flooding e MAC spoofing*. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.4.41. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.4.42. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

2.4.43. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.4.43.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.4.43.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.4.44. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
2.4.44.1. Discos de armazenamento locais;
2.4.44.2. Armazenamento removível;

2.4.44.3. Impressoras;
2.4.44.4. CD/DVD;
2.4.44.5. Drives de disquete;
2.4.44.6. Modems;
2.4.44.7. Dispositivos de fita;
2.4.44.8. Dispositivos multifuncionais;
2.4.44.9. Leitores de smart card;
2.4.44.10. Wi-Fi;
2.4.44.11. Adaptadores de rede externos;
2.4.44.12. Dispositivos MP3 ou smartphones;
2.4.44.13. Dispositivos Bluetooth;
2.4.44.14. Câmeras e Scanners.

2.4.45. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
2.4.46. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
2.4.47. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
2.4.48. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.
2.4.49. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.
2.4.50. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
2.4.51. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
2.4.52. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.
2.4.53. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;
2.4.54. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
2.4.54.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.4.54.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.4.55. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.4.56. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
2.4.57. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
2.4.58. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
2.4.59. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
2.4.60. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
2.4.61. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
2.4.62. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.4.63. Deve permitir realizar o gerenciamento por meio de integração via REST API.
2.4.64. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

3. Estações Mac OS X

3.1. Compatibilidade:

3.1.1. macOS Mojave 10.14

3.1.2. macOS Catalina 10.15
3.1.3. macOS Big Sur 11.0
3.1.4. macOS Monterey 12 ou superior

3.2. Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;
3.2.3. Possuir módulo de bloqueio á ataques na rede;
3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
3.2.6. Possibilidade de importar uma chave no pacote de instalação;
3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
3.2.9. Capacidade de voltar para a base de dados de vacina anterior;
3.2.11. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
3.2.12. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.2.13. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
3.2.14. Capacidade de verificar somente arquivos novos e alterados;
3.2.15. Capacidade de verificar objetos usando heurística;
3.2.16. Capacidade de agendar uma pausa na verificação;
3.2.17. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.2.17.1. Perguntar o que fazer, ou;
3.2.17.2. Bloquear acesso ao objeto;
3.2.17.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.17.2.2. Caso positivo de desinfecção:
3.2.17.2.2.1. Restaurar o objeto para uso;
3.2.17.2.3. Caso negativo de desinfecção:
3.2.17.2.3.1. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.18. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.2.19. Capacidade de verificar arquivos de formato de email;
3.2.20. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
3.2.21. Capacidade de, através da mesma console central de gerenciamento:
3.2.21.1. Ser instalado;

3.2.21.2. Ser removido;
3.2.21.3. Ser gerenciado;

4. Sistemas operacionais Linux

4.1. Compatibilidade:

4.1.1. Plataforma 32-bits:

4.1.1.1. Red Hat Linux 6.7 e superior;
4.1.1.2. CentOS 6.7 e superior;
4.1.1.3. Debian 9.4 e superior;
4.1.1.4. Debian 10.1 e superior;
4.1.1.5. Debian 11.1 e superior;
4.1.1.6. Linux Mint 19 e superior;
4.1.1.7. Mageia 4;

4.1.2. Plataforma 64-bits:

4.1.2.1. Ubuntu 18.04 e superior;
4.1.2.2. Ubuntu 20.04;
4.1.2.3. Red Hat Enterprise Linux 6.7;
4.1.2.4. Red Hat Enterprise Linux 7.2;
4.1.2.5. Red Hat Enterprise Linux 8.0;
4.1.2.6. CentOS 6.7 e superior;
4.1.2.7. CentOS 7.2 e superior;
4.1.2.8. CentOS 8.0 e superior;
4.1.2.9. Debian 9.4 e superior;
4.1.2.10. Debian 10.1 e superior;
4.1.2.11. OracleLinux 7.3 e superior;
4.1.2.12. OracleLinux 8 e sueperior;
4.1.2.13. SUSE Server 12 e superior
4.1.2.14. SUSE Server 15 e superior;
4.1.2.15. openSUSE Leap 15;
4.1.2.16. Amazon Linux 2;
4.1.2.17. Linux Mint 19 e superior;
4.1.2.18. Linux Mint 20.1 e superior;
4.1.2.19. Oracle Linux 7.3 e superior;
4.1.2.20. Oracle Linux 8.0 e superior;
4.1.2.21. RED OS 7.2;

4.2. Características:

4.2.1. Deve prover as seguintes proteções:
4.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
4.2.3.1. Via linha de comando;
4.2.3.2. Via console administrativa;
4.2.3.3. Via GUI;
4.2.3.4. Via web (remotamente);

4.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
- 4.2.4.1. CDs;
- 4.2.4.2. DVDs;
- 4.2.4.3. Discos blu-ray;
- 4.2.4.4. Flash drives (pen drives);
- 4.2.4.5. HDs externos;
- 4.2.4.6. Disquetes;

4.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
- 4.2.5.1. Por tipo de dispositivo;
- 4.2.5.2. Por barramento de conexão.

4.2.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

4.2.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- 4.2.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- 4.2.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- 4.2.7.3. Leitura de configurações;
- 4.2.7.4. Modificação de configurações;
- 4.2.7.5. Gerenciamento de Backup;
- 4.2.7.6. Visualização de logs;
- 4.2.7.7. Gerenciamento de logs;
- 4.2.7.8. Gerenciamento de ativação da aplicação;
- 4.2.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

4.2.8. Capacidade de criar exclusões por local, máscara e nome da ameaça;

4.2.9. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.10. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

4.2.11. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

4.2.12. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
- 4.2.12.1. Alta;
- 4.2.12.2. Média;
- 4.2.12.3. Baixa;
- 4.2.12.4. Recomendado;

4.2.13. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;

4.2.14. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

4.2.15. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

4.2.16. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

4.2.17. Deverá ser possível priorizar a execução de tarefas;

4.2.18. Capacidade de verificar objetos usando heurística;

4.2.19. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

4.2.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

4.2.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
- 4.2.21.1. Detecção de phishing e sites maliciosos;
- 4.2.21.2. Bloqueio de download de arquivos maliciosos;
- 4.2.21.3. Bloqueio de adware;

4.2.22. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

4.2.23. 4.2.23. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
4.2.24. Deverá fornecer informações de todas os executáveis das aplicações;
4.2.25. Deve possuir módulo de proteção contra criptografia maliciosa.
4.2.26. Deverá possuir controle de execução de aplicações;
4.2.27. O modulo de controle de aplicação deverá possuir as seguintes funcionalidades:
4.2.27.1. Criação de lista de bloqueio de aplicação;
4.2.27.2. Criação de lista de permissão de aplicação;
4.2.28. Deverá realizar busca de ameaças em setores críticos do sistema operacional:
4.2.28.1. Setor de inicialização;
4.2.28.2. Objetos de inicialização;
4.2.28.3. Processos de memória;
4.2.28.4. Memória do kernel;

5. Compatibilidade com servidores windows

5.1. Compatibilidade de sistema legado:

5.2. Plataforma x32 ou x64:

5.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

5.3. Características:

5.3.1. Deve prover as seguintes proteções:
5.3.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.3.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.3.1.3. Firewall com IDS;
5.3.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.3.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
5.3.3.1. Via console administrativa;
5.3.3.2. Via web (remotamente);
5.3.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.3.5. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.
5.3.6. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.3.6.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.3.6.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.3.6.3. Leitura de configurações;
5.3.6.4. Modificação de configurações;
5.3.6.5. Gerenciamento de backup;
5.3.6.6. Visualização de logs;
5.3.6.7. Gerenciamento de logs;
5.3.6.8. Gerenciamento de ativação da aplicação;
5.3.6.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.3.6.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

5.3.7. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.3.7.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.3.7.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
5.3.8. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
5.3.9. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
5.3.10. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.3.11. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
5.3.12. Deve possuir funcionalidade de análise personalizada de logs do Windows.
5.3.13. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.3.14. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.3.15. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.3.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.3.17. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
5.3.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
5.3.19. Capacidade de verificar somente arquivos novos e alterados;
5.3.20. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.3.21. Capacidade de verificar objetos usando heurística;
5.3.22. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.3.23. Capacidade de agendar uma pausa na verificação;
5.3.25. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.3.25.1. Perguntar o que fazer, ou;
5.3.25.2. Bloquear acesso ao objeto;
5.3.25.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.3.25.2.2. Caso positivo de desinfecção:
5.3.25.2.2.1. Restaurar o objeto para uso;
5.3.25.2.3. Caso negativo de desinfecção:
5.3.25.2.3.1. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.3.26. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.3.27. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos malicioso em área de backup;
5.3.28. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

5.3.29. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:
5.3.29.1. Executar os procedimentos pré-configurados pelo administrador;
5.3.29.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.
5.3.30. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
5.3.31. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
5.3.32. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.
5.3.33. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.
5.3.34. Deve possuir controle de dispositivos externos.

7. Smartphones e tablets

7.1. Compatibilidade:

7.1.1. Suportar o Android das versões: 5.0 ao 13.

7.2. Características:

7.2.1. Deve prover as seguintes proteções:
7.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
7.2.1.2. Proteção contra adware e autodialers;
7.2.1.3. Todos os objetos transmitidos;
7.2.1.4. Arquivos abertos no smartphone;
7.2.1.5. Programas instalados usando a interface do smartphone
7.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
7.2.2. Deverá isolar em área de backup os arquivos infectados;
7.2.3. Deverá atualizar as bases de vacinas de modo agendado;
7.2.4. Capacidade de desativar por política:
7.4.2.1. Wi-fi;
7.4.2.2. Câmera;
7.4.2.3. Bluetooth.
7.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
7.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
7.2.7. Deverá ter firewall pessoal;
7.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente;
7.2.9. Capacidade de enviar comandos remotamente de:
7.2.9.1. Localizar;
7.2.9.2. Bloquear.
7.2.10. Capacidade de detectar Root nos dispositivos;
7.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos;
7.2.12. Capacidade de bloquear o acesso a sites phishing ou maliciosos;
7.2.13. Capacidade de configurar White e blacklist de aplicativos;
7.2.14. Capacidade de localizar o dispositivo quando necessário;
7.2.15. Permitir atualização das definições quando estiver em “roaming”;
7.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
7.2.17. Capacidade de agendar uma verificação;
7.2.18. Capacidade de enviar URL de instalação por e-mail;
7.2.19. Capacidade de fazer a instalação do agente através de um link QRCode;

7.2.20. Capacidade de executar as seguintes ações caso a desinfecção falhe:
- Deletar;
- Ignorar;
- Fazer backup;
- Perguntar ao usuário.

8. Gerenciamento de dispositivos móveis (MDM) - Android

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:
8.1.1.1. Do Android versão 5.0 a 12

8.1.2. Deverá possuir integração com sistemas de gerenciamentos:
8.1.2.1. VMWare AirWatch 9.3;
8.1.2.2. MobileIron;
8.1.2.3. IBM Maas360;
8.1.2.4. Microsoft Intune;
8.1.2.5. SOTI MobiControl;

8.2. Características:

8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
8.2.2. Capacidade de ajustar as configurações de:
8.2.2.1. Sincronização de e-mail;
8.2.2.2. Uso de aplicativos;
8.2.2.3. Senha do usuário;
8.2.2.4. Criptografia de dados;
8.2.2.5. Conexão de mídia removível.
8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
8.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
8.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;
8.2.6. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
8.2.7. Capacidade de sincronizar com Samsung Knox;

9. Gerenciamento de dispositivos móveis (MDM) – iOS

9.1. Compatibilidade:

9.1.1. Ser compatível com dispositivos com os sistemas operacionais:
9.1.1.1. iOS 10.0 – 10.3.3
9.1.1.2. iOS 11.0 – 11.3
9.1.1.3. iOS 12.0
9.1.1.4. iOS 13.0 ou superior
9.1.1.5. IPadOS 13 ao 15

9.2. Características:

9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
9.2.2. Capacidade de ajustar as configurações de:
9.2.2.1. Sincronização de e-mail;

9.2.2.2. Senha do usuário;
9.2.2.3. Criptografia de dados;
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
9.2.4. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:
9.2.4.1. Link por e-mail;
9.2.4.2. Link por mensagem de texto;
9.2.4.3. QR Code
9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

/////

ANEXO II

REQUISITOS BÁSICOS DE ENGENHARIA DE SEGURANÇA E MEDICINA DO TRABALHO

1. INTRODUÇÃO

O presente anexo tem por objetivo determinar parâmetros de Engenharia de Segurança e Medicina do Trabalho com relação à prestação de serviços pela empresa CONTRATADA nas dependências do CONTRATANTE sempre atendendo ao cumprimento da Portaria 3.214/78 do Ministério do Trabalho, e todas as suas atualizações, bem como as legislações complementares que regem a presente matéria. O cumprimento das legislações pertinentes a essa matéria, estará sob a coordenação do Serviço Especializado em Engenharia de Segurança e Medicina do Trabalho (SESMT) da CONTRATANTE.

2. OBRIGAÇÕES DA CONTRATADA

2.1 A CONTRATADA obriga-se a cumprir integralmente as presentes instruções no tocante a Engenharia de Segurança e Medicina do Trabalho, com o objetivo de proteger os funcionários de ambas as partes e demais bens e equipamentos próprios da CONTRATANTE, sem qualquer restrição à supervisão do SESMT.

2.2 A CONTRATADA obriga-se a cumprir e respeitar as determinações do presente documento e as Normas de Engenharia de Segurança e Medicina do Trabalho vigentes no âmbito da CONTRATANTE e, em nenhuma hipótese poderá alegar desconhecimento das mesmas, ficando responsável pelos atos de seus empregados decorrentes da inobservância das mesmas.

2.3 A CONTRATADA obriga-se a ter implementado GERENCIAMENTO DE RISCOS OCUPACIONAIS (GRO) e neste, constituir o PROGRAMA DE GERENCIAMENTO DE RISCOS (PGR), incluindo o INVENTÁRIO DE RISCOS ESPECÍFICO e o PROGRAMA DE CONTROLE MÉDICO DE SAÚDE OCUPACIONAL (PCMSO) aos seus empregados de acordo com o que estabelece a NR-1 e NR-7 aprovadas pela portaria 3.214 de 08 de junho de 1978. Em especial a CONTRATADA deverá observar as adequações à NR-32, conforme o trabalho executado por seus empregados nas dependências da CONTRATANTE.

2.4 A CONTRATADA compromete-se a manter arquivado e à disposição, tanto da supervisão da CONTRATANTE como por parte de fiscalizações oficiais, cópia da carteira de vacinação; com as seguintes vacinas: *COVID-19, hepatite B, tríplice viral (sarampo, rubéola e caxumba – SRC), dupla adulto (difteria e tétano – DT), varicela* e todas as campanhas preconizadas pelo Ministério da Saúde.

2.4.1 A CONTRATADA compromete-se a manter arquivado e à disposição a primeira via do ATESTADO DE SAÚDE OCUPACIONAL (ASO) dos seus empregados que vierem a operar neste contrato conforme previsto na NR-7 da Portaria já referida no item acima. Em especial o Programa de Vacinação deverá constar como item de adequação a NR-32, incluindo o resultado da soroconversão para Hepatite B.

2.5 A CONTRATADA deve encaminhar a Engenharia de Segurança do Trabalho da CONTRATANTE uma relação documental de acordo com o explicitado abaixo, a saber:

2.5.1 COMPOSIÇÃO DOCUMENTAL REQUERIDA AOS PRESTADORES DE SERVIÇOS NO CSSBC.

Base Legal**:** Em atendimento à Portaria 3.214/78, Norma Regulamentadora NR-1 (Disposições Gerais), ao Artigo 927 do Código Civil, e em observância às Normas de Segurança do Trabalho, a CONTRATADA deve fornecer em até 07 dias corridos da data de assinatura do contrato, cópias das seguintes documentações:

- Relação de funcionários contendo unidade de trabalho, nome completo, função, idade, RG e CPF.
- Cópia da Ficha de Registro de empregados ou livro de Registro;

- Cópia da Carteira de Trabalho e Previdência Social - CTPS (Páginas da Foto e qualificação civil, página do último contrato de trabalho e página seguinte);
- Cópia das Fichas de Equipamento de Proteção Individual- EPI e Equipamento de Proteção Coletiva- EPC, fornecido aos colaboradores para as atividades a serem desempenhadas;
- Cópia atualizada do Gerenciamento do Riscos Ocupacionais – GRO;
- Cópia atualizada do Programa de Gerenciamento de Riscos – PGR;
- Cópia atualizada do Programa de Controle Medico de Saúde Ocupacional – PCMSO;
- Cópia do Atestado de Saúde Ocupacional - ASO's, Exames complementares pertinentes a cada função e ao Risco de cada atividade;
- Cópia atualizada da Carteira de Vacinação, contendo as seguintes vacinas: hepatite B, gripe influenza – H1N1 (do ano vigente), tríplice viral (sarampo, rubéola e caxumba – SRC), dupla adulto (difteria e tétano – DT), varicela e todas as campanhas preconizadas pelo Ministério da Saúde;
- Lista com as ferramentas e equipamentos a serem utilizados em cada função;
- Análise Preliminar de Risco (APR) para quaisquer atividades de risco (Altura, Espaço Confinado, Alta Tensão, Trabalho a Quente e etc);
- Cópia da Ordem de Serviço (NR-1) - sobre segurança e saúde no trabalho, evidenciando a ciência dos funcionários envolvidos na tarefa;
- Liberação de participação da equipe em treinamento de integração, fluxo de acidente e instruções básicas sobre o Plano de Atendimento a Emergência - PAE na unidade de destino ou labor;
- Cópia do processo eleitoral de CIPA, Ata de instalação e posse e atas de reuniões mensais. Caso a empresa não constitua CIPA, apresentar carta de designado;
- Cópia de todas as Ficha de Informação de Segurança de Produtos Químicos – FISPQ. Caso a empresa utilize produtos químicos para execução da tarefa.

2.5.1.1 DOCUMENTOS COMPLEMENTARES RELACIONADOS A NATUREZA DA ATIVIDADE:

- Cópia do Certificado de HABILITAÇÃO e/ou Qualificação Profissional;
- Cópia do (s) Certificado (s) de Treinamentos Ministrados de Saúde e Segurança do Trabalho e Meio Ambiente:
    - NR-10 - Para atividades com energia elétrica em geral;
    - SEP- Sistema elevado de Potência - Para atividades com energia elétrica de alta tensão;
    - NR-33 - Para atividades em espaço confinado;
    - NR-35 - Para atividades de trabalho em altura.

2.5.2 Em caso de trabalho em espaço confinado, A CONTRATADA deve fornecer a CONTRANTE uma cópia do Permissão de Entrada e Trabalho (PET) e nos convocar para participar da instrução à equipe envolvida na tarefa.

2.5.3 A CONTRATADA deve informar imediatamente a CONTRATANTE quando ocorrer qualquer alteração em seu quadro funcionários e enviar toda a documentação relacionada acima.

2.5.4 As informações devem ser renovadas de acordo com os prazos legais, na ausência deste seguir os prazos determinados pela CONTRATANTE, sendo este semestralmente.

2.6 A CONTRATADA deve providenciar crachá de identificação, de uso obrigatório, para todos os funcionários que estiverem prestando serviço nas instalações da CONTRATANTE**,** especificando o cargo ocupado pelos mesmos.

2.7 Todo primeiro dia útil do mês, a CONTRATADA deve enviar cronograma de atividades ordinárias ao setor da Engenharia de Segurança do Trabalho da CONTRATANTE. Em caso de atividade extraordinárias, a CONTRATADA deve enviar de imediato cronograma compatível para ciência e a programação para acompanhamento da Engenharia de Segurança do Trabalho da CONTRATANTE.

3. DESTAQUES SOBRE AS NORMAS REGULAMENTADORAS

3.1 A CONTRATADA deve obrigatoriamente adotar as medidas de proteção previstas em todas as NRs que forem aplicáveis ao seu processo de trabalho dentro das instalações da CONTRATANTE**.**

4. ESCLARECIMENTOS SOBRE PREVENÇÃO CONTRA INCÊNDIO

4.1 É proibido fumar em toda área interna das unidades da CONTRATANTE, Decreto 2018 de 01.10.96 que regulamenta a Lei 9294 de 15.07.96, nos termos do 4º do art. 220 da Constituição.

4.2 É proibido abrir válvula dos hidrantes, retirar mangueiras ou usá-las para qualquer finalidade sem prévio conhecimento e anuência da Engenharia de Segurança do Trabalho.

4.3 Os extintores de incêndio não devem ser retirados de seus pontos fixos sob nenhuma alegação, sem prévio conhecimento e anuência do Engenharia de Segurança do Trabalho.

4.4 Comunicar com antecedência à Engenharia de Segurança do Trabalho quaisquer intervenções que se fizerem necessárias para execução dos serviços no sistema de detecção, alarme e combate à incêndios, bem como realocação de equipamentos e periféricos.

4.5 Quando for necessária alteração de layout (pequenas obras) da área útil ocupada pela CONTRATADA, está deve comunicar previamente a Engenharia de Segurança do Trabalho da CONTRATANTE.

5. EQUIPAMENTOS DE PROTEÇÃO INDIVIDUAL

5.1 A CONTRATADA deve fornecer e obrigar ao uso de todos os Equipamentos de Proteção Individual (EPI) que se fizerem necessários para a execução das tarefas correspondentes.

Deve observar os seguintes aspectos com relação à melhor adequação dos mesmos:

5.1.1 Deve selecionar o EPI adequação e seguir as recomendações da NR-6;

5.1.2 Ser de boa qualidade;

5.1.3 Possuir Certificado de Aprovação (CA) válido pelo Ministério do Trabalho e Previdência (MTP).

5.2 Os Equipamentos de Proteção Individual devem ser mantidos em perfeitas condições de uso e em bom estado de higienização, devendo ser armazenados em local próprio, longe de qualquer outro material. O referido equipamento deverá ser fornecido gratuitamente ao funcionário.

5.3 A CONTRATADA deve ter documentado a entrega dos referidos equipamentos aos seus funcionários, bem como fazer orientação sobre a obrigatoriedade de seu uso.

5.4 A CONTRATADA deve manter nas instalações cedidas pelo CONTRATANTE, estoque dos EPIs utilizados por seus funcionários, a fim de que não falte em caso de substituição por perda, extravio ou qualquer outro motivo.

5.5 A CONTRATANTE reserva-se o direito de suspender o serviço, sem gerar qualquer ônus por tal interrupção, quando for detectado a falta do conjunto de EPIs necessários à execução do serviço.

5.6 A CONTRATANTE deve deixar a disposição dos funcionários da CONTRATADA os itens de proteção individual descartáveis que compõem suas instalações, nas atividades específicas que os demandam, a saber:

- Máscara descartável;
- Gorro descartável;
- Pro-pé descartável;
- Luva descartável;
- Avental descartável.

5.7 A CONTRATADA pode solicitar a Engenharia de Segurança do Trabalho da CONTRATANTE o Certificado de Aprovação (CA) dos EPI descartáveis relacionados no item 5.6.

6. INSPEÇÕES DE SEGURANÇA

6.1 É facultado à CONTRATANTE**,** através de sua Engenharia de Segurança do Trabalho**,** realizar inspeções periódicas nas instalações tanto quanto no local de execução dos serviços da CONTRATADA, com vistas a verificar o cumprimento das determinações legais bem como as recomendações constantes neste Documento, ou ainda recomendações de caráter geral, sempre com o objetivo de cumprir as legislações vigentes, os protocolos institucionais e assim, evitar Acidentes de Trabalho ou Doenças Profissionais.

6.2 A CONTRATANTE**,** através de sua Engenharia de Segurança do Trabalho**,** pode suspender qualquer trabalho no qual se evidencie risco iminente, ameaçando a integridade física dos funcionários de ambas as partes, ou ainda que possa resultar em prejuízo material de grande monta para a própria CONTRATANTE**.**

6.3 As irregularidades apontadas nas Inspeções devem ser sanadas pela CONTRATADA**,** sob pena de sofrer suspensão do trabalho.

7. COMUNICAÇÃO DE ACIDENTES DE TRABALHO

7.1 Quando da ocorrência de Acidente de Trabalho, com o funcionário da CONTRATADA**,** este deve seguir o Fluxo de Acidente do Trabalho da CONTRATADA na unidade de labor, tanto para acidente biológico, não biológico e trajeto.

7.2 A CONTRATADA deve emitir a CAT - Comunicação de Acidente de Trabalho, e informar de imediato a Engenharia de Segurança do Trabalho da CONTRATANTE, fornecendo cópia deste documento.

7.3 Todo Acidente de Trabalho, com ou sem perda de tempo, deve ser comunicado através de relatório ao SESMT da CONTRATANTE**,** da maneira mais detalhada possível, preferencialmente, na data de ocorrência do mesmo.

8. TREINAMENTOS E EDUCAÇÃO CONTINUADA

8.1 Os funcionários da CONTRATADA devem receber capacitação continuada, seguida de acompanhamento e avaliação (ênfase no uso de proteção individual e conhecimento de procedimentos operacionais) antes de iniciar as atividades nas dependências da CONTRATANTE**,** para que a qualidade dos serviços sejam sempre a mesma e para evitar Acidentes de Trabalho.

8.2 A CONTRATADA deve disponibilizar a relação de nomes e RG dos funcionários que prestarão serviços na CONTRATANTE em até 07 dias corridos da data de assinatura do contrato, para realização do treinamento de integração.

8.3 A CONTRATADA deve enviar atualização dos nomes dos funcionários sempre que houver mudança.

8.4 Os funcionários da CONTRATADA devem receber treinamento em relação aos produtos químicos, como por exemplo: *fumos metálicos, cola de contato, tinta, solventes, particulados sólidos de mercúrio nas lâmpadas fluorescentes e etc.*

8.5 Em caso de trabalho em altura, a CONTRATADA deve evidenciar treinamento para execução da atividade em conformidade com a NR-35, inclusive destinar um técnico de segurança do trabalho para acompanhamento.

8.6 Em caso de trabalho em espaço confinado, a CONTRATADA deve evidenciar o treinamento para execução da atividade em conformidade com a NR-33, inclusive destinar um técnico de segurança do trabalho para acompanhamento.

8.7 A CONTRATADA deve apresentar cópia do Programa de Treinamento, mencionado no itens 8.1 e 8.2, bem como as atualizações que vier a fazer do mesmo, observando os dispostos na NR-32.

8.8 A CONTRATADA deve liberar seus funcionários para treinamento de integração, fluxo de acidente do trabalho e Instruções básicas sobre o Plano de Atendimento a Emergência - PAE na unidade de destino ou labor.

9. DISPOSIÇÕES GERAIS

9.1 A CONTRATADA**,** que pelo número de funcionários não for obrigada a manter pessoal especializado em Engenharia de Segurança e Medicina do Trabalho, como previsto na NR-4, deverá designar profissional da área, para que uma vez por mês mantenha intercâmbio com o SESMT da CONTRATANTE**,** sobre as ocorrências e possíveis sugestões para o bom desenvolvimento do trabalho.

9.5. Qualquer interrupção ou suspensão dos trabalhos, motivados pela não observância das instruções constantes neste documento, não exime a CONTRATADA das obrigações contratuais e penalidades constantes das cláusulas contratuais referentes a multa e prazos.

9.3 A CONTRATADA deve atender ao disposto no Quadro I da NR-5, da portaria 3214/78, e encaminhar a Engenharia de Segurança do Trabalho da CONTRATANTE cópia do edital de convocação e do calendário anual de reuniões da CIPA.

9.4 Em caso de não enquadramento no Quadro I da NR-5, a CONTRATADA deve promover anualmente treinamento para o designado responsável pelo cumprimento do objetivo desta NR.

9.5 A CONTRATANTE reserva-se o direito de fazer outras exigências com respeito a Engenharia de Segurança e Medicina do Trabalho, sempre que julgue necessário, para a proteção dos funcionários e bens materiais de sua propriedade.

9.6 A CONTRATADA deve obedecer às legislações pertinentes ao destino de Resíduos Sólidos, em especial a RDC 306 da ANVISA, tendo inclusive PGRSS próprio, caso seja da área de saúde.

Assinado eletronicamente por: Walter Ferreira
Motivo: Estou de acordo com o conteúdo deste documento
Data: 1 de Agosto de 2023 16:47 ADT

Assinado eletronicamente por: Eduardo Sukarie
Motivo: Estou de acordo com o conteúdo deste documento
Data: 1 de Agosto de 2023 16:55 ADT

Assinado eletronicamente por: Agnes Mello Farias Ferrari
Motivo: Estou de acordo com o conteúdo deste documento
Data: 2 de Agosto de 2023 17:16 ADT

Assinado eletronicamente por: Luís H. Cambraia Galvão
Motivo: Estou de acordo com o conteúdo deste documento
Data: 1 de Agosto de 2023 17:39 ADT

Assinado eletronicamente por: Mariana Nascimento Sousa
Motivo: Estou de acordo com o conteúdo deste documento
Data: 1 de Agosto de 2023 17:41 ADT

Assinado eletronicamente por: j RAMDE
Motivo: Estou de acordo com o conteúdo deste documento
Data: 2 de Agosto de 2023 15:22 ADT

Termo contratual - Prestação de serviços de licença de antivírus para estações de trabalho e servidores Windows, pelo período de 24 (vinte e quatro) meses.

Relatório de auditoria final 2023-08-02

Criado em:	2023-08-01
Por:	Michele Leocadio (michele.leocadio@brasoftware.com.br)
Status:	Assinado
ID da transação:	CBJCHBCAABAAwAyACmC9czHQpGg0zsszLj42PQcRuUaI
Quantidade de documentos:	1
Contagem de páginas do documento:	29
Quantidade de arquivos de apoio:	0
Contagem de páginas dos arquivos de apoio:	0

Histórico de "Termo contratual - Prestação de serviços de licença de antivírus para estações de trabalho e servidores Windows, pelo período de 24 (vinte e quatro) meses."

Documento criado por Michele Leocadio (michele.leocadio@brasoftware.com.br)
2023-08-01 - 19:43:47 GMT- Endereço IP: 187.122.57.4

Documento enviado por email para Walter Ferreira (walter.ferreira@brasoftware.com.br) para assinatura
2023-08-01 - 19:46:11 GMT

Email visualizado por Walter Ferreira (walter.ferreira@brasoftware.com.br)
2023-08-01 - 19:46:45 GMT- Endereço IP: 104.47.58.126

Contrato visualizado por Walter Ferreira (walter.ferreira@brasoftware.com.br)
2023-08-01 - 19:46:46 GMT- Endereço IP: 104.47.58.126

Documento assinado eletronicamente por Walter Ferreira (walter.ferreira@brasoftware.com.br)
Motivo da assinatura: Estou de acordo com o conteúdo deste documento
Data da assinatura: 2023-08-01 - 19:47:21 GMT - Fonte da hora: servidor- Endereço IP: 191.181.59.173

Documento enviado por email para Eduardo Sukarie (eduardo.sukarie@brasoftware.com.br) para assinatura
2023-08-01 - 19:47:23 GMT

Email visualizado por Eduardo Sukarie (eduardo.sukarie@brasoftware.com.br)
2023-08-01 - 19:54:29 GMT- Endereço IP: 172.226.102.16

Contrato visualizado por Eduardo Sukarie (eduardo.sukarie@brasoftware.com.br)
2023-08-01 - 19:54:34 GMT- Endereço IP: 104.47.70.126

Documento assinado eletronicamente por Eduardo Sukarie (eduardo.sukarie@brasoftware.com.br)
Motivo da assinatura: Estou de acordo com o conteúdo deste documento
Data da assinatura: 2023-08-01 - 19:55:25 GMT - Fonte da hora: servidor- Endereço IP: 138.117.145.150

Documento enviado por email para luis.galvao@chmsbc.org.br para assinatura
2023-08-01 - 19:55:27 GMT

Email visualizado por luis.galvao@chmsbc.org.br
2023-08-01 - 20:37:05 GMT- Endereço IP: 201.72.58.140

Contrato visualizado por luis.galvao@chmsbc.org.br
2023-08-01 - 20:37:06 GMT- Endereço IP: 201.72.58.140

O signatário luis.galvao@chmsbc.org.br inseriu o nome Luís H. Cambraia Galvão ao assinar
2023-08-01 - 20:39:28 GMT- Endereço IP: 201.72.58.140

Documento assinado eletronicamente por Luís H. Cambraia Galvão (luis.galvao@chmsbc.org.br)
Motivo da assinatura: Estou de acordo com o conteúdo deste documento
Data da assinatura: 2023-08-01 - 20:39:30 GMT - Fonte da hora: servidor- Endereço IP: 201.72.58.140

Documento enviado por email para juridico@chmsbc.org.br para assinatura
2023-08-01 - 20:39:32 GMT

Email visualizado por juridico@chmsbc.org.br
2023-08-01 - 20:40:10 GMT- Endereço IP: 201.72.58.140

Contrato visualizado por juridico@chmsbc.org.br
2023-08-01 - 20:40:11 GMT- Endereço IP: 201.72.58.140

O signatário juridico@chmsbc.org.br inseriu o nome Mariana Nascimento Sousa ao assinar
2023-08-01 - 20:41:32 GMT- Endereço IP: 201.72.58.140

Documento assinado eletronicamente por Mariana Nascimento Sousa (juridico@chmsbc.org.br)
Motivo da assinatura: Estou de acordo com o conteúdo deste documento
Data da assinatura: 2023-08-01 - 20:41:34 GMT - Fonte da hora: servidor- Endereço IP: 201.72.58.140

Documento enviado por email para ramde.jardim@chmsbc.org.br para assinatura
2023-08-01 - 20:41:35 GMT

Email visualizado por ramde.jardim@chmsbc.org.br
2023-08-02 - 1:54:19 GMT- Endereço IP: 187.74.204.159

Contrato visualizado por ramde.jardim@chmsbc.org.br

2023-08-02 - 18:21:24 GMT- Endereço IP: 189.1.163.210

O signatário ramde.jardim@chmsbc.org.br inseriu o nome j RAMDE ao assinar

2023-08-02 - 18:22:44 GMT- Endereço IP: 189.1.163.210

Documento assinado eletronicamente por j RAMDE (ramde.jardim@chmsbc.org.br)

Motivo da assinatura: Estou de acordo com o conteúdo deste documento

Data da assinatura: 2023-08-02 - 18:22:46 GMT - Fonte da hora: servidor- Endereço IP: 189.1.163.210

Documento enviado por email para agnes.ferrari@chmsbc.org.br para assinatura

2023-08-02 - 18:22:49 GMT

Email visualizado por agnes.ferrari@chmsbc.org.br

2023-08-02 - 19:56:22 GMT- Endereço IP: 189.126.205.55

Contrato visualizado por agnes.ferrari@chmsbc.org.br

2023-08-02 - 19:56:28 GMT- Endereço IP: 189.126.205.55

O signatário agnes.ferrari@chmsbc.org.br inseriu o nome Agnes Mello Farias Ferrari ao assinar

2023-08-02 - 20:15:59 GMT- Endereço IP: 177.26.237.198

Documento assinado eletronicamente por Agnes Mello Farias Ferrari (agnes.ferrari@chmsbc.org.br)

Motivo da assinatura: Estou de acordo com o conteúdo deste documento

Data da assinatura: 2023-08-02 - 20:16:01 GMT - Fonte da hora: servidor- Endereço IP: 177.26.237.198

Contrato finalizado.

2023-08-02 - 20:16:01 GMT