Licitação Eletrônica nº 2022/25

CONTRATO PARA PRESTAÇÃO DE SERVIÇOS

DGCO nº 00185/2022
OC nº 193737

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DECORRENTE DA LICITAÇÃO ELETRÔNICA Nº 2022/25 – LOTE ÚNICO REALIZADA EM CONFORMIDADE COM A LEI Nº 13.303, DE 30.06.2016, E O REGULAMENTO DE LICITAÇÕES E CONTRATOS DA BB TECNOLOGIA E SERVIÇOS S.A., PUBLICADO EM SUA PÁGINA ELETRÔNICA (WWW.BBTS.COM.BR), em 01.02.2018, QUE ENTRE SI FAZEM NESTA E MELHOR FORMA DE DIREITO, DE UM LADO A **BB TECNOLOGIA E SERVIÇOS S.A.**, EMPRESA COM SEDE EM BRASÍLIA/DF, INSCRITA NO CADASTRO NACIONAL DA PESSOA JURÍDICA SOB O NÚMERO 42.318.949/0013-18, ADIANTE DENOMINADA **CONTRATANTE,** REPRESENTADA PELO(S) ADMINISTRADOR(ES) NO FINAL QUALIFICADO(S) E, DO OUTRO LADO, A EMPRESA **NETSAFE CORP LTDA**, SITUADA NA TR SCES TRECHO 2, S/N, CONJ 32 PARTE R 06C PARTE 30 PARTE SALA 108 E 109, ASA SUL, BRASILIA – DF , CEP: 70.200-002, INSCRITA NO CADASTRO NACIONAL DE PESSOA JURÍDICA SOB O NÚMERO 03.476.184/0002-30, NESTE ATO REPRESENTADA NA FORMA DE SEUS ATOS CONSTITUTIVOS PELO(S) SEU(S), REPRESENTANTE(S) LEGAL(IS) AO FINAL QUALIFICADO(S) E ASSINADO(S), ADIANTE DENOMINADA **CONTRATADA**, CONSOANTE AS CLÁUSULAS ABAIXO. **A MINUTA-PADRÃO DO PRESENTE CONTRATO FOI APROVADA PELOS PARECERES JURÍDICOS Nº 602/2020 DE 01.11.2020 E Nº 1166/2022 de 06.02.2022**.

OBJETO

CLÁUSULA PRIMEIRA - O presente contrato tem por objeto a prestação de serviços de aquisição de 6.000 licenças perpétuas de solução EDR, para upgrade da solução McAfee e garantia de 36 meses, de acordo com as condições e especificações mínimas exigidas no Documento nº 1, no Edital e conforme proposta comercial do dia 06 de junho de 2022, obrigando-se a CONTRATADA a realizar as tarefas constantes do Documento nº 1 e nº 2 deste contrato.

Parágrafo Primeiro - Os serviços serão prestados diretamente pela CONTRATADA, vedada a cessão, transferência ou subcontratação, total ou parcial, exceto se previstas neste contrato.

Parágrafo Segundo - O presente contrato poderá ser alterado nas hipóteses elencadas no art. 127 do Regulamento de Licitações e Contratos da BB Tecnologia e Serviços S.A., disponibilizado no site www.bbts.com.br, desde que acordado entre as partes.

Parágrafo Terceiro – Em havendo necessidade de acréscimos ao contrato, o novo valor total pactuado não poderá ultrapassar em 25% (vinte e cinco por cento) o valor total inicial atualizado do contrato.

Parágrafo Quarto - Entende-se como VALOR TOTAL INICIAL ATUALIZADO, o valor total inicial do contrato acrescido de eventual reequilíbrio e das repactuações porventura concedidas, desconsiderando os acréscimos ou supressões realizadas.

VIGÊNCIA E RESCISÃO

CLÁUSULA SEGUNDA - A vigência deste contrato é de 36 (trinta e seis) meses, contado da assinatura do contrato, podendo ser prorrogado até o limite de 60 (sessenta) meses.

Parágrafo Primeiro - Os serviços deverão ser iniciados no prazo definido no Documento nº 1.

Parágrafo Segundo - Toda prorrogação de prazo será justificada por escrito e previamente autorizada pela CONTRATANTE, passando tal documento a integrar o contrato.

Parágrafo Terceiro – Constituem motivos, dentre outros, para a rescisão contratual:

a) Não apresentar comprovante de garantia na forma da Cláusula Sétima para o cumprimento das obrigações contratuais;

b) O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

c) O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

d) A lentidão do seu cumprimento, levando a CONTRATANTE a comprovar a impossibilidade do prosseguimento do fornecimento no prazo estipulado;

e) O atraso injustificado no início do serviço;

f) Paralisação do serviço sem justa causa e prévia comunicação à CONTRATANTE. Neste caso, a CONTRATADA responderá por eventual aumento de custos daí decorrentes e por perdas e danos que a CONTRATANTE, como consequência, venha a sofrer;

g) A subcontratação total ou parcial do seu objeto, a associação da CONTRATADA a outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital.

h) Deixar a CONTRATADA de comprovar sua habilitação, nos termos do edital, e sua capacidade econômico-financeira para a execução do contrato;

i) O desatendimento das determinações regulares da CONTRATANTE decorrentes do acompanhamento e fiscalização do contrato;

j) A decretação de falência ou a instauração de insolvência civil;

k) A dissolução da sociedade ou o falecimento do contratado;

l) A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

m) A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

n) Utilizar a CONTRATADA, em benefício próprio ou de terceiros informações sigilosas às quais tenha acesso por força de suas atribuições contratuais;

o) Deixar de comprovar os requisitos de habilitação, inclusive os que são avaliados nos documentos fiscais federais e o relativo ao FGTS dos seus empregados;

p) Vier a ser declarada inidônea pela União;

q) Vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira;

r) Praticar atos lesivos, devidamente comprovados à Administração Pública, Nacional ou Estrangeira, nos termos da Lei nº 12.846/2013;

s) Razões de interesse da CONTRATANTE, de alta relevância e amplo conhecimento, justificadas e exaradas no processo a que se refere o contrato.

Parágrafo Quarto - A rescisão deste contrato poderá ocorrer também da seguinte forma:

a) Amigavelmente, formalizada mediante acordo entre as partes à época da rescisão;

b) Judicialmente, nos termos da legislação.

Parágrafo Quinto - Os casos de rescisão contratual serão formalmente motivados nos autos do processo, observado o rito previsto no Regulamento de Licitações e Contratos da BB Tecnologia e Serviços S.A.

Parágrafo Sexto - As responsabilidades imputadas à CONTRATADA, por prejuízos decorrentes de ações delitivas perpetradas contra a CONTRATANTE, não cessam com a rescisão do contrato.

Parágrafo Sétimo - A rescisão acarretará, de imediato:

a) Execução da garantia, para ressarcimento, à CONTRATANTE, dos valores das multas aplicadas ou de quaisquer outras quantias ou indenizações a ele devidas;

b) Retenção dos créditos decorrentes do contrato, até o limite dos prejuízos causados à CONTRATANTE.

PREÇO

CLÁUSULA TERCEIRA - A CONTRATANTE pagará à CONTRATADA, a importância total estimada de R$ 1.129.980,00 (Hum Milhão, Cento e Vinte e Nove Mil e Novecentos e Oitenta Reais) para 6.000 (Seis Mil) Licenças Perpétuas com suporte por 36 (trinta e seis) meses, pela prestação dos serviços objeto deste contrato, preço apurado conforme metodologia de cálculo constante do Demonstrativo de Orçamento de Custos - Documento nº 2, que integra este contrato, sendo o valor unitário de R$ 188,33 (Cento e Oitenta e Oito Reais e Trinta e Três Centavos) .

CLÁUSULA QUARTA - Nos valores fixados na cláusula acima, estão incluídas todas as despesas necessárias à plena execução dos serviços, tais como de pessoal, de administração e todos os encargos (obrigações sociais, impostos, taxas, etc.) incidentes sobre o serviço.

CLÁUSULA QUINTA - O valor estipulado na cláusula anterior é fixo e irreajustável para o período de 36 meses.

Parágrafo Único - O disposto nesta cláusula não impede a eventual concessão de reequilíbrio contratual, na forma do § 6º do art. 81 da Lei 13.303/16.

PAGAMENTO

CLÁUSULA SEXTA - A nota fiscal/fatura deverá:

a) Conter o número da Ordem de Compra, número do DGCO do Contrato, o objeto contratual e o mês da prestação dos serviços;

b) Conter agência e número da conta corrente;

c) Conter o endereço onde os serviços foram efetivamente prestados.

d) Ser entregue à CONTRATANTE, em até 5 (cinco) dias úteis subsequentes a data de sua emissão, sendo entregue até o dia 21 (vinte e um) do mês de sua emissão, acompanhada do Documento Auxiliar da Nota Fiscal Eletrônica, relativo a prestação de serviços nos municípios em que o documento é exigido.

e) Deverá também ser informado de maneira clara, no caso de empresas não domiciliadas no local da prestação de serviço, número referente ao cadastramento de prestador de outro Município (CPOM), cadastro de empresa não estabelecida (CENE), ou similar, de acordo com exigência legal determinada pelos Municípios.

f) Nas localidades que exigem cadastramento de prestador de outro Município (CPOM), cadastro de empresa não estabelecida (CENE) ou similar de empresas não domiciliadas nas mesmas, a CONTRATADA deverá apresentar na NF-e o número do cadastro referente ao serviço prestado, ou na impossibilidade, anexar declaração formal fornecida pelo site da prefeitura.

Parágrafo Primeiro - O pagamento será creditado em conta corrente mantida preferencialmente no Banco do Brasil S.A., em nome da CONTRATADA, em 30 dias corridos a contar da emissão da Nota fiscal, acompanhado do Documento Auxiliar da Nota Fiscal Eletrônica, relativo à prestação de serviços nos municípios em que o documento é exigido.

Parágrafo Segundo - Constatando a CONTRATANTE qualquer divergência ou irregularidade na nota fiscal/fatura ou recibo de prestação de serviços, esta será devolvida à CONTRATADA em, no máximo, 2 (dois) dias úteis a contar da apresentação, acompanhada das informações correspondentes às irregularidades verificadas, para as devidas correções. Caso até o dia ajustado para o pagamento, a Nota Fiscal não tenha sido atestada pela CONTRATANTE, na forma ajustada neste contrato, por culpa da CONTRATADA, o prazo para pagamento será prorrogado para até 07 (sete) dias úteis após o ateste pela CONTRATANTE.

Parágrafo Terceiro - A CONTRATANTE efetuará a retenção e o recolhimento de tributos, quando a legislação assim exigir.

Parágrafo Quarto - A CONTRATADA que se declarar amparada por isenção de tributos, nos moldes tratados pela Instrução Normativa RFB nº 1234/12, da Receita Federal em que não ocorra a incidência ou alíquota zero, deve informar esta condição no documento fiscal, inclusive o enquadramento legal, apresentando as declarações pertinentes, conforme modelos contidos na mencionada Instrução Normativa.

GARANTIA

CLÁUSULA SÉTIMA - A CONTRATADA entregará à CONTRATANTE comprovante de garantia, em uma das modalidades previstas no Art. 70 da Lei 13.303/2016, no valor de R$ 56.499,00 (Cinquenta e Seis Mil e Quatrocentos e Noventa e Nove Reais), correspondente a 5% (cinco por cento) do valor deste contrato, como forma de garantir a perfeita execução de seu objeto.

Parágrafo Primeiro - A garantia deverá ser enviada através do e-mail contratos@bbts.com.br, no prazo máximo de 30 (trinta) dias corridos contados da data da assinatura do contrato por todos os signatários), prorrogável por mais 10 (dez) dias, mediante aceitação pela CONTRATANTE de justificativa encaminhada pela CONTRATADA, a qual deverá ser válida durante todo o período de vigência contratual, e se solicitada a via original deverá ser entregue no seguinte endereço: SEPN Comércio Residencial Norte 508 - Asa Norte, Brasília - DF, 70740-543.

Parágrafo Segundo - O pagamento das faturas poderá ser suspenso quando não apresentada a garantia, no prazo e local estipulados no parágrafo anterior.

Parágrafo Terceiro - Havendo majoração do preço contratado, fica a critério da CONTRATANTE solicitar formalmente à CONTRATADA a integralização da garantia, limitada a 5% (cinco por cento) do novo preço. No caso de supressão, a alteração na garantia para adequação ao novo valor ocorrerá mediante solicitação da CONTRATADA, respeitado o percentual de 5% (cinco por cento) do novo preço contratado.

Parágrafo Quarto - A garantia responderá pelo fiel cumprimento das disposições do contrato, ficando a CONTRATANTE autorizado a executá-la para cobrir multas, indenizações ou pagamento de qualquer obrigação, inclusive em caso de rescisão.

Parágrafo Quinto - Utilizada a garantia, a CONTRATADA obriga-se a integralizá-la no prazo de 5 (cinco) dias úteis contado da data em que for notificada formalmente pela CONTRATANTE.

Parágrafo Sexto - O valor da garantia somente será liberado à CONTRATADA quando do término ou rescisão do contrato, desde que não possua dívida inadimplida com a CONTRATANTE e mediante expressa autorização deste.

Parágrafo Sétimo - A garantia a ser apresentada responderá pelo cumprimento das obrigações da contratada eventualmente inadimplidas na vigência deste Contrato e da garantia.

CLÁUSULAS GERAIS

CLÁUSULA OITAVA - Para realização dos serviços ajustados, a CONTRATADA designará empregados de seu quadro, especializados e devidamente credenciados, assumindo total responsabilidade pelo controle de frequência, disciplina e pelo cumprimento de todas as obrigações trabalhistas, fiscais e previdenciárias, inclusive as decorrentes de acidentes, indenizações, multas, seguros, pagamentos a fornecedores diretos, normas de saúde pública e regulamentadoras do trabalho, assim como pelo cumprimento de todas as demais obrigações atinentes ao presente contrato.

Parágrafo Primeiro - A inadimplência da CONTRATADA, com referência aos encargos mencionados nesta cláusula, não transfere à CONTRATANTE a responsabilidade por seu pagamento. Caso venha a CONTRATANTE a satisfazê-los ser-lhe-á assegurado direito de regresso, sendo os valores pagos atualizados financeiramente, desde a data em que tiverem sido pagos pela CONTRATANTE até aquela em que ocorrer o ressarcimento pela CONTRATADA.

Parágrafo Segundo - A CONTRATANTE poderá exigir, a qualquer momento, a comprovação do cumprimento das obrigações mencionadas no *"caput"* desta cláusula.

Parágrafo Terceiro - A CONTRATADA se obriga a substituir, mediante solicitação formal e a critério da CONTRATANTE, quaisquer de seus empregados designados para executar as tarefas pertinentes a este contrato, que não esteja correspondendo aos padrões estabelecidos pela CONTRATANTE. A CONTRATADA terá o prazo de 48 (quarenta e oito) horas, a contar da data da solicitação, para proceder à troca, sob pena de multa.

Parágrafo Quarto - Será de inteira responsabilidade da CONTRATADA o cumprimento das normas regulamentares da "Segurança e Medicina do Trabalho" cabíveis, bem como, se for o caso, a obrigação de organizar "Comissão Interna de Prevenção de Acidentes - CIPA."

Parágrafo Quinto - O não cumprimento das obrigações mencionadas no *caput* desta cláusula ensejará a instauração de processo administrativo em desfavor da CONTRATADA para aplicação das penalidades previstas por este instrumento contratual, sem prejuízo de eventual rescisão do contrato.

Parágrafo Sexto - Quando solicitada pela CONTRATANTE, a CONTRATADA deverá preencher, assinar e encaminhar o FQ415-042 - Questionário de Due Diligence (Documento nº 4) com as devidas evidências, no prazo máximo de 3 (três) dias úteis, contados da solicitação do envio do documento, observando que a entrega do questionário respondido é fato determinante para a assinatura de contrato e seus respectivos aditamentos.

CLÁUSULA NONA - A CONTRATADA se compromete a fornecer, por escrito e mediante solicitação da CONTRATANTE, relatório sobre os serviços prestados, acatando sugestões motivadas, visando corrigir possíveis falhas e melhor atender às necessidades da CONTRATANTE.

CLÁUSULA DÉCIMA - A CONTRATADA se obriga a manter, durante a vigência do contrato, todas as condições de habilitação exigidas na licitação. Assume, ainda, a obrigação de apresentar, no término do prazo de validade de cada um, os seguintes documentos:

a) Prova de regularidade com a Fazenda Nacional, mediante apresentação de certidão Unificada, expedida conjuntamente pela Secretaria da Receita Federal do Brasil - RFB e pela Procuradoria-Geral da Fazenda Nacional - PGFN, referente a todos os tributos federais e à Dívida Ativa da União - DAU, por elas administrados, inclusive contribuições previdenciárias;

b) Prova de regularidade perante o FGTS - Fundo de Garantia do Tempo de Serviço, mediante apresentação do CRF - Certificado de Regularidade de Fundo de Garantia, fornecido pela Caixa Econômica Federal;

Parágrafo Primeiro - A CONTRATADA estará dispensada de apresentar os documentos de que trata as alíneas “a” e “b” acima, caso seja possível, à CONTRATANTE, verificar a regularidade da situação da CONTRATADA por meio de consulta on-line ao SICAF.

Parágrafo Segundo - Se a CONTRATADA estiver desobrigada da apresentação de quaisquer documentos solicitados nesta cláusula deverá comprovar esta condição por meio de certificado expedido por órgão competente ou legislação em vigor.

Parágrafo Terceiro - Além dos documentos relacionados no *caput* desta cláusula, a CONTRATADA deverá apresentar à CONTRATANTE os seguintes documentos:

a) Anualmente: balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, acompanhado do demonstrativo das contas de lucros e prejuízos que comprovem possuir a CONTRATADA boa situação financeira;

CLÁUSULA DÉCIMA PRIMEIRA - A CONTRATADA declara e obriga-se a:

a) Exercer suas atividades em conformidade com a legislação vigente;

b) Não se utilizar direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, de trabalho ilegal e/ou análogo ao escravo;

c) Não empregar direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, menor de 18 (dezoito) anos em trabalho noturno, insalubre ou perigoso;

d) Não empregar direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, menor de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, e, neste caso, o trabalho não poderá ser perigoso ou insalubre, ocorrer em horário noturno e/ou de modo a não permitir a frequência escolar;

e) Não se utilizar de práticas de discriminação negativa e limitativas para o acesso e manutenção do emprego, tais como por motivo de sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar, estado gravídico etc.;

f) Proteger e preservar o meio ambiente, prevenindo práticas danosas e executando seus serviços em observância à legislação vigente, principalmente no que se refere aos crimes ambientais;

g) Observar e cumprir as disposições contidas na Lei 12.846/2013, incluindo, mas não se limitando a, não se utilizar de práticas corruptas e/ou antiéticas visando obter ou dar vantagem indevida, de forma direta ou indireta, perante a CONTRATANTE.

Parágrafo Único - A CONTRATADA declara que o seu quadro societário não é integrado por atual ou ex-agente da CONTRATANTE, que tenha sido dispensado, exonerado, destituído, demitido ou aposentado no período de 6 (seis) meses da data da respectiva desvinculação com a administração pública, ou de parentes dos mesmos, em até terceiro grau.

CLÁUSULA DÉCIMA SEGUNDA – A contratada (e suas coligadas ou as consorciadas), no âmbito deste contrato, declara(m) e se compromete(m) a:

a) Adotar boas práticas de preservação ambiental, protegendo o meio ambiente, prevenindo práticas danosas e executando seus serviços em observância à legislação vigente, principalmente no que se refere aos crimes ambientais.

b) Não constar, esta empresa e seus sócios-diretores, em listas oficiais por infringir as regulamentações pertinentes a valores socioambientais, bem como não contratar pessoas físicas ou jurídicas, dentro de sua cadeia produtiva, que constem de tais listas;

c) Repudiar condutas que possam caracterizar assédio de qualquer natureza.

d) Combater práticas de exploração sexual de crianças e adolescentes.

e) Respeitar à Declaração Universal dos Direitos Humanos combatendo à discriminação em todas as suas formas.

f) Reconhecer, aceitar e valorizar a diversidade do conjunto de pessoas que compõem a empresa.

g) Obedecer e fazer com que seus empregados, representantes e fornecedores obedeçam a toda legislação, normas e regulamentos aplicáveis à condução dos projetos sociais.

h) Respeitar à livre associação sindical e direito à negociação coletiva.

i) Cumprir a legislação trabalhista e previdenciária.

j) Disseminar práticas de responsabilidade socioambiental na cadeia de fornecedores.

k) Criar ou reforçar, bem como manter, todas as ações e procedimentos necessários para que as pessoas que integram as suas estruturas da empresa conheçam as leis a que estão vinculadas, em especial art. 299 do Código Penal Brasileiro, artigo 5º da Lei 12.846/2013 e art. 90 da Lei 8.666/1993 e art. 1º da Lei 9.613/1998, ao atuarem em seu nome ou em seu benefício, para que possam cumpri-las integralmente, especialmente, na condição de fornecedor de bens e serviços para a CONTRATANTE;

l) Vedar que qualquer pessoa ou organização que atue em seu nome ou em seu benefício prometa, ofereça, comprometa-se a dar qualquer tipo de vantagem indevida, de forma direta ou indireta, a qualquer empregado da CONTRATANTE, ou a qualquer pessoa ou empresa em nome da CONTRATANTE.

m) Não financiar, custear, patrocinar ou subvencionar a prática dos atos ilícitos;

n) Proibir ou reforçar a proibição de que qualquer pessoa ou organização que aja em seu nome, seja como representante, agente, mandatária ou sob qualquer outro vínculo, utilize qualquer meio imoral ou antiético nos relacionamentos com empregados da CONTRATANTE;

o) Não fraudar, tampouco manipular o equilíbrio econômico-financeiro dos contratos celebrados com a CONTRATANTE e não criar pessoa jurídica de modo fraudulento ou irregular para celebrar contrato administrativo;

p) Apoiar e colaborar com a CONTRATANTE e demais órgãos, entidades ou agentes públicos em qualquer apuração de suspeita de irregularidades e/ou violação da lei, refletidos nesta declaração, sempre em estrito respeito à legislação vigente.

q) E, ainda, declara que:

i. Tem ciência e se obriga a cumprir integralmente a Lei nº 12.846/2013, observados os atos considerados lesivos à administração pública relacionados no artigo 5º do respectivo normativo legal e a responsabilização e aplicação administrativa e civil que é atribuída à pessoa jurídica em razão do seu cometimento;

ii. O conteúdo da proposta apresentada não foi informado ou discutido com ou recebido de qualquer outro participante do presente certame, por qualquer meio ou por qualquer pessoa antes da abertura oficial das propostas;

iii. Tem ciência de que, conforme disposto no artigo 30 da Lei 12.846/2013, não se afasta o processo de responsabilização e aplicação das penalidades decorrentes de: I – ato de improbidade administrativa nos termos da Lei 8.429, de junho de 1992; e, II – atos ilícitos alcançados pela Lei nº 8.666, de 21 de junho de 1993, ou outras normas de licitações e contratos da administração pública, inclusive no tocante ao Regime Diferenciado de Contratações Públicas – RDC instituído pela Lei 12.462, de 4 de agosto de 2011. III – Atos que configurem prática de lavagem ou ocultação de bens direitos e valores alcançados pela Lei nº 9.613/1998.

iv. Que o descumprimento das alíneas “k” a “p” ensejará penalidades de acordo com o art. 299 do Código Penal Brasileiro, artigo 5º da Lei 12.846/2013 e art. 90 da Lei 8.666/1993.

CLÁUSULA DÉCIMA TERCEIRA - Os serviços objeto deste contrato serão fiscalizados por representantes ou comissão de representantes da CONTRATANTE, que terão a atribuição de prestar orientações gerais e exercer o controle e a fiscalização da execução contratual. As orientações serão prestadas diretamente ao preposto da CONTRATADA, designado por ocasião da assinatura do presente contrato.

Parágrafo Único - A ação da fiscalização não exonera a CONTRATADA de cumprir as obrigações contratuais assumidas neste contrato.

CLÁUSULA DÉCIMA QUARTA - Qualquer reclamação sobre a inexecução ou deficiente execução dos serviços ora contratados, deverá ser feita pela CONTRATANTE à CONTRATADA, por escrito, podendo ser entregue mediante protocolo - Aviso de Recebimento (AR) ou por outros meios com confirmação de recebimento. O não atendimento aos termos da reclamação a que alude esta cláusula, dentro de 5 (cinco) dias úteis a contar da data da entrega da reclamação, facultará a rescisão contratual, sem prejuízo do disposto na Cláusula Décima Quinta e da aplicação das penalidades estabelecidas neste contrato.

CLÁUSULA DÉCIMA QUINTA - A CONTRATADA responderá pecuniariamente por danos e/ou prejuízos que forem causados à CONTRATANTE, ou a terceiros, decorrentes de falha dos serviços ora contratados, inclusive os motivados por greves ou atos dolosos de seus empregados. Assume a CONTRATADA, nesse caso, a obrigação de efetuar a respectiva indenização até o 5º (quinto) dia útil após a comunicação, que lhe deverá ser feita por escrito.

CLÁUSULA DÉCIMA SEXTA - A CONTRATADA se obriga a informar à CONTRATANTE, no prazo de 48 (quarenta e oito) horas, qualquer alteração social ou modificação da finalidade ou da estrutura da empresa.

CLÁUSULA DÉCIMA SÉTIMA - Na hipótese de fusão, cisão, incorporação ou associação da CONTRATADA com outrem, a CONTRATANTE reserva-se o direito de rescindir o contrato, ou continuar sua execução com a empresa resultante da alteração social.

CLÁUSULA DÉCIMA OITAVA - É vedado à CONTRATADA caucionar ou utilizar o presente contrato como garantia para qualquer operação financeira.

CLÁUSULA DÉCIMA NONA - A CONTRATADA não poderá utilizar o nome da CONTRATANTE, ou sua qualidade de CONTRATADA em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visitas, anúncios diversos, impressos etc., sob pena de imediata rescisão do presente contrato, independentemente de aviso ou interpelação judicial ou extrajudicial, sem prejuízo da responsabilidade da CONTRATADA.

CLÁUSULA VIGÉSIMA - A não utilização, pelas partes, de qualquer dos direitos assegurados neste contrato, ou na lei em geral, não implica em novação, não devendo ser interpretada como desistência de ações futuras. Todos os meios postos a disposição neste contrato são cumulativos e não alternativos, inclusive com relação a dispositivos legais.

CLÁUSULA VIGÉSIMA PRIMEIRA - São assegurados à CONTRATANTE todos os direitos e faculdades previstos na Lei nº 8.078, de 11.09.1990 (Código de Defesa do Consumidor).

CONFIDENCIALIDADE E SIGILO

CLÁUSULA VIGÉSIMA SEGUNDA- A CONTRATADA se compromete a manter sigilo e confidencialidade absoluto sobre as atividades decorrentes da execução dos serviços e sobre as informações a que venha a ter acesso por força da execução deste contrato, no que se refere a não divulgação, integral ou parcial, por qualquer forma, das informações ou dos documentos a eles relativos e decorrentes da execução dos serviços.

Parágrafo Único - Durante a execução deste contrato, a CONTRATADA dará acesso, em tempo hábil, às informações, processos, serviços e/ou suas instalações à CONTRATANTE.

CLÁUSULA VIGÉSIMA TERCEIRA - A CONTRATADA, por seus dirigentes, prepostos ou empregados, compromete-se, mesmo após o término do presente contrato, a manter completa confidencialidade e sigilo sobre quaisquer dados ou informações obtidas em razão do presente contrato, reconhecendo que não poderão ser divulgados ou fornecidos a terceiros, salvo com expressa autorização, por escrito, da CONTRATANTE.

Parágrafo Único - A CONTRATADA será responsável, civil e criminalmente, por quaisquer danos causados a CONTRATANTE e/ou terceiros em virtude da quebra da confidencialidade e sigilo a que estão obrigadas.

SANÇÕES ADMINISTRATIVAS

CLÁUSULA VIGÉSIMA QUARTA - Os atos praticados pela CONTRATADA, prejudiciais à execução do contrato, sujeitam-na às seguintes sanções:

a) advertência;

b) multa;

c) suspensão temporária do direito de licitar e contratar com a CONTRATANTE, por período não superior a 2 (dois) anos;

Parágrafo Primeiro – Nenhuma sanção será aplicada sem o devido processo, observadas as normas do Regulamento de Licitações e Contratos da BB Tecnologia e Serviços S.A.

Parágrafo Segundo - A aplicação das penalidades ocorrerá após defesa prévia do interessado, no prazo de 10 (dez) dias úteis a contar da intimação do ato.

Parágrafo Terceiro - No caso de aplicação de multa por inexecução total ou parcial do Contrato e suspensão temporária, caberá apresentação de recurso no prazo de 2 (dois) dias úteis a contar da intimação do ato.

Parágrafo Quarto - Nos prazos de defesa prévia e recurso, será aberta vista do processo aos INTERESSADOS.

CLÁUSULA VIGÉSIMA QUINTA - Ressalvados os casos fortuitos ou de força maior e aqueles que não acarretem prejuízos para a CONTRATANTE, a advertência poderá ser aplicada quando ocorrer execução insatisfatória ou pequenos transtornos ao desenvolvimento deste Contrato, desde que sua gravidade não recomende a aplicação da suspensão temporária, impedimento ou declaração de inidoneidade.

CLÁUSULA VIGÉSIMA SEXTA - A CONTRATANTE poderá aplicar multa à CONTRATADA nas situações, condições e percentuais indicados a seguir:

Parágrafo Primeiro – Em caso de atraso na apresentação ou integralização da garantia de execução contratual, será aplicada multa de: 0,5% (zero vírgula cinco por cento) sobre o valor total da garantia, por dia útil de atraso, até o limite de 10% (dez por cento);

Parágrafo Segundo – Multa de até 20% (vinte por cento) do valor da nota fiscal/fatura do objeto contratado, nas seguintes situações:

a) Inexecução total ou parcial do contrato;

b) Apresentação de documentos falsos ou falsificados;

c) Atraso, injustificado, na execução/conclusão dos serviços, contrariando o disposto no contrato;

d) Irregularidades que ensejem a rescisão contratual;

e) Condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos;

f) Prática de atos ilícitos visando prejudicar a execução do contrato;

g) Prática de atos ilícitos que demonstrem não possuir idoneidade para contratar com a CONTRATANTE;

h) Inadimplemento, por parte da CONTRATADA, de obrigações trabalhistas e previdenciárias devidas aos seus empregados;

i) Descumprimento das obrigações deste Contrato, especialmente aquelas relativas às características dos serviços, previstas no Documento nº 1 deste Contrato.

Parágrafo Terceiro - Em caso de reincidência, o valor da multa estipulada no parágrafo anterior desta cláusula será elevado em 1% (um por cento) a cada reincidência, até o limite de 30% (trinta por cento) do valor da nota fiscal/fatura do objeto contratado.

Parágrafo Quarto - A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório, e a sua cobrança não isentará a CONTRATADA da obrigação de indenizar eventuais perdas e danos.

Parágrafo Quinto - A multa aplicada à CONTRATADA e os prejuízos por ela causados à CONTRATANTE serão deduzidos de qualquer crédito a ela devido, cobrados diretamente ou judicialmente.

Parágrafo Sexto - A CONTRATADA desde logo autoriza a CONTRATANTE a descontar dos valores por ele devidos o montante das multas a ela aplicadas.

CLÁUSULA VIGÉSIMA SÉTIMA - A suspensão temporária poderá ser aplicada quando ocorrer:

a) Apresentação de documentos falsos ou falsificados;

b) Reincidência de execução insatisfatória dos serviços contratados;

c) Atraso, injustificado, na execução/conclusão dos serviços, contrariando o disposto no contrato;

d) Reincidência na aplicação das penalidades de advertência ou multa;

e) Irregularidades que ensejem a rescisão contratual;

f) Condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

g) Prática de atos ilícitos visando prejudicar a execução do contrato;

h) Prática de atos ilícitos que demonstrem não possuir idoneidade para contratar com a CONTRATANTE;

i) Inadimplemento, por parte da CONTRATADA, de obrigações trabalhistas e previdenciárias devidas aos seus empregados;

j) Descumprimento das obrigações deste Contrato, especialmente aquelas relativas às características dos serviços, previstas no Documento nº 1 deste Contrato.

CLÁUSULA VIGÉSIMA OITAVA - Adicionalmente, a CONTRATADA declara ter ciência de que as disposições contidas na Lei nº 12.846/2013 e na Lei nº 9.613/1998 se aplicam ao presente contrato, conforme o disposto nas Cláusulas Décima Primeira e Décima Segunda deste contrato.

CÓDIGO DE ÉTICA E NORMAS DE CONDUTA

CLÁUSULA VIGÉSIMA NONA - A CONTRATADA declara conhecer e corroborar com os princípios constantes no Código de Ética e Normas de Conduta da CONTRATANTE, disponível na Internet no endereço http://www.bbts.com.br.

POLÍTICA DE RELACIONAMENTO COM FORNECEDORES

CLÁUSULA TRIGÉSIMA - A CONTRATADA declara conhecer e corroborar com as diretrizes constantes na Política de Relacionamento com fornecedores da CONTRATANTE, disponível na Internet no endereço http://www.bbts.com.br.

DA DECLARAÇÃO E GARANTIA ANTICORRUPÇÃO

CLÁUSULA TRIGÉSIMA PRIMEIRA - A CONTRATADA declara neste ato que está ciente, conhece e entende os termos da Lei Anticorrupção nº 12.846/2013 e, por si e por seus administradores, diretores, funcionários e agentes, bem como seus sócios que venham a agir em seu nome, se obriga a abster-se de qualquer atividade que constitua violação das disposições dos termos da lei mencionada.

CLÁUSULA TRIGÉSIMA SEGUNDA - Para a execução deste contrato, nenhuma das partes poderá se oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma que não relacionada a este contrato, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

POLÍTICA DE PREVENÇÃO E COMBATE À CORRUPÇÃO, À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

CLÁUSULA TRIGÉSIMA TERCEIRA - A CONTRATADA declara conhecer e corroborar com as diretrizes constantes na Política de Prevenção e Combate à Corrupção, à Lavagem de Dinheiro e ao Financiamento do Terrorismo da CONTRATANTE, disponível na Internet no endereço http://www.bbts.com.br, e, também, que divulga tais diretrizes a seus funcionários alocados na execução do objeto deste contrato.

AUDITAGEM

CLÁUSULA TRIGÉSIMA QUARTA - A CONTRATADA declara também concordar com a possibilidade de realização de auditorias por parte da CONTRATANTE visando verificar o cumprimento das cláusulas contratuais e o comprometimento com o seu Código de Ética e Normas de Conduta e Programa de Compliance, devendo o escopo da auditoria ser definido e avaliado mediante os riscos do contrato.

MATRIZ DE RISCOS

CLÁUSULA TRIGÉSIMA QUINTA - Tendo como premissa a obtenção do melhor custo contratual, mediante a alocação de riscos à parte com maior capacidade para geri-los e absorvê-los, a CONTRATANTE e a CONTRATADA identificam os riscos decorrentes desta relação e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Risco constante do Documento nº 1 deste Contrato.

Parágrafo Único - É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na matriz de riscos, como de responsabilidade da CONTRATADA.

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

CLÁUSULA TRIGÉSIMA SEXTA - A CONTRATADA declara conhecer e cumprir todas as leis vigentes envolvendo proteção de dados pessoais, em especial a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais") e, quando for o caso, o Regulamento 679/2016 da União Europeia ("Regulamento Geral sobre a Proteção de Dados"), conhecida pela sigla GDPR, comprometendo-se, assim, a limitar a utilização dos dados pessoais a que tiver acesso apenas para execução dos serviços deste Contrato, abstendo-se de utilizá-los em proveito próprio ou alheio, para fins comerciais ou quaisquer outros.

Paragrafo Primeiro - Os termos utilizados neste contrato apresentam os mesmos significados do art. 5º da Lei Geral de Proteção de Dados Pessoais;

Parágrafo Segundo - Se quaisquer alterações nas Leis de Proteção de Dados, regulamentos ou recomendações da Autoridade Nacional resultarem no descumprimento das Leis de Proteção de Dados, em relação ao processamento de Dados Pessoais realizadas sob este Contrato, as Partes deverão empenhar seus melhores esforços, de forma imediata, para remediar tal descumprimento, sob pena de inexecução total ou parcial do contrato.

DAS OBRIGAÇÕES DAS PARTES

CLÁUSULA TRIGÉSIMA SÉTIMA - As Partes reconhecem que, como parte da execução do Contrato, armazenam, coletam, tratam ou de qualquer outra forma processam dados pessoais na categoria de Controlador para Operador. No sentido dado pela legislação vigente aplicável, a CONTRATANTE será considerada "Controladora de Dados", e a CONTRATADA "Operadora" ou "Processadora de Dados".

Parágrafo Primeiro - As partes concordam que o tratamento de Dados Pessoais resultante do presente Contrato será realizado estritamente para os fins de Aquisição de licença perpétua, para upgrade da solução McAfee e garantia de 36 meses, conforme condições e exigências estabelecidas neste documento.

Parágrafo Segundo - As Partes garantem que adotam políticas de boas práticas e governança, que contém e asseguram, obrigatoriamente: níveis de segurança tecnológica; procedimentos que assegurem integridade, confidencialidade e disponibilidade no tratamento de dados; regras de organização, funcionamento, procedimento, obrigações para os agentes de tratamento, ações educativas, mecanismos internos de supervisão e de mitigação de riscos.

CLÁUSULA TRIGÉSIMA OITAVA - As Partes comprometem-se a:

i) cumprir com as obrigações e requisitos das legislações de proteção de informações relacionadas à pessoas naturais identificadas ou identificáveis ("Dados Pessoais") vigentes ou que entrarem em vigor na vigência deste Contrato, incluindo, mas não se limitando à Lei Geral de Proteção de Dados Pessoais, Marco Civil da Internet, Lei no 8.078, de 11 de setembro de 1990 ("Código de Defesa do Consumidor"), Lei Complementar nº 166, de 08 de abril de 2019 ("Lei do Cadastro Positivo"), Lei nº 12.527, de 18 de novembro de 2011 ("Lei de Acesso à Informação") e Decreto no 7.962, de 15 de março de 2013 ("Decreto Comércio Eletrônico"), conforme aplicável ("Legislações de Proteção de Dados Pessoais");

ii) abster-se de realizar quaisquer ações ou omissões que possam resultar de alguma forma em violação das Legislações de Proteção de Dados Pessoais;

iii) tratar os dados pessoais apenas para fins lícitos, adotando as melhores posturas e práticas para preservar o direito à privacidade dos titulares e dar cumprimento às regras e princípios previstos na Lei Geral de Proteção de Dados Pessoais – LGPD.

iv) tomar todas as medidas razoavelmente necessárias para manter a conformidade com as Legislações de Proteção de Dados Pessoais;

v) garantir que qualquer atividade realizada envolvendo o tratamento de Dados Pessoais, resultante do objeto do presente Contrato, e as medidas adotadas para a privacidade e segurança estejam em conformidade com as Legislações de Proteção de Dados Pessoais e sejam consistentes com a Política de Privacidade e Política de Segurança da Informação da BB Tecnologia e Serviços, conforme disposto em seu sítio eletrônico https://bbts.com.br/index.php/politicas, a qual poderá ser atualizada a qualquer tempo visando conformidade com a legislação brasileira e internacional de proteção de dados pessoais;

vi) não realizar qualquer Tratamento de Dados Pessoais, resultantes da execução do Contrato, sem enquadramento em uma das bases legais estipuladas no art. 7º da LGPD;

vii) adotar medidas técnicas e organizacionais adequadas para garantir a segurança dos Dados Pessoais;

viii) somente realizar o Tratamento de Dados Pessoas como resultado do presente Contrato com a finalidade de cumprir com as respectivas obrigações contratuais;

ix) respeitar as políticas e regras editadas ou que vierem a ser editadas por elas no tocante ao armazenamento e tratamento de dados e informações, sem prejuízo do estrito respeito à Lei n. 12.965 de 2014 ("Marco Civil da Internet"), Decreto n. 8.771 de 2016 ("Regulamento do Marco Civil da Internet"), bem como quaisquer outras leis relativas à proteção de dados pessoais que vierem a ser promulgadas ou entrarem em vigor no curso da vigência deste Contrato, em especial com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais.

x) não permitir ou facilitar o Tratamento de Dados Pessoais por terceiros para qualquer finalidade que não seja o cumprimento de suas respectivas obrigações contratuais; e

l) assinar quaisquer documentos que possam ser exigidos ocasionalmente pela outra parte para implementar ou cumprir as obrigações de proteção de dados.

Parágrafo Único - As Partes, desde já pactuam que o descumprimento por uma delas, de qualquer Legislação de Proteção de Dados Pessoais, das políticas da CONTRATANTE ou das provisões contidas neste contrato gerará obrigação da Parte culpada em indenizar, defender e manter isento(a)(s) a(s) outra(s) Parte(s), suas entidades afiliadas, conselheiros, diretores, executivos e empregados de e contra todas as responsabilidades, perdas, os danos, prejuízos, custos, despesas, ações, processos, demandas, multas e penalidades decorrentes do descumprimento, por uma das Partes, de suas obrigações, declarações e garantias previstas nesta Cláusula, sendo que nenhuma limitação de responsabilidade eventualmente acordada neste Contrato será aplicada para as indenizações por descumprimento das obrigações previstas neste contrato.

DAS OBRIGAÇÕES DA CONTRATANTE

CLÁUSULA TRIGÉSIMA NONA – A CONTRATANTE se compromete a:

i) Garantir que os Dados Pessoais serão tratados e transferidos nos termos das Leis de Proteção de Dados Pessoais;

ii) Garantir que sejam tomadas todas as medidas de segurança para Tratamento dos Dados Pessoais;

iii) Empenhar esforços razoáveis para assegurar que a CONTRATADA possa cumprir com as obrigações contratuais resultantes das presentes cláusulas;

iv) Responder às consultas de Titulares, da Autoridade Nacional e/ou autoridades competentes em relação ao Tratamento de Dados Pessoais. As respostas serão dadas num prazo razoável, de acordo com as Leis de Proteção de Dados Pessoais;

v) Divulgar orientações de boas práticas e de governança para serem cumpridas pela CONTRATADA no âmbito da execução deste contrato;

DAS OBRIGAÇÕES DA CONTRATADA

CLÁSULA QUADRAGÉSIMA - A CONTRATADA tratará os dados pessoais a que tiver acesso em virtude deste contrato apenas nas seguintes condições:

i) em nome da CONTRATANTE e para atender as finalidades deste contrato;

ii) para a execução do Contrato e somente na medida do necessário para fazê-lo;

iii) de acordo com as instruções periódicas, razoáveis e documentadas da CONTRATANTE; e

iv) em conformidade com todas as leis de proteção de dados aplicáveis, incluindo legislação extraterritorial ao qual a CONTRATANTE esteja sujeita.

Parágrafo Primeiro - A CONTRATADA deverá assegurar que qualquer pessoa física ou jurídica, agindo sob sua autorização e que possua acesso aos dados pessoais, esteja vinculada por obrigações contratuais que disponham de proteções equivalentes às previstas nesta cláusula em relação aos dados pessoais que tiver acesso.
Parágrafo Segundo - Nos casos onde o tratamento de dados pessoais forem realizados através de sistemas de informação ou computação em nuvem, a CONTRATADA se compromete em tornar transparente à CONTRATANTE cada intervenção ou manutenção, proveniente de suporte técnico, que exija acesso direto aos dados ou acesso aos ambientes restritos das soluções ou serviços hospedados em nuvem (em âmbito nacional e internacional), de modo a manter registrada a motivação e os responsáveis por cada intervenção.

Parágrafo Terceiro - Em caso de dúvidas sobre o tratamento dos dados, a CONTRATADA deverá notificar a CONTRATANTE e aguardar as instruções.

CLÁUSULA QUADRAGÉSIMA PRIMEIRA - São partes integrantes deste contrato, independentemente de transcrição ou futuras atualizações:

i) A Política de Privacidade da CONTRATANTE, disponível no sítio eletrônico https://bbts.com.br/index.php/politicas;

ii) A Política de Segurança da Informação, disponível no sítio eletrônico https://bbts.com.br/index.php/politicas;

iii) O Inventário de Tratamentos de Dados Pessoais, mantido entre as partes, para relacionar todas as operações realizadas em virtude deste contrato, contendo: hipóteses legais, finalidades específicas, tipos de dados, tipos de tratamentos, duração dos tratamentos, informações acerca de compartilhamento de dados pessoais com entidades públicas e privadas, possíveis transferências internacionais de dados, responsabilidades dos agentes que realizarão o tratamento, a origem dos dados e a forma com os dados são tratados.

Parágrafo Primeiro - A CONTRATADA declara que seguirá as orientações da Política de Privacidade da CONTRATANTE, inclusive as suas atualizações, as quais serão informadas por meio de mensagem eletrônica, sobre as novas versões.

Parágrafo Segundo - As obrigações de sigilo e processamento dos dados pessoais impostos à CONTRATADA se estendem a seus prepostos e subcontratados (se autorizado em contrato), garantindo que o acesso aos dados pessoais somente seja concedido às pessoas designadas para executar as atividades descritas neste Contrato e que estejam sob obrigação de confidencialidade com relação aos dados pessoais tratados.

Parágrafo Terceiro - Para o cumprimento desta cláusula, a CONTRATADA se compromete a firmar Acordos de Confidencialidade e de não divulgação que reflitam a criticidade dos dados tratados e/ou compartilhados.

CLÁUSULA QUADRAGÉSIMA SEGUNDA - A CONTRATADA declara que, caso utilize sistema próprio para armazenamento dos dados fornecidos pela CONTRATANTE para execução dos serviços:

i) adotará procedimentos e controles, abrangendo, no mínimo, a autenticação, a criptografia, a detecção de intrusão e a prevenção de vazamento de informações e dados recebidos da CONTRATANTE para execução do objeto do Contrato;

ii) realizará testes e varreduras para detecção de vulnerabilidade, mantendo seus sistemas eletrônicos livres de programas maliciosos;

iii) efetuará o controle de acessos aos seus sistemas eletrônicos pelos seus prepostos, de forma efetiva, o cumprimento das obrigações deste Contrato e da legislação reguladora;

iv) manterá o registro das operações de tratamento de dados pessoais que realizarem;

v) seguirá os padrões de segurança técnica validados no mercado e referendados pela CONTRATANTE por meio deste contrato ou em sua Política de Privacidade e Política de Segurança da Informação.

CLÁUSULA QUADRAGÉSIMA TERCEIRA - A execução e a manutenção de medidas tecnológicas e físicas adotadas pela CONTRATADA, adequadas ao risco decorrente do Tratamento e a natureza dos Dados Pessoais, deverão ser apropriadas e suficientes para proteger os dados pessoais contra, inclusive, mas não se limitando a alteração, divulgação ou acesso não autorizado, notadamente quando o processo envolver a transmissão de dados através de uma rede de tecnologia/informática/internet e contra todas as outras formas de processamento de dados ilícitas.

CLÁUSULA QUADRAGÉSIMA QUARTA - A CONTRATADA se compromete a:

i) Tratar os Dados Pessoais disponibilizados pela CONTRATANTE em conformidade com as suas instruções, as cláusulas do presente Contrato e as Leis de Proteção de Dados Pessoais, sendo certo que caso não possa cumprir estas obrigações por qualquer razão, concorda em informar imediatamente a **CONTRATANTE** desse fato, o qual terá o direito de suspender o compartilhamento dos Dados Pessoais e/ou de rescindir o Contrato;

ii) Dispor de procedimentos necessários para que terceiros autorizados a acessar os Dados Pessoais, incluindo os subcontratantes, respeitem e mantenham a confidencialidade e a segurança dos Dados Pessoais. Todas as pessoas sob a autoridade do Operador, incluindo os subcontratantes, devem ser obrigados a tratar os Dados Pessoais apenas sob a orientação da CONTRATADA;

iii) Indicar à CONTRATANTE um setor profissional capacitado a responder às consultas relativas ao Tratamento de Dados Pessoais e cooperar de boa-fé com a CONTRATANTE, os Titulares e a Autoridade Nacional em todas as eventuais consultas num prazo razoável;

iv) Não divulgar nem transferir Dados Pessoais a terceiros responsáveis pelo Tratamento de Dados Pessoais estabelecidos em países que não possuam regime de proteção de Dados Pessoais compatível com os termos deste Contrato e as Leis de Proteção de Dados Pessoais;

v) No que tange às transferências posteriores de Dados Sensíveis, garantir que os Titulares deem o seu consentimento inequívoco para esse efeito.

vi) Notificar imediatamente a CONTRATANTE e em prazo nunca superior a 24 (vinte e quatro) horas no que diz respeito a:

a) Qualquer intimação, pedido, requisição de cooperação judicial no que diz respeito a divulgação de Dados Pessoais;

b) Qualquer acesso acidental ou não autorizado;

c) Qualquer solicitação ou reclamação realizada diretamente pelo Titular, Autoridade Nacional de Proteção de dados, Organismos de Defesa ao Consumidor ou outros agentes legitimados.

Parágrafo Único - A CONTRATADA não poderá, sem instruções prévias da CONTRATANTE, transferir ou, de qualquer outra forma, compartilhar e/ou garantir acesso aos Dados Pessoais ou a quaisquer outras informações a terceiros.

CLÁUSULA QUADRAGÉSIMA QUINTA - A CONTRATADA se compromete a cooperar e a fornecer ao à CONTRATANTE, no prazo por ele estabelecido, todas as informações relacionadas ao tratamento de Dados Pessoais que estiverem sob sua custódia e que sejam necessárias para responder às solicitações ou reclamações feitas com fundamento na Lei Geral de Proteção de Dados Pessoais.

Parágrafo Primeiro - A CONTRATADA se certificará que seus empregados, representantes, e prepostos agirão de acordo com a finalidade do Contrato, as leis de proteção de dados e as instruções transmitidas pela CONTRATANTE.

Parágrafo Segundo - A CONTRATADA se responsabiliza, irrestritamente, pela inviolabilidade ou má utilização das informações e dados recebidos da CONTRATANTE para execução do objeto deste Contrato e por quaisquer invasões, física ou lógica, realizadas por terceiros.
Parágrafo Terceiro - Entende-se por má-utilização o uso dos dados compartilhados em desacordo com o previsto neste Contrato com finalidade diversa da permitida pela CONTRATANTE e em desconformidade com a necessidade para a prestação dos serviços previsto no objeto.

Parágrafo Quarto - A CONTRATADA, sempre que for solicitado pela CONTRATANTE, deverá fornecer por escrito documentação e relatório sobre as medidas de segurança e proteção dos dados implementados para o tratamento dos dados relacionados à execução deste contrato.

Parágrafo Quinto - Se a CONTRATADA processar Dados Pessoais relativos a pessoas localizadas na UE ou em empresas com sede na UE, durante a vigência deste contrato, cumprirá com as regras da GPDR.

CLÁUSULA QUADRAGÉSIMA SEXTA - O descumprimento das obrigações pela CONTRATADA poderá ensejar a rescisão imediata deste Contrato. O descumprimento acarretará no ressarcimento, por parte da CONTRATADA dos prejuízos causados à CONTRATANTE, além da possibilidade da aplicação de multa equivalente a 5 (cinco) vezes o valor do último faturamento decorrente deste Contrato, sem prejuízo de perdas e danos e outras penalidades previstas, sendo que nenhuma limitação de responsabilidade eventualmente acordada neste Contrato será aplicada para as indenizações por descumprimento das obrigações contidas nesta Cláusula.

Parágrafo Único - A CONTRATADA indenizará a CONTRATANTE por eventuais danos que esta venha a sofrer em decorrência de uso indevido dos dados pessoais por parte da CONTRATADA.

CLÁUSULA QUADRAGÉSIMA SÉTIMA - Todos os dados e informações enviados pela CONTRATANTE à CONTRATADA deverão ser excluídos, pela CONTRATADA, em até 10 (dez) dias úteis após o recebimento do produto final pela CONTRATANTE, sendo comprovado o ato por meio de documento apresentado em até 05 (cinco) dias úteis.

SUBCONTRATAÇÃO E TRANSFERÊNCIA INTERNACIONAL DE DADOS

CLÁUSULA QUADRAGÉSIMA OITAVA - Os serviços descritos neste Contrato não configuram, em hipótese alguma, o fornecimento de informações e dados pessoais de responsabilidade da CONTRATANTE à CONTRATADA com fim comercial, sendo certo que a CONTRATADA está expressamente proibida de compartilhar dados e informações com quaisquer terceiros que não sejam os prepostos e subcontratados destacados para executar as atividades deste Contrato, se autorizada, neste contrato, a subcontratação.

Parágrafo Primeiro - A CONTRATADA não poderá transferir Dados Pessoais para fora do Brasil, da União Europeia (UE) ou do Espaço Econômico Europeu (EEE) ou subcontratar o tratamento de Dados Pessoais sem a devida aprovação, por escrito, da CONTRATANTE.
Parágrafo Segundo - A CONTRATADA deverá assegurar que qualquer pessoa física ou jurídica, agindo sob sua autorização e que possua acesso aos dados pessoais, esteja vinculada por obrigações contratuais que disponham de proteções equivalentes às previstas nesta cláusula em relação aos dados pessoais que tiver acesso.

Parágrafo Terceiro - Nos casos em que a subcontratada deixar de cumprir com a obrigação de proteger os dados, a CONTRATADA será a exclusiva responsável pelo cumprimento das obrigações perante a CONTRATANTE.

CLÁUSULA QUADRAGÉSIMA NONA - A substituição da subcontratada deve ser precedida de nova autorização da CONTRATANTE, e estará condicionada a assunção de todas as obrigações concernentes à proteção de dados previstas neste contrato.

Parágrafo Primeiro - Se a subcontratada estiver localizada fora do Brasil e/ou da UE/EEE, a CONTRATADA assegurará que as devidas Cláusulas Contratuais-Padrão façam parte do contrato celebrado com a subcontratada ou assegurará que essa transferência seja, de outra forma, permitida pelas leis de proteção de dados.

Parágrafo Segundo - A CONTRATADA deverá ajustar a possibilidade de, quando entender necessário, auditar e fiscalizar o estabelecimento e os mecanismos de tratamento de dados do subcontratado, com previsão da possibilidade de a CONTRATANTE ter acesso aos relatórios elaborados por auditoria especializada contratada às expensas da CONTRATADA.

SEGURANÇA

CLÁUSULA QUINQUAGÉSIMA - A CONTRATADA implementará as medidas apropriadas para proteger os Dados Pessoais em conformidade com as técnicas adequadas às finalidades do tratamento e ao contexto de risco. As medidas de segurança da CONTRATADA atenderão as exigências das leis de proteção de dados e da Política de Privacidade e Política de Segurança da Informação da CONTRATANTE.

Parágrafo Primeiro - A CONTRATADA deverá utilizar recursos de segurança da informação e de tecnologia em versões comprovadamente seguras e atualizadas, inclusive os mecanismos de detecção e prevenção de ataques cibernéticos. Os dados armazenados em rede corporativa deverão ser segmentados em domínios lógicos.

Parágrafo Segundo - A CONTRATADA é a única responsável pelo correto e seguro armazenamento de dados em seu sistema eletrônico e única responsável por eventuais danos diretos e indiretos causados à CONTRATANTE ou terceiros, especialmente titulares de dados pessoais vazados, alterados, indevidamente comunicados ou que de qualquer forma tenha sofrido tratamento inadequado ou ilícito.

VIOLAÇÃO DOS DADOS

CLÁUSULA QUINQUAGÉSIMA PRIMEIRA - A CONTRATADA deverá notificar a CONTRATANTE, por escrito, sobre a violação dos Dados Pessoais, em prazo não superior a 24 (vinte e quatro) horas, a contar do momento em que tomou ciência da violação. As informações incluirão:

i) descrição da natureza da violação dos Dados Pessoais, incluindo as categorias e o número aproximado de titulares de dados lesado, bem como as categorias e o número aproximado de registros de dados comprometidos;

ii) descrição das prováveis consequências ou das consequências já concretizadas da violação dos Dados Pessoais; e

iii) descrição das medidas adotadas ou propostas para reparar a violação dos Dados Pessoais, com a indicação de cronograma, para corrigir ou mitigar os possíveis efeitos adversos.

Parágrafo Único - A CONTRATADA arcará com todos os custos, incluindo indenizações e penalidades aplicadas à CONTRATANTE e seus prepostos por eventuais danos que esta venha a sofrer em decorrência do uso indevido dos dados pessoais por parte da CONTRATADA, sempre que ficar comprovado que houve falha de segurança (técnica e administrativa), descumprimento das regras da lei geral de proteção de dados citadas neste contrato e das orientações da CONTRATANTE, sem prejuízo da aplicação das penalidades deste contrato.

FISCALIZAÇÕES

CLÁUSULA QUINQUAGÉSIMA SEGUNDA - A CONTRATADA obriga-se a permitir à CONTRATANTE, quando esta entender necessário e for razoável, o integral e irrestrito acesso ao seu estabelecimento, aos seus sistemas eletrônicos, às informações, dados e documentos sob sua posse e que estejam relacionadas à execução deste contrato, permitindo, inclusive, a realização de auditoria em suas dependências, pela CONTRATANTE, por meio de seus prepostos ou terceiros por este indicado, sem que haja necessidade de agendamento prévio, e/ou possibilitar o acesso da CONTRATANTE aos relatórios elaborados pela CONTRATADA ou pela auditoria especializada realizada a pedido desta.

TÉRMINO DO TRATAMENTO DOS DADOS

CLÁUSULA QUINQUAGÉSIMA TERCEIRA - O tratamento dos dados terminará com a rescisão ou fim da vigência deste Contrato ou mediante solicitação escrita da CONTRATANTE, o que ocorrer primeiro. A CONTRATADA se obriga a devolver, de seus sistemas eletrônicos, todas as informações a que teve acesso em decorrência dos serviços objeto deste Contrato, e a devolver qualquer documento que contenha referidos dados no seu conteúdo, no prazo de 10 (dez) dias úteis após os termos de encerramento citados nesta cláusula. Os dados serão excluídos dos sistemas eletrônicos, não sendo permitido que a CONTRATADA promova qualquer tipo de cópia dos arquivos.

Parágrafo Primeiro - A CONTRATADA garantirá que seus Subcontratados cessem, imediatamente, todo e qualquer uso dos Dados Pessoais a partir da ocorrência dos termos de encerramento mencionados no caput, cabendo adotar as medidas solicitadas, a exemplo de destruição, devolução ou anonimização permanente, utilizando, em cada caso, as medidas de segurança deste contrato.

Parágrafo Segundo - O armazenamento dos dados após a ocorrência dos termos de encerramento somente será permitido quando for necessário ao cumprimento de obrigações legais ou regulatórias, na forma da Lei Geral de Proteção de Dados Pessoais.

DA RESPONSABILIDADE E DIREITOS DE TERCEIROS

CLÁUSULA QUINQUAGÉSIMA QUARTA - As Partes concordam que qualquer Titular que tenha sofrido danos resultantes de qualquer descumprimento das obrigações referidas no presente instrumento e nas Legislações de Proteção de Dados Pessoais, por qualquer parte ou subcontratante ulterior, têm o direito de obter reparação do Controlador e Operador pelos danos sofridos, sendo esta responsabilidade solidária.

i) Cada parte é responsável perante a outra parte pelos danos causados pela violação das presentes cláusulas. A responsabilidade entre partes limita-se aos danos efetivamente sofridos. Cada uma das Partes é responsável perante os Titulares pela violação de direitos de terceiros, nos termos das presentes cláusulas.

ii) O Operador não pode invocar o descumprimento das disposições contratuais e Legislações de Proteção de Dados por subcontratante ulterior das suas obrigações para eximir-se de suas responsabilidades.

PREPOSTOS

CLÁUSULA QUINQUAGÉSIMA QUINTA – As partes nomeiam, neste ato, para representá-la no cumprimento deste Contrato, os seus funcionários:

Pela CONTRATANTE

Nome: Waldo Baptista Gomes

Cargo: Diretor de Marketing e Relacionamento

E-mail: [redacted]

Telefone: [redacted]

Pela CONTRATADA

Nome: Bruno Pinheiro dos Reis

Cargo: Gerente do Centro de TIC I

E-mail: [redacted]

Telefone: [redacted]

DISPOSIÇÕES FINAIS

CLÁUSULA QUINQUAGÉSIMA SEXTA - Fazem parte integrante deste contrato, independente de transcrição, todas as disposições do instrumento convocatório da Licitação referido no preâmbulo, bem como aquelas constantes da Carta-Proposta apresentada, prevalecendo, onde houver conflito, as disposições deste contrato.

CLÁUSULA QUINQUAGÉSIMA SÉTIMA - As partes elegem o foro da Comarca de Brasília para dirimir qualquer questão oriunda deste contrato, com exclusão de qualquer outro por mais privilegiado que se apresente.

E, por se acharem justas e contratadas, assinam as partes o presente instrumento.

INDICAÇÃO DOS SIGNATÁRIOS:

CONTRATANTE: BB TECNOLOGIA E SERVIÇOS S.A.

Nome: Sérgio Gonzaga Wenceslau
Cargo: Gerente de Divisão
CPF: [redacted]

Nome: Isaac Nicholas Siqueira Viana
Cargo: Gerente Executivo
CPF: [redacted]

CONTRATADA: NETSAFE CORP LTDA

Nome: Waldo Baptista Gomes
Cargo: Diretor de Marketing e Relacionamento
CPF: [redacted]

DOCUMENTO Nº 1 DO CONTRATO

DESCRIÇÃO DOS SERVIÇOS

ESPECIFICAÇÕES TÉCNICAS

1. Objeto:

1.1. Aquisição de licença perpétua de solução EDR, para upgrade da solução McAfee antivírus, garantia de 36 meses, conforme condições e exigências estabelecidas neste documento.

Lote	Item	Descrição	Unidade	Quantidade
1	1	Aquisição de licença perpétua de solução EDR, para upgrade da solução McAfee antivírus, garantia de 36 meses, conforme condições e exigências estabelecidas neste documento.	Usuários	6.000

2. Especificações técnicas:

2.1. Solução para proteção de estações de trabalho e servidores

2.1.1. Características Gerais da Solução EDR:

2.1.1.1. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3Gb de memória RAM.

2.1.1.2. Deve suportar as seguintes plataformas clientes:

2.1.1.2.1. Windows 11;

2.1.1.2.2. Windows 10;

2.1.1.2.3. Windows 8.1;

2.1.1.2.4. Windows 8;

2.1.1.2.5. Monterey 12.0;

2.1.1.2.6. Big Sur 11.0.x, 11.1 e/ou superiores;

2.1.1.2.7. Catalina 10.15.6 e superiores;

2.1.1.3. Deve suportar as seguintes plataformas servidores:

2.1.1.3.1. Windows Server 2019;

2.1.1.3.2. Windows Server 2016;

2.1.1.3.3. Windows Server 2012 R2;

2.1.1.3.4. Windows Server 2012;

2.1.1.4. Deve inclusive suportar o modo Server Core.

2.1.1.5. Deve suportar, pelo menos as funções de antivírus e firewall de host, nas seguintes distribuições de Linux:

2.1.1.5.1. Red Hat Enterprise 7.x e 8.x, 64bits;

2.1.1.5.2. SUSE Linux Enterprise Server 12.x e 15.x, 64bits;

2.1.1.5.3. Ubuntu 16.04, 18.04, 19.10, 20.04, 20.10 64bits;

2.1.1.5.4. CentOS 7.x e 8.x, 64bits;

2.1.1.5.5. Oracle Linux 7 e 8, 64bits;

2.1.1.6. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:

2.1.1.6.1. AWS;

2.1.1.6.2. Azure;

2.1.1.6.3. Citrix XenApp;

2.1.1.6.4. Citrix XenDesktop;

2.1.1.6.5. Citrix XenServer;

2.1.1.6.6. Microsoft Hyper-V 2012 R2;

2.1.1.6.7. Vmware ESXi;

2.1.1.6.8. Vmware Player;

2.1.1.6.9. Vmware vShpere;

2.1.1.6.10. Vmware Workstation;

2.1.1.7. A solução deve compreender, no mínimo, as seguintes funcionalidades:

2.1.1.7.1. Módulo antimalware;

2.1.1.7.2. Módulo de firewall de host;

2.1.1.7.3. Módulo de filtragem web;

2.1.1.7.4. Módulo de proteção contra ameaças avançadas;

2.1.1.7.5. Módulo de reputação de arquivos;

2.1.1.7.6. Módulo de detecção e resposta a incidentes;

2.1.1.7.7. Módulo para controle de dispositivos;

2.1.1.7.8. Módulo para controle de aplicações;

2.1.1.8. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

2.1.1.8.1. Relatórios;

2.1.1.8.2. Dashboards;

2.1.1.8.3. Políticas;

2.1.1.8.4. Configuração;

2.1.1.8.5. Instalação/Desinstalação;

2.1.1.9. O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

2.1.1.10. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.

2.1.1.11. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

2.1.1.12. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

2.1.1.13. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)

2.1.2. Características Módulo Antimalware (Clientes Windows)

2.1.2.1. Características da prevenção contra exploração

2.1.2.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).

2.1.2.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.

2.1.2.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

2.1.2.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

2.1.2.1.5. Deve ser possível bloquear contra falsificação de IP (IP Spoofing).

2.1.2.1.6. Deve ser possível incluir exclusões por:

2.1.2.1.6.1. Processo

2.1.2.1.6.1.1. Nome;

2.1.2.1.6.1.2. Caminho do Arquivo;

2.1.2.1.6.1.3. Hash MD5

2.1.2.1.6.2. Módulo chamador

2.1.2.1.6.2.1. Nome

2.1.2.1.6.2.2. Caminho

2.1.2.1.6.2.3. Hash MD5

2.1.2.1.6.2.4. Signatário Digital

2.1.2.2. Características da Proteção de acesso

2.1.2.2.1. Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definidas pelo fabricante da solução, no mínimo, para:

2.1.2.2.1.1. Acesso remoto a pastas locais;

2.1.2.2.1.2. Alteração políticas de direitos dos usuários;

2.1.2.2.1.3. Alterar os registros de extensão dos arquivos;

2.1.2.2.1.4. Criação de novos arquivos na pasta Arquivo de Programas;

2.1.2.2.1.5. Criação de novos executáveis na pasta Windows;

2.1.2.2.1.6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;

2.1.2.2.1.7. Criar ou Modificar remotamente arquivos ou pastas;

2.1.2.2.1.8. Desativar o editor de registro e o gerenciador de tarefas;

2.1.2.2.1.9. Executar arquivos das pastas do usuário;

2.1.2.2.1.10. Execução de scripts pelo host de script do Windows;

2.1.2.2.1.11. Instalar objetos de ajuda a navegação ou extensões de shell;

2.1.2.2.1.12. Instalar novos CLSIDs, APPIDs e TYPELIBs;

2.1.2.2.1.13. Modificar configurações de rede;

2.1.2.2.1.14. Modificar configurações do Internet Explorer;

2.1.2.2.1.15. Modificar processos principais do Windows;

2.1.2.2.1.16. Navegadores iniciando programas da pasta de downloads;

2.1.2.2.1.17. Registrar programas para execução automática;

2.1.2.2.2. As regras especificadas devem permitir o:

2.1.2.2.2.1. Bloqueio, ou

2.1.2.2.2.2. Evento de Informação, ou

2.1.2.2.2.3. Bloqueio e Evento de Informação;

2.1.2.2.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:

2.1.2.2.3.1. Processos;

2.1.2.2.3.1.1. Nome do processo;

2.1.2.2.3.1.2. Hash MD5;

2.1.2.2.3.1.3. Assinatura Digital;

2.1.2.2.3.2. Usuário;

2.1.2.2.3.3. Arquivos;

2.1.2.2.3.3.1. Criação;

2.1.2.2.3.3.2. Deletar;

2.1.2.2.3.3.3. Executar;

2.1.2.2.3.3.4. Alteração de permissão;

2.1.2.2.3.3.5. Leitura;

2.1.2.2.3.3.6. Renomear;

2.1.2.2.3.3.7. Escrever;

2.1.2.2.3.4. Chave de Registro

2.1.2.2.3.4.1. Escrever;

2.1.2.2.3.4.2. Criar;

2.1.2.2.3.4.3. Deletar;

2.1.2.2.3.4.4. Ler;

2.1.2.2.3.4.5. Enumerar;

2.1.2.2.3.4.6. Carregar;

2.1.2.2.3.4.7. Substituir;

2.1.2.2.3.4.8. Restaurar;

2.1.2.2.3.4.9. Alterar permissão;

2.1.2.2.3.5. Valor de Registro

2.1.2.2.3.5.1. Ler;

2.1.2.2.3.5.2. Criar;

2.1.2.2.3.5.3. Deletar;

2.1.2.2.3.6. Processo

2.1.2.2.3.6.1. Qualquer acesso;

2.1.2.2.3.6.2. Criar thread;

2.1.2.2.3.6.3. Modificar;

2.1.2.2.3.6.4. Terminar;

2.1.2.2.3.6.5. Executar;

2.1.2.2.4. Deve permitir a configuração de exclusões;

2.1.2.3. Características da varredura ao acessar

2.1.2.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;

2.1.2.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;

2.1.2.3.3. Deve ser capaz de realizar análise no setor de boot;

2.1.2.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;

2.1.2.3.5. Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;

2.1.2.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;

2.1.2.3.7. Deve realizar análise durante cópia entre pastas locais;

2.1.2.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;

2.1.2.3.9. Deve permitir a configuração do nível de agressividade da análise entre:

2.1.2.3.9.1. Muito Baixo

2.1.2.3.9.2. Baixo

2.1.2.3.9.3. Médio

2.1.2.3.9.4. Alto

2.1.2.3.9.5. Muito Alto

2.1.2.3.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;

2.1.2.3.11. Deve realizar varredura quando o processo:

2.1.2.3.11.1. Ler o disco;

2.1.2.3.11.2. Gravar no disco;

2.1.2.3.11.3. Deixar a solução decidir;

2.1.2.3.12. Deve possibilitar análise em

2.1.2.3.12.1. Unidades de Rede;

2.1.2.3.12.2. Arquivos abertos para backup;

2.1.2.3.12.3. Arquivos compactados, por exemplo .jar;

2.1.2.3.12.4. Arquivos codificados (MIME);

2.1.2.3.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;

2.1.2.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

2.1.2.3.14.1. Limpar o arquivo;

2.1.2.3.14.2. Excluir o arquivo;

2.1.2.3.14.3. Negar acesso ao arquivo;

2.1.2.3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

2.1.2.3.15.1. Limpar o arquivo;

2.1.2.3.15.2. Excluir o arquivo;

2.1.2.3.15.3. Permitir acesso ao arquivo;

2.1.2.3.15.4. Negar acesso ao arquivo;

2.1.2.3.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;

2.1.2.3.17. Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;

2.1.2.3.18. Deve permitir a criação de listas de exclusão de URLs que não sofrerão interceptação e análise de scripts;

2.1.2.3.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

2.1.2.4. Características da Varredura sob demanda

2.1.2.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

2.1.2.4.2. Deve permitir a criação de repetição da tarefa.

2.1.2.4.3. Deve permitir definir a hora da execução da tarefa de análise;

2.1.2.4.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;

2.1.2.4.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

2.1.2.4.6. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:

2.1.2.4.6.1. Os locais da varredura:

2.1.2.4.6.1.1. Memória para rootkits;

2.1.2.4.6.1.2. Processos em execução;

2.1.2.4.6.1.3. Arquivos registrados;

2.1.2.4.6.1.4. Meu computador;

2.1.2.4.6.1.5. Todas as unidades locais;

2.1.2.4.6.1.6. Todas as unidades fixas;

2.1.2.4.6.1.7. Todas as unidades removíveis;

2.1.2.4.6.1.8. Todas as unidades mapeadas;

2.1.2.4.6.1.9. Pasta inicial;

2.1.2.4.6.1.10. Pasta de perfil do usuário;

2.1.2.4.6.1.11. Pasta Windows;

2.1.2.4.6.1.12. Pasta de arquivos de programas;

2.1.2.4.6.1.13. Pasta temporária;

2.1.2.4.6.1.14. Lixeira;

2.1.2.4.6.1.15. Arquivo ou pasta especificada pelo administrador;

2.1.2.4.6.1.16. Setor de inicialização (boot);

2.1.2.4.6.1.17. Arquivos compactados;

2.1.2.4.6.1.18. Arquivos MIME;

2.1.2.4.6.2. Os tipos de arquivos que serão analisados;

2.1.2.4.6.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.

2.1.2.4.6.4. Áreas de exclusão que não deverão ser varridas;

2.1.2.4.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.

2.1.2.4.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

2.1.2.4.8.1. Limpar o arquivo;

2.1.2.4.8.2. Excluir o arquivo;

2.1.2.4.8.3. Negar acesso ao arquivo;

2.1.2.4.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após

detectar um programa indesejado:

2.1.2.4.9.1. Limpar o arquivo;

2.1.2.4.9.2. Excluir o arquivo;

2.1.2.4.9.3. Permitir acesso ao arquivo;

2.1.2.4.9.4. Negar acesso ao arquivo;

2.1.2.4.10. Para minimizar o impacto ao usuário, a solução deve permitir:

2.1.2.4.10.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;

2.1.2.4.10.2. Iniciar a varredura apenas quando o sistema estiver ocioso;

2.1.2.4.10.3. Permitir ao usuário retomar varreduras pausadas;

2.1.2.4.11. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

2.1.3. Características Módulo Antimalware (Clientes Linux)

2.1.3.1. Características da prevenção de ameaças

2.1.3.1.1. Deve permitir a atualização automática das vacinas de detecção;

2.1.3.1.2. Deve permitir a atualização automática das vacinas de detecção;

2.1.3.1.3. Deve detectar ameaças usando métodos de acesso e de varredura sob demanda;

2.1.3.1.4. Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas;

2.1.3.1.5. Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações:

2.1.3.1.5.1. Limpar o arquivo

2.1.3.1.5.2. Deletar o arquivo

2.1.3.1.5.3. Negar acesso ao arquivo;

2.1.3.1.6. Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos;

2.1.3.1.7. Deve permitir a opção de manter a configuração de exclusão realizada no agente, não sendo sobrescrita pela política principal;

2.1.3.1.8. Deve permitir a gestão do agente local por meio de linha de comando;

2.1.3.1.9. Ao configurar a análise ao acessar, deve permitir:

2.1.3.1.9.1. Quando analisar (exemplo: ao ler o arquivo)

2.1.3.1.9.2. O que analisar (exemplo: todos os arquivos);

2.1.3.1.9.3. Análise de arquivos compressos

2.1.3.1.9.4. Análise de volumes de rede

2.1.3.1.9.5. Análise de programas não desejados;

2.1.3.1.9.6. Ao configurar a análise sob demanda, deve permitir:

2.1.3.1.9.7. Análise de arquivos compressos

2.1.3.1.9.8. Análise de PUP;

2.1.3.1.9.9. Análise de macros desconhecidos

2.1.3.1.9.10. Análise de programas desconhecidos

2.1.3.1.9.11. Caminhos da análise (path);

2.1.3.1.9.12. Análise de pastas e subpastas

2.1.3.1.9.13. Análise de macros;

2.1.3.1.9.14. Exclusão de paths, pastas e tipos de arquivos

2.1.3.1.9.15. Uso de cache

2.1.3.1.9.16. Ação Primária e Secundária

2.1.3.1.10. Deve possuir quarentena local para armazenar ameaças desconhecidas;

2.1.3.1.11. Deve possuir ação para mover artefatos maliciosos para a área de quarentena;

2.1.3.1.12. Deve usar heurística para detectar arquivos potencialmente maliciosos;

2.1.3.1.13. Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo;

2.1.4. Características do Módulo de Firewall de Host (Clientes Windows)

2.1.4.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;

2.1.4.2. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura para ataques dia zero;

2.1.4.3. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;

2.1.4.4. Deve possuir assinaturas de proteção para:

2.1.4.4.1. Arquivos

2.1.4.4.2. Chave de Registro

2.1.4.4.3. Processos

2.1.4.4.4. Serviços;

2.1.4.5. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;

2.1.4.6. Deve ser possível bloquear tráfego bridge;

2.1.4.7. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

2.1.4.8. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;

2.1.4.9. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:

2.1.4.9.1. Nome

2.1.4.9.2. Nome do arquivo ou Caminho;

2.1.4.9.3. Hash MD5

2.1.4.9.4. Assinador Digital

2.1.4.10. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;

2.1.4.11. As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.

2.1.4.12. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;

2.1.4.13. Deve permitir inspeção do protocolo FTP;

2.1.4.14. Deve ser possível permitir tráfego de protocolos não suportados;

2.1.4.15. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

2.1.4.16. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:

2.1.4.16.1. Ação

2.1.4.16.1.1. Bloquear

2.1.4.16.1.2. Permitir

2.1.4.16.2. Direção

2.1.4.16.2.1. Ambas

2.1.4.16.2.2. Entrada

2.1.4.16.2.3. Saída

2.1.4.16.3. Protocolo

2.1.4.16.3.1. Qualquer protocolo

2.1.4.16.3.2. Protocolo IP

2.1.4.16.3.3. Ipv4

2.1.4.16.3.4. Ipv6

2.1.4.16.3.5. Protocolo Não-IP

2.1.4.16.4. Tipo de Conexão

2.1.4.16.4.1. Rede Sem Fio

2.1.4.16.4.2. Rede Cabeada

2.1.4.16.4.3. Rede Virtual

2.1.4.16.5. Especificação da Rede

2.1.4.16.5.1. Endereço IP

2.1.4.16.5.2. Subnet

2.1.4.16.5.3. Range

2.1.4.16.5.4. FQDN

2.1.4.16.6. Protocolo de Transporte

2.1.4.16.6.1. Todos

2.1.4.16.6.2. ICMP

2.1.4.16.6.3. ICMPv6

2.1.4.16.6.4. TCP

2.1.4.16.6.5. UDP

2.1.4.16.6.6. STP

2.1.4.16.6.7. GRE

2.1.4.16.6.8. IGMP

2.1.4.16.6.9. IPSEC AH

2.1.4.16.6.10. IPSEC ESP

2.1.4.16.6.11. Ipv6 in Ipv4

2.1.4.16.6.12. ISIS over Ipv4

2.1.4.16.6.13. L2TP

2.1.4.16.7. Agendamento

2.1.4.16.7.1. Dias da Semana

2.1.4.16.7.2. Hora Início

2.1.4.16.7.3. Hora Fim

2.1.4.16.8. Aplicações

2.1.5. Características do Módulo de Firewall de Host (Clientes Linux)

2.1.5.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;

2.1.5.2. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;

2.1.5.3. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

2.1.5.4. Deve permitir inspeção do protocolo FTP;

2.1.5.5. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

2.1.5.6. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:

2.1.5.6.1. Ação

2.1.5.6.1.1. Bloquear

2.1.5.6.1.2. Permitir

2.1.5.6.2. Direção

2.1.5.6.2.1. Ambas

2.1.5.6.2.2. Entrada

2.1.5.6.2.3. Saída

2.1.5.6.3. Protocolo

2.1.5.6.3.1. Qualquer protocolo

2.1.5.6.3.2. Protocolo IP

2.1.5.6.3.3. Ipv4

2.1.5.6.4. Tipo de Conexão

2.1.5.6.4.1. Rede Sem Fio

2.1.5.6.4.2. Rede Cabeada

2.1.5.6.4.3. Rede Virtual

2.1.5.6.5. Especificação da Rede

2.1.5.6.5.1. Endereço IP

2.1.5.6.5.2. Subnet

2.1.5.6.5.3. Range

2.1.5.6.5.4. FQDN

2.1.5.6.6. Protocolo de Transporte

2.1.5.6.6.1. Todos

2.1.5.6.6.2. ICMP

2.1.5.6.6.3. TCP

2.1.5.6.6.4. UDP

2.1.5.6.7. Agendamento

2.1.5.6.7.1. Dias da Semana

2.1.5.6.7.2. Hora Início

2.1.5.6.7.3. Hora Fim

2.1.6. Características do Módulo de Filtragem Web

2.1.6.1. Deve permitir o bloqueio de browsers não suportados, dentre eles:

2.1.6.1.1. Opera

2.1.6.1.2. Safari for Windows;

2.1.6.1.3. Netscape

2.1.6.1.4. Maxthon

2.1.6.1.5. Flock;

2.1.6.1.6. Avant Browser;

2.1.6.1.7. Deepnet Explorer

2.1.6.1.8. PhaseOut

2.1.6.2. Deve permitir o controle de browsers suportados, dentre eles:

2.1.6.2.1. Chrome

2.1.6.2.2. Firefox

2.1.6.2.3. Internet Explorer

2.1.6.3. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.

2.1.6.4. Deve possuir, no mínimo, as seguintes categorias:

2.1.6.4.1. Browser Exploits;

2.1.6.4.2. Download Maliciosos;

2.1.6.4.3. Sites Maliciosos;

2.1.6.4.4. Phishing;

2.1.6.4.5. Pornografia;

2.1.6.4.6. Hacking/Computer Crime;

2.1.6.4.7. Spyware/Adware/Keyloggers;

2.1.6.4.8. Anonymizer;

2.1.6.4.9. Anonymizer Utilities;

2.1.6.4.10. Dating

2.1.6.4.11. Dating/Social Networking

2.1.6.4.12. Discrimination;

2.1.6.4.13. Drugs;

2.1.6.4.14. Gambling

2.1.6.4.15. Games

2.1.6.4.16. Government/Military

2.1.6.4.17. Media Downloads

2.1.6.4.18. Media Sharing

2.1.6.4.19. Nudity

2.1.6.4.20. P2P/File Sharing

2.1.6.4.21. Potentially Unwanted Programs

2.1.6.4.22. Social Networking

2.1.6.4.23. Streaming Media

2.1.6.4.24. Text Translators

2.1.6.4.25. Web Mail

2.1.6.5. Deve ser possível bloquear um site conforme a sua classificação:

2.1.6.5.1. Vermelho: Alto Risco

2.1.6.5.2. Amarelo: Médio Risco

2.1.6.5.3. Cinza: Não categorizado

2.1.6.6. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;

2.1.6.7. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;

2.1.6.8. Deve permitir a varredura de arquivos baixados da internet;

2.1.6.9. Deve ser possível excluir endereços IP da análise;

2.1.6.10. Deve permitir a busca segura para buscadores, dentre eles:

2.1.6.10.1. Google;

2.1.6.10.2. Yahoo

2.1.6.10.3. Bing;

2.1.6.10.4. Ask;

2.1.6.11. Deve bloquear links que direcionem para sites com alto risco.

2.1.6.12. Deve permitir a customização das mensagens apresentadas para o usuário;

2.1.7. Características do Módulo de Ameaças Avançadas

2.1.7.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)

2.1.7.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;

2.1.7.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;

2.1.7.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada

2.1.7.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas.

2.1.7.6. Dentre os comportamentos maliciosos, deve ser capaz de:

2.1.7.6.1. Bloquear acesso local a partir de cookies;

2.1.7.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

2.1.7.6.3. Criação de arquivos em qualquer local de rede;

2.1.7.6.4. Criação de novos CLSIDs, APPIDs e TYPELIBs;

2.1.7.6.5. Criação de threads em outro processo;

2.1.7.6.6. Bloquear a desativação de executáveis críticos do sistema operacional;

2.1.7.6.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

2.1.7.6.8. Gravação e Leitura na memória de outro processo;

2.1.7.6.9. Bloqueio de Modificação da política de firewall do Windows;

2.1.7.6.10. Bloqueio de Modificação da pasta de tarefas do Windows;

2.1.7.6.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;

2.1.7.6.12. Bloqueio de Modificação de arquivos executáveis portáteis;

2.1.7.6.13. Bloqueio de Modificação de bit de atributo oculto;

2.1.7.6.14. Bloqueio de Modificação de bit de atributo somente leitura;

2.1.7.6.15. Bloqueio de Modificação de entradas de registro de DLL AppInit;

2.1.7.6.16. Bloqueio de Modificação de locais do registro de inicialização;

2.1.7.6.17. Bloqueio de Modificação de pastas de dados de usuários;

2.1.7.6.18. Bloqueio de Modificação do local do Registro de Serviços;

2.1.7.6.19. Bloqueio de Suspensão de um processo;

2.1.7.6.20. Bloqueio de Término de outro processo.

2.1.7.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

2.1.7.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.

2.1.7.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

2.1.7.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário

2.1.7.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção

2.1.7.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";

2.1.7.13. A solução deve ter a capacidade de remediação de ações efetuadas por artefatos maliciosos, como criação de arquivos e alteração de chaves de registro.

2.1.7.13.1. A remediação deve ser efetuada de maneira automática, a partir do momento em que o artefato é identificado como malicioso.

2.1.8. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:

2.1.8.1. A solução deve possuir capacidade de criar uma reputação local, além de utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;

2.1.8.2. O servidor de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos.

2.1.8.3. Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;

2.1.8.4. A troca de informação de ameaças deve se dar por meio de protocolo performático;

2.1.8.5. De forma a permitir menor impacto na rede, para tal método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona;

2.1.8.6. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:

2.1.8.6.1. Reputação local

2.1.8.6.2. Reputação do centro de inteligência

2.1.8.7. Ao catalogar um arquivo, a solução deve apresentar, no mínimo as seguintes informações:

2.1.8.7.1. Nome do arquivo

2.1.8.7.2. Caminho do arquivo

2.1.8.7.3. Hash sha-1

2.1.8.7.4. Hash 256

2.1.8.7.5. Primeira visualização do arquivo na rede

2.1.8.7.6. Última visualização do arquivo na rede

2.1.8.7.7. Tamanho do arquivo

2.1.8.7.8. Data de compilação

2.1.8.7.9. Se o mesmo consta no adicionar/remover programas

2.1.8.7.10. Se está registrado como serviço

2.1.8.7.11. Se está registrado para ser executado automaticamente

2.1.8.7.12. Tipo de compactador

2.1.8.7.13. Se é arquivo do sistema

2.1.8.7.14. Se foi executado a partir do cmd.exe

2.1.8.7.15. Se tem entrada no menu iniciar

2.1.8.7.16. Se foi executado a partir de uma mídia removível

2.1.8.7.17. Se foi executado a partir da raiz da unidade do sistema

2.1.8.8. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;

2.1.8.9. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (exemplo: Virus Total);

2.1.8.10. Após análise pela solução o administrador deve ter a possibilidade de:

2.1.8.10.1. Rastrear em quais estações o arquivo foi executado;

2.1.8.10.2. Identificar o arquivo como confiável;

2.1.8.10.3. Identificar o arquivo como desconhecido;

2.1.8.10.4. Identificar o arquivo como malicioso

2.1.8.10.5. Analisar o certificado associado ao arquivo;

2.1.8.10.6. Identificar o certificado associado como confiável ou malicioso;

2.1.8.11. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação nos endpoints e servidores protegidos;

2.1.8.12. Deve ser possível bloquear a execução de arquivos nunca antes vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem.

2.1.8.13. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;

2.1.8.14. Deve ser gerenciado pela mesma console de gerenciamento da solução de proteção de endpoints e servidores.

2.1.9. Características da solução de Detecção e Resposta a Incidentes

2.1.9.1. Capacidade de Detectar e Responder a incidentes relacionadas a ameaças avançadas, com capacidade avançada de investigação e que permita ao gestor da solução rápida resposta.

2.1.9.2. Deve permitir por meio de severidade dos alertas que o operador da solução facilmente entenda a ameaça e priorize o tratamento.

2.1.9.3. Deve facilitar a operação por meio de guias de investigação que automaticamente coleta, sumariza e visualmente evidencie, por meio de fontes diversas, a interação conforme a investigação avance.

2.1.9.4. A ferramenta deve possuir capacidade de monitoramento contínuo em tempo real.

2.1.9.5. Deve possuir base de dados analítica na nuvem, permitindo uma adoção mais rápida e otimizada das novas técnicas e motores analíticos para auxiliar na detecção de ameaça.

2.1.9.6. A ferramenta deve possuir mapeamento do framework do MITRE ATT&CK para determinar a fase de uma determinada ameaça, risco associado e que com base nestas informações auxilie na priorização de uma resposta.

2.1.9.7. Os guias de investigação devem utilizar inteligência artificial para auxiliar na identificação dos principais problemas detectados que identifiquem a causa raíz do ataque.

2.1.9.8. Deve permitir a integração com outras soluções e bases terceiras para coletar informações que agreguem mais contexto e relevância a investigação, como por exemplo:

2.1.9.8.1. SIEM – Splunk Enterprise Security Manager

2.1.9.8.2. SIEM – Micros Focus ArcSight Enterprise Security Manager

2.1.9.8.3. SIEM – McAfee Enterprise Security Manager

2.1.9.8.4. SIEM - Microsoft Sentinel

2.1.9.8.5. Centro de Inteligência do próprio fabricante

2.1.9.8.6. VirusTotal

2.1.9.9. A solução deverá prover buscas diversas, abrangendo:

2.1.9.9.1. Busca histórica, permitindo a visibilidade, em detalhes, dos indicadores de comprometimento e indicadores de ataque. A informação deverá estar disponível mesmo que o dispositivo investigado esteja desligado.

2.1.9.9.2. Busca Tempo Real, permite o acesso em tempo real ao dispositivo investigado em busca de uma determinada informação.

2.1.9.9.3. Busca Sob-Demanda, para suplementar uma investigação, deve permitir a captura de uma imagem (snapshot) do dispositivo investigado, permitindo que esta imagem seja capturada de máquinas gerenciadas e não gerenciadas.

2.1.9.10. A gestão dos dispositivos, pode ser feita por meio de console:

2.1.9.10.1. On-Premise: Toda camada de comunicação e gestão dos agentes é instalada no ambiente, entretanto a console de investigação está na nuvem do fabricante (SaaS)

2.1.9.10.2. SaaS: Toda camada de comunicação e gestão dos agentes é gestionada na nuvem do fabricante, em conjunto com a console de investigação.

2.1.9.11. Deve suportar os sistemas operacionais:

2.1.9.11.1. Windows:

2.1.9.11.1.1. Windows 10 Enterprise

2.1.9.11.1.2. Windows 8.1 Enterprise

2.1.9.11.1.3. Windows 8

2.1.9.11.1.4. Windows Server 2019 (64-bits)

2.1.9.11.1.5. Windows Server 2016 (64-bits)

2.1.9.11.1.6. Windows Server 2012 (64-bits)

2.1.9.11.2. MacOS

2.1.9.11.2.1. BigSur 11.0;

2.1.9.11.2.2. Catalina 10.15.6 e superiores;

2.1.9.11.3. Linux

2.1.9.11.3.1. CentOS (64-bits)

2.1.9.11.3.2. Red Hat (64-bits)

2.1.9.11.3.3. SUSE (64-bits)

2.1.9.12. A solução deve possuir capacidade investigativa, informando:

2.1.9.12.1. Total de investigações abertas

2.1.9.12.2. Novas Investigações por dia

2.1.9.12.3. Principais Detecções

2.1.9.12.4. Tempo total gasto nas investigações

2.1.9.12.5. Tempo total gasto nas investigações pelo usuário logado

2.1.9.12.6. Quantidade de investigações com prioridade alta

2.1.9.12.7. Quantidade de investigações fechadas

2.1.9.12.8. Quantidade de investigações em aberto

2.1.9.13. A solução deverá possuir um painel de alertas, contendo os principais “achados” (findings) detectados pela solução;

2.1.9.14. Deverá dividir os alertas por prioridade, entre:

2.1.9.14.1. Alto

2.1.9.14.2. Médio

2.1.9.14.3. Baixo

2.1.9.15. O painel de alerta, deverá possuir integração com o Framework do MITRE ATT&CK, apresentando:

2.1.9.15.1. Data, hora e ano da ocorrência

2.1.9.15.2. Linha de comando envolvida

2.1.9.15.3. Tática

2.1.9.15.4. Técnica

2.1.9.15.5. Ativo envolvido

2.1.9.15.6. Nome do Processo

2.1.9.15.7. Indicadores Suspeitos, com detalhes

2.1.9.16. O Painel de Alertas deverá permitir ao analista, que este possa visualizar, em mais detalhes o alerta, apresentando:

2.1.9.16.1. Versão do Sistema Operacional

2.1.9.16.2. Endereço IP

2.1.9.16.3. MAC Address

2.1.9.16.4. Última data de Boot

2.1.9.16.5. Tags

2.1.9.16.6. Usuário Logado

2.1.9.17. A solução deverá permitir buscas, nos dispositivos gerenciados, nos modos histórico e em tempo-real.

2.1.9.18. No modo histórico, deverá apresentar as informações correlacionadas com o Framework do MITRE ATT&CK

2.1.9.19. No modo histórico, ao selecionar um dos dispositivos gerenciados, deverá apresentar:

2.1.9.19.1. Detecções e Alertas, contendo:

2.1.9.19.1.1. Data, hora e ano

2.1.9.19.1.2. ID do Processo envolvido

2.1.9.19.1.3. Nome do Processo

2.1.9.19.1.4. Linha de Comando

2.1.9.19.1.5. Usuário

2.1.9.19.1.6. Tática

2.1.9.19.1.7. Técnicas

2.1.9.19.2. Histórico de execução de Processos

2.1.9.19.2.1. Data, hora e ano

2.1.9.19.2.2. ID do processo

2.1.9.19.2.3. Usuário (Autor)

2.1.9.19.2.4. Nome original do processo

2.1.9.19.2.5. MD5/SHA-256

2.1.9.19.2.6. Linha de Comando

2.1.9.19.3. Manipulação de arquivos

2.1.9.19.3.1. Data, hora e ano

2.1.9.19.3.2. Atividade (Deletado, Executado, Criado)

2.1.9.19.3.3. MD5/SHA-256 do arquivo

2.1.9.19.3.4. Nome do arquivo
2.1.9.19.3.5. ID do Processo
2.1.9.19.3.6. Nome original do arquivo
2.1.9.19.3.7. Linha de comando de execução
2.1.9.19.3.8. Tamanho (bytes)
2.1.9.19.4. Criação de arquivos do tipo Archive
2.1.9.19.4.1. Data, hora e ano
2.1.9.19.4.2. Atividade
2.1.9.19.4.3. Nome do arquivo
2.1.9.19.4.4. Extensão (Exemplo: Bin, ZIP, dentre outros)
2.1.9.19.4.5. Caminho
2.1.9.19.5. Detecção de Scripts
2.1.9.19.5.1. Data, hora e ano
2.1.9.19.5.2. Atividade (Leitura, Criação, Movido, dentre outros)
2.1.9.19.5.3. Nome do arquivo
2.1.9.19.5.4. Extensão (Exemplo: JS, Powershell)
2.1.9.19.6. Ferramentas Administrativas ou Hacking
2.1.9.19.6.1. Data, hora e ano
2.1.9.19.6.2. Usuário (Autor)
2.1.9.19.6.3. Processo
2.1.9.19.6.4. ID do processo
2.1.9.19.6.5. MD5/SHA-256
2.1.9.19.6.6. Linha de comando
2.1.9.19.7. Alteração dos Serviços do Sistema Operacional
2.1.9.19.7.1. Data, hora e ano
2.1.9.19.7.2. Nome do Serviço
2.1.9.19.7.3. Ação (Exemplo: Adicionado, Modificado)
2.1.9.19.7.4. Tipo
2.1.9.19.7.5. Tipo de inicialização do processo
2.1.9.19.8. Conexão de Rede
2.1.9.19.8.1. Data, hora e ano
2.1.9.19.8.2. ID do Processo
2.1.9.19.8.3. Tipo (Exemplo: Conexão aberta)
2.1.9.19.8.4. Direção do fluxo
2.1.9.19.8.5. Endereço IP de Origem
2.1.9.19.8.6. Porta de Origem

2.1.9.19.8.7. Endereço IP de Destino

2.1.9.19.8.8. Porta de Destino

2.1.9.19.8.9. Protocolo

2.1.9.19.8.10. Hostname

2.1.9.19.9. Tarefas agendadas

2.1.9.19.9.1. Data, hora e ano

2.1.9.19.9.2. Usuário

2.1.9.19.9.3. Nome da tarefa

2.1.9.19.9.4. Comando da tarefa

2.1.9.19.9.5. Ação

2.1.9.19.10. Requisições de DNS

2.1.9.19.10.1. Data, hora e ano

2.1.9.19.10.2. ID do processo

2.1.9.19.10.3. Dominio

2.1.9.19.10.4. Tipo

2.1.9.19.11. Atividade de Logon

2.1.9.19.11.1. Data, hora e ano

2.1.9.19.11.2. Usuário

2.1.9.19.11.3. Tipo

2.1.9.19.11.4. Domínio

2.1.9.19.11.5. Tipo de Logon

2.1.9.19.12. DLLs Carregadas

2.1.9.19.12.1. Data. Hora e ano

2.1.9.19.12.2. Módulo

2.1.9.19.12.3. Caminho

2.1.9.19.12.4. Sha256 da DLL

2.1.9.19.12.5. Data, hora e ano que a dll foi carregada

2.1.9.19.12.6. Id do processo

2.1.9.20. Adicionalmente a busca histórica a ferramenta deve possuir capacidade de busca nos equipamentos gerenciados em tempo real.

2.1.9.21. Para a busca nos equipamentos gerenciados, a solução deve ser composta por coletores capazes de consolidar informações relacionadas a dados que devem ser monitorados e apresentados na console para investigação.

2.1.9.22. O fabricante deverá disponibilizar coletores para, no mínimo, a coleta das seguintes informações nos dispositivos gerenciados:

2.1.9.22.1. Registro do Windows;

2.1.9.22.2. Perfil dos Usuários

2.1.9.22.3. Dispositivos USB;

2.1.9.22.4. Informação de inicialização do sistema operacional;

2.1.9.22.5. Softwares instalados;

2.1.9.22.6. Serviços do sistema operacional

2.1.9.22.7. Tarefas agendadas

2.1.9.22.8. Processos em execução;

2.1.9.22.9. Drives de Rede

2.1.9.22.10. Sessão de Rede

2.1.9.22.11. Flows de Rede

2.1.9.22.12. Usuários Logados

2.1.9.22.13. Updates do Windows instalados;

2.1.9.23. Ferramenta deve permitir que coletores customizados sejam criados para as seguintes plataformas:

2.1.9.23.1. Windows

2.1.9.23.2. Mac

2.1.9.23.3. Linux

2.1.9.24. A criação de coletores customizados deve utilizar linguagem comum aos sistemas, como por exemplo:

2.1.9.24.1. Powershell

2.1.9.24.2. Python

2.1.9.24.3. Visual Basic

2.1.9.24.4. Bash

2.1.9.24.5. Comandos do sistema operacional

2.1.9.25. A busca em tempo real, ao se obter o resultado desejado, deve permitir que se aplique reações, frente a busca realizada.

2.1.9.26. As reações devem conter:

2.1.9.26.1. Isolamento de um Endpoint;

2.1.9.26.2. Matar Processo

2.1.9.26.3. Remover um arquivo

2.1.9.26.4. Logoff do usuário logado

2.1.9.27. Deve permitir a criação de reações customizadas para atuar em conjunto com a busca realizada e seu respectivo resultado

2.1.9.28. A busca em tempo real deve possuir capacidade de sugerir os parâmetros de busca para facilitar a obtenção do resultado desejado

2.1.9.29. Caso a busca tenha um erro em sua sintaxe, a console deverá emitir um alerta de erro. Caso contrário, apresentar que a busca é válida.

2.1.9.30. Deve apresentar a quantidade de hosts que receberam o comando de busca em tempo real.

2.1.9.31. Deve prover registro do histórico de ações executados com as seguintes informações em tela:

2.1.9.31.1. Dispositivo

2.1.9.31.2. Ação

2.1.9.31.3. Sistema Operacional

2.1.9.31.4. Tag ePO

2.1.9.31.5. Endereço MAC

2.1.9.31.6. Endereço IP

2.1.9.32. Deve ser capaz de implementar visibilidade dos dados gerados pelo Endpoint, como por exemplo:

2.1.9.32.1. Processos;

2.1.9.32.2. Fluxos de comunicação de rede;

2.1.9.32.3. Arquivos;

2.1.9.32.4. Perfil de Usuários;

2.1.9.32.5. Registro do Windows;

2.1.9.32.6. Atualizações Instalados;

2.1.9.32.7. Grupos Locais

2.1.9.32.8. Informação do Host;

2.1.9.33. Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca:

2.1.9.33.1. Endereço IP Local;

2.1.9.33.2. Hash do processo em execução;

2.1.9.33.3. ID do processo;

2.1.9.33.4. Status da transação TCP;

2.1.9.33.5. Número da porta que originou o pacote de rede;

2.1.9.33.6. Nome do arquivo;

2.1.9.33.7. Última data de gravação do arquivo;

2.1.9.33.8. Data de Criação do arquivo

2.1.9.33.9. Data de deleção do arquivo

2.1.9.33.10. Versão do Sistema Operacional;

2.1.9.33.11. Nome do Grupo de usuários

2.1.9.33.12. Se o grupo é local

2.1.9.33.13. SID do grupo

2.1.9.33.14. MAC de origem

2.1.9.33.15. MAC de destino

2.1.9.33.16. FLAGS TCP (ACK, SYN, RST e FIN)

2.1.9.33.17. Número de transação TCP;

2.1.9.33.18. Kernel Time;

2.1.9.33.19. User Time;

2.1.9.33.20. Comando que iniciou o processo;

2.1.9.33.21. Quantidade de RAM utilizada pelo processo;

2.1.9.33.22. Quantidade de Threads criadas pelo processo;

2.1.9.33.23. MD5 do processo;

2.1.9.33.24. SHA-1 do processo;

2.1.9.33.25. Valor da chave de registro

2.1.9.33.26. Caminho da chave de registro;

2.1.9.34. A resposta a uma determinada condição deverá ser executada como um serviço não interativo;

2.1.9.35. O Painel de investigação deve ser simples, intuitivo e capaz de informar, de maneira resumida, a postura corrente das investigações, em curso e fechadas.

2.1.9.36. Deve permitir a criação de até 10 investigações por hora.

2.1.9.37. Cada porção de dado coletado pela solução para apresentação no painel de investigação, deve ficar disponível por até 30 dias.

2.1.9.38. As investigações, podem ser classificadas por severidade (exemplo: Severidade Alta)

2.1.9.39. Ao acessar um caso de investigação, a solução deverá apresentar, de maneira sumarizada, a quantidade de artefatos descoberta, a quantidade de artefatos chave e a quantidade de pontos chave no qual o operador da solução deve focar.

2.1.9.40. Deve permitir adicionar integrações que suplementem a investigação de um determinado caso, a exemplo o envio de um phishing para análise pela solução e posterior adição a um caso de investigação.

2.1.9.41. Por meio de painéis interativos (widgets) a solução deve prover informações relacionadas a:

2.1.9.41.1. Sumário: informando a criação, dono da investigação e um campo para detalhamento da descrição

2.1.9.41.2. Notas: inserção de notas pertinentes a investigação em curso

2.1.9.41.3. Itens Investigados: Sumário contendo a quantidade de dispositivos envolvidos, contas de usuário, endereços IP's, DNS, FQDN, processos, serviços, arquivos e conexões de rede.

2.1.9.41.4. Investigações Correlacionadas

2.1.9.41.5. Guias de Investigações: Os guias de investigação deverão ser baseados em:

2.1.9.41.5.1. Perguntas Respondidas: Contendo as principais perguntas que devem ser respondidas pelos analistas, como por exemplo: Quais processos desconhecidos em execução foram encontrados? Existe algum processo abrindo alguma comunicação de rede que não é comum? Existe processo em execução com nome randomizado? Existe alguma evidência de uso de ferramentas de hacking ou admin?

2.1.9.41.5.2. Questões Mitre: deve relacionar as principais respostas do MITRE framework

relacionadas a evidências encontradas

2.1.9.41.5.3. Hipótese: indicativo de comportamento anômalo baseado em hipótese com base em perguntas chave (Inteligência Artificial)

2.1.9.41.6. Visualização Geral da Investigação:

2.1.9.41.6.1. Sumarizada: Deve apresentar um sumário geral da situação, progresso, entidades envolvidas na investigação, investigações similares e os principais indicadores de comprometimento.

2.1.9.41.6.2. Gráfica: Apresentação em formato gráfico com os links de relacionamento entre todos os artefatos encontrados. A visualização gráfica deve se moldar, permitindo o drill-down desde o montante total de artefatos descobertos até os achados principais.

2.1.9.41.6.2.1. Deve ser possível identificar, por meio de cores distintas, os relacionamentos entre entidades externas e entidades internas.

2.1.9.41.6.2.2. Deve ser possível agrupar os artefatos descobertos e os principais indicios por grupo, para facilitar a visualização.

2.1.9.41.6.2.3. Deve ser possível filtrar o gráfico dentre as opções:

2.1.9.41.6.2.3.1. Endereço IP

2.1.9.41.6.2.3.2. DNS Lookup

2.1.9.41.6.2.3.3. Dispositivo

2.1.9.41.6.2.3.4. FQDN

2.1.9.41.6.2.3.5. Arquivo

2.1.9.41.6.2.3.6. Conexão de Rede

2.1.9.41.6.2.3.7. Processo

2.1.9.41.6.2.3.8. Serviço

2.1.9.41.6.2.4. Ao interagir com algum dos indícios encontrados, a solução de investigação deverá apresentar um widget na qual deverá apresentar mais detalhes sobre os indicativos, inclusive permitindo a interação por meio de ações, como por exemplo:

2.1.9.41.6.2.4.1. Capturar uma imagem da máquina,

2.1.9.41.6.2.4.2. Isolar a máquina da rede,

2.1.9.41.6.2.4.3. Buscar um processo executado em outras máquinas monitoradas

2.1.9.41.6.2.5. O Widget deverá trazer informações capazes de suplementar a investigação, trazendo informações com mais detalhes.

2.1.9.41.6.3. Guias: Apresentar um sumário do guia de investigação

2.1.9.41.6.4. Tabulada: Visão geral sobre os artefatos identificados, com sumário e um detalhamento do mesmo.

2.1.9.41.6.5. Dispositivos: Dispositivos afetados, incluindo nome, versão do sistema operacional, identificador e o status.

2.1.9.42. Deverá possuir um painel de monitoramento onde a incidência de atividade maliciosa deve ser apresentada.

2.1.9.43. Para cada artefato malicioso monitorado, deve apresentar:

2.1.9.43.1. Painel de ação:

2.1.9.43.1.1. Iniciar uma investigação

2.1.9.43.1.2. Excluir do monitoramento

2.1.9.43.2. Painel com detalhes do processo:

2.1.9.43.2.1. Modo de detecção

2.1.9.43.2.2. Primeira detecção

2.1.9.43.2.3. Última detecção

2.1.9.43.2.4. Dispositivos afetados

2.1.9.43.2.5. Tempo de vida no ambiente

2.1.9.43.2.6. MD5, SHA-1 e SHA-256

2.1.9.43.3. Painel de Ação – Dispositivos:

2.1.9.43.3.1. Parar um processo

2.1.9.43.3.2. Parar e remover

2.1.9.43.3.3. Quarentenar a estação de trabalho

2.1.9.43.4. Painel de Comportamento

2.1.9.43.4.1. Apresentar as Técnicas observadas e compará-las a matriz do Mitre.

2.1.9.43.4.2. Apresentar os indicadores suspeitos identificados

2.1.9.43.5. Atividade do Processo

2.1.9.43.5.1. Sumário

2.1.9.43.5.2. Deve permitir comparar o observado com o guia SANS DFIR

2.1.9.43.5.3. Deve apresentar a interação do processo por:

2.1.9.43.5.4. Modo sequencial: Sequência de interações do processo, até o ponto de identificação da atividade suspeita

2.1.9.43.5.5. Modo Temporal: Linha de tempo, até o ponto de identificação da atividade suspeita

2.1.9.43.5.6. Modo tabulado: Detalhamento dos eventos por linhas, até a identificação da atividade suspeita.

2.1.10. Solução de proteção para dispositivos móveis

2.1.10.1. A solução de "Proteção para dispositivos móveis", deve proteger a CONTRATANTE contra as ameaças em dispositivos móveis, Android e IOS, incluindo malwares, ameaças de rede, identificação de vulnerabilidades e defesa física dos dispositivos. O objetivo principal desta solução é proteger os usuários móveis, impedindo que ameaças nestes dispositivos possam impactar nos serviços e na rede da CONTRATANTE.

2.1.10.2. Características Gerais:

2.1.10.2.1. Deverá ser ofertado como um serviço on premises (local) ou em console baseada em nuvem de forma a garantir suas funcionalidades independente da rede que o dispositivo estiver conectado;

2.1.10.2.2. A solução deverá possuir console WEB para administração da solução;

2.1.10.2.3. Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;

2.1.10.2.4. Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede, vulnerabilidades e malwares encontrados;

2.1.10.2.5. Deverá possuir uma apresentação gráfica referente as informações dos dispositivos registrados na solução;

2.1.10.2.6. Associar o nome do usuário ao nome do dispositivo, o modelo e a versão do sistema operacional, em console gráfica;

2.1.10.2.7. A console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o mesmo e o dispositivo que gerou o incidente;

2.1.10.2.8. A solução deverá apresentar um relatório de ações recomendadas, para que com tais dados os administradores da solução possam criar ações para melhorar a segurança dos dispositivos móveis da empresa;

2.1.10.2.9. A solução deverá ser categorizada como uma solução de MTD (Mobile Threat Defense);

2.1.10.2.10. Deverá ser compatível com os sistemas operacionais IOS e Android;

2.1.10.2.11. Deverá integrar-se com as principais tecnologias de MDM ou EMM do mercado, no mínimo com MobileIron, Microsoft Intune e Airwatch;

2.1.10.2.12. O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para IOS e Google Play para Android;

2.1.10.2.13. Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alertas seja visível para o usuário final, através de modo não interativo;

2.1.10.2.14. Deverá possuir as seguintes características mínimas de proteção:

2.1.10.2.14.1. Proteção contra Malwares:

2.1.10.2.14.1.1. Proteção em tempo real contra malwares conhecidos e desconhecidos;

2.1.10.2.14.2. Defesa física

2.1.10.2.14.2.1. Identificação de upgrades do sistema operacional;

2.1.10.2.14.2.2. Identificação de dispositivo com root;

2.1.10.2.14.2.3. Identificação de configurações de segurança, como tela de bloqueio não habilitada;

2.1.10.2.15. Deverá ser possível instalar a solução através de integração com solução de MDM/EMM ou através da própria console, utilizando e-mail;

2.1.10.2.16. Deverá possuir integração com solução de SIEM de mercado;

2.1.10.2.17. A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de Email.

2.1.11. Características do Módulo de Controle de Dispositivos

2.1.11.1. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;

2.1.11.2. Deve permitir a configuração dos dispositivos nos modos:

2.1.11.2.1. Bloqueio, ou;

2.1.11.2.2. Somente Leitura;

2.1.11.3. Deve classificar os dispositivos removíveis em 3 categorias:

2.1.11.3.1. Gerenciado;

2.1.11.3.2. Não Gerenciável (Exemplo: Bateria de Notebooks);

2.1.11.3.3. Não Gerenciado;

2.1.11.4. Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:

2.1.11.4.1. Tipo de BUS;

2.1.11.4.2. Classe do Dispositivo (Device Class)

2.1.11.4.3. ID do fabricante (Vendor ID)

2.1.11.4.4. ID do produto (Product ID)

2.1.11.5. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:

2.1.11.5.1. Tipo de BUS

2.1.11.5.2. Se o sistema de arquivo é passível de escrita;

2.1.11.5.3. Se o sistema de arquivo é somente leitura;

2.1.11.5.4. Tipo de Sistema de Arquivo

2.1.11.5.5. Nome do Sistema de Arquivo;

2.1.11.5.6. Número de Série do Sistema de Arquivo;

2.1.11.6. Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive);

2.1.12. Características do Módulo de Controle de Aplicações

2.1.12.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

2.1.12.2. Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.

2.1.12.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;

2.1.12.4. Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);

2.1.12.5. Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;

2.1.12.6. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas

aplicações instaladas na máquina;

2.1.12.7. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;

2.1.12.8. Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:

2.1.12.8.1. Desabilitado: proteção desativada

2.1.12.8.2. Monitoramento: Monitora toda a atividade da Estação de Trabalho;

2.1.12.8.3. Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;

2.1.12.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).

2.1.12.10. A solução deve suportar as seguintes modalidades de proteção:

2.1.12.10.1. Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.

2.1.12.10.2. Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

2.1.12.11. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.

2.1.12.12. Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.

2.1.12.13. Suporta os mecanismos:

2.1.12.13.1. Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, entre outros) possam ser executados.

2.1.12.13.2. Memory Protection: permite proteção para ataques e exploração de vulnerabilidades para os programas em Whitelist.

2.1.12.14. Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:

2.1.12.14.1. Binário: binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.

2.1.12.14.2. Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).

2.1.12.14.3. Trusted Installer: software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.

2.1.12.14.4. Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

2.1.12.14.5. Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

2.1.12.14.6. Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

2.1.12.14.7. Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.

2.1.12.15. Deve ser capaz de proteger em modo standalone - online ou offline;

2.1.12.16. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;

2.1.12.17. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%)

2.1.12.18. Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo:%PROGRAMFILES (x86)%)

2.1.12.19. Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:

2.1.12.19.1. Critical Address Space Protection;

2.1.12.19.2. NX - No eXecute (mp-nx)

2.1.12.19.3. Virtual Address Space Randomization

2.1.12.19.4. Mp-vasr-randomization

2.1.12.19.5. Mp-vasr-relocation

2.1.12.19.6. Mp-vasr-reloc

2.1.12.19.7. Forced DLL Relocation

2.1.12.20. Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.

2.1.13. Características do Módulo de Gerenciamento

2.1.13.1. Deve ser disponibilizado em solução local (on-premise) ou em nuvem;

2.1.13.2. Solução de gerenciamento on-premise:

2.1.13.2.1. Deve suportar a instalação nos seguintes sistemas operacionais:

2.1.13.2.1.1. Windows Server 2019;

2.1.13.2.1.2. Windows Server 2016;

2.1.13.2.1.3. Windows Server 2012 Release 2;

2.1.13.2.1.4. Windows Server 2012.

2.1.13.2.2. A arquitetura dos Sistemas Operacionais deve ser 64-bits;

2.1.13.2.3. Deve suportar a instalação em Cluster Microsoft;

2.1.13.2.4. Deve suportar Ipv4 e Ipv6;

2.1.13.2.5. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

2.1.13.2.5.1. Vmware ESX

2.1.13.2.5.2. Citrix Xen Server

2.1.13.2.5.3. Microsoft Hyper-V

2.1.13.2.6. Deve possuir suporte a base de dados:

2.1.13.2.6.1. SQL Server 2014 ou superior

2.1.13.2.7. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

2.1.13.2.8. Deve ser possível segregar a instalação da solução em:

2.1.13.2.8.1. Servidor Console Central

2.1.13.2.8.2. Servidor Base de Dados

2.1.13.2.8.3. Servidor de Interação com os Agentes

2.1.13.2.8.4. Agentes Distribuidores de Vacina

2.1.13.2.9. Deve suportar o uso do SQL Server em ambientes SAN;

2.1.13.2.10. Permitir a instalação dos Módulos da Solução a partir de um único servidor;

2.1.13.3. A console de gerência deve ser acessada via WEB;

2.1.13.4. Deve possuir compatibilidade com os seguintes browsers:

2.1.13.4.1. Google Chrome;

2.1.13.4.2. Firefox;

2.1.13.4.3. Internet Explorer 7 ou superior;

2.1.13.4.4. Safari 6.0 ou superior;

2.1.13.5. Permitir a alteração das configurações dos Módulos da Solução nos clientes de maneira remota

2.1.13.6. Permitir a atualização incremental da lista de definições de vírus nos clientes.

2.1.13.7. Permitir a visualização das características básicas de hardware das máquinas

2.1.13.8. Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local

2.1.13.9. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

2.1.13.10. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado.

2.1.13.11. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

2.1.13.12. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

2.1.13.13. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente.

2.1.13.14. Permitir a criação de grupos virtuais através de marcadores;

2.1.13.15. Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

2.1.13.16. Forçar a configuração determinada no servidor para os clientes;

2.1.13.17. Caso o cliente altere a configuração, ela deverá retornar ao padrão estabelecido no servidor, quando ela for verificada pelo agente.

2.1.13.18. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS.

2.1.13.19. Forçar a instalação dos Módulos da Solução nos clientes;

2.1.13.20. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

2.1.13.21. O módulo de gestão deverá apresentar relatórios e dashboards consolidados, sem necessidade de ferramenta externa.

2.1.13.22. Deve ser possível realizar a customização dos relatórios gráficos gerados;

2.1.13.23. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML

2.1.13.24. Geração de relatórios que contenham as seguintes informações:

2.1.13.24.1. Máquinas com a lista de definições de vírus desatualizada;

2.1.13.24.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

2.1.13.24.3. Os vírus que mais foram detectados;

2.1.13.24.4. As máquinas que mais sofreram infecções em um determinado período;

2.1.13.24.5. Os usuários que mais sofreram infecções em um determinado período;

2.1.13.25. A solução de gestão deve possuir dashboards no gerenciamento da solução;

2.1.13.26. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:

2.1.13.26.1. Relatório dos últimos 7 dias da detecção de códigos maliciosos;

2.1.13.26.2. Sites bloqueados pela política;

2.1.13.27. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN);

2.1.13.28. Deve possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;

2.1.13.29. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por vertical de negócio;

2.1.13.30. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por pais, incluindo o Brasil;

2.1.13.31. A solução deve ser capaz de proporcionar a busca em campanhas globais por ameaças baseadas em nome e/ou IOCs;

2.1.13.32. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a uma determinada campanha;

2.1.13.33. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação as campanhas de ameaças globais identificadas na base de inteligência do fabricante;

2.1.13.34. Deve ser capaz de propor procedimentos de mitigação dos riscos de segurança

nos endpoints referentes a campanhas de ameaças específicas;

2.1.13.35. Cada campanha identificada pela solução deverá possuir as seguintes informações:

2.1.13.35.1. Descrição;

2.1.13.35.2. IOCs;

2.1.13.35.3. Detalhes do Impacto no ambiente;

2.1.13.35.4. Prevalência Global;

2.1.13.35.5. Endpoints afetados.

2.1.13.35.6. Comportamento da ameaça.

2.1.13.36. Deve ser capaz de identificar em cada campanha de ameaça as técnicas utilizadas, relacionadas e mapeadas ao MITRE Framework.

2.1.13.37. Ter a capacidade de gerar registros/logs para auditoria;

2.1.13.38. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

2.2. Serviço de implementação e transferência de conhecimento

2.2.1. Implementação

2.2.1.1. Para a execução dos serviços de instalação e configuração, a CONTRATADA deverá disponibilizar profissionais devidamente habilitados pelo fabricante.

2.2.1.2. A instalação, atualização ou migração dos softwares poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

2.2.1.3. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

2.2.1.4. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por analistas da CONTRATANTE;

2.2.2. Transferência de conhecimento

2.2.2.1. Deverá ser fornecida transferência de conhecimento para todas as soluções ofertadas.

2.2.2.2. Para cada solução, a CONTRATADA deverá fornecer transferência de conhecimento com carga horária mínima de 20 (vinte) horas, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização das soluções contratadas;

2.2.2.3. Para cada solução, a transferência de conhecimento deve ser fornecida para uma turma de no máximo 10 alunos.

2.2.2.4. As transferências de conhecimento deverão ser realizadas em dias úteis, em horário comercial, de forma remota e/ou presencial;
2.2.2.5. As transferências de conhecimento deverão ser ministradas preferencialmente em língua portuguesa, podendo ser em idioma estrangeiro (inglês);
2.2.2.6. Deverá ser disponibilizado material didático impresso e/ou em mídia, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);
2.2.2.7. Deverá ser emitido certificado de participação ao final do curso a cada participante;
2.2.2.8. O cronograma efetivo das transferências de conhecimento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato;
2.2.2.9. Caso a transferência de conhecimento fornecida não seja satisfatória, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-las novamente, sem ônus adicional a CONTRATANTE.

3. Subcontratação:

3.1 Não será admitida a subcontratação total ou parcial do objeto do contrato.

4. Condições de Entrega:

4.1 Prazo de Entrega: 30 (trinta) dias após a colocação do pedido pela CONTRATANTE.

4.2 Impostos e Frete: Inclusos.

4.3 Por ocasião da entrega das licenças, caso seja detectado que eles não atendem às especificações contratadas, a CONTRATANTE poderá rejeitá-las, integralmente ou em parte, obrigando-se a contratada a providenciar a substituição das licenças e/ou equipamentos não aceitos no prazo de até 5 (cinco) dias úteis.

5. Informações de Faturamento:

CNPJ de faturamento: 42.318.949/0013-18
Endereço de faturamento: SEPN - Setor de Edifícios de Utilidade Norte - Quadra 508 Conjunto "C" Lote 07
Bairro: Asa Norte CEP: 70740-543
Inscrição Estadual: 07.322.007/002-03

6. Condições de Instalação, Implementação e/ou Customização:

6.1 A CONTRATADA deverá implementar as soluções contratadas no ambiente da CONTRATANTE no período de até 60 (sessenta) dias após a entrega.

7. Condições de Aceite:

7.1 O aceite, por parte da CONTRATANTE, será concedido a partir de validação e homologação dos produtos/serviços contratados, após certificado o bom funcionamento das soluções instaladas no ambiente da CONTRATANTE.

8. Condições de Garantia e Assistência Técnica, Manutenção e Suporte Técnico:

8.1 A garantia de atualização, manutenção e serviços de suporte técnico será atrelada ao tempo de contrato, considerando período de 36 (trinta e seis) meses e deverá compreender eventuais correções de falhas de funcionamento do software e/ou equipamentos, independente de correções tornadas públicas, desde que tenham sido detectadas e formalmente informadas à CONTRATADA.

8.2 A CONTRATADA concederá ao CONTRATANTE garantia integral, com prazo de 36 (trinta e seis) meses, a contar da data da INSTALAÇÃO, contra qualquer defeito de fabricação que o material/bem/equipamento venha a apresentar, incluindo avarias no transporte até o(s) local(is) de entrega, mesmo após ocorrida sua aceitação/aprovação pelo CONTRATANTE.

8.2.1 A garantia técnica compreende manutenção, atualização e suporte técnico e todas as demais condições detalhadas no Documento nº 1 deste Contrato.

8.2.2 A garantia inclui a substituição do material defeituoso no prazo máximo de 5 (cinco) dias, a contar da comunicação do fato, sem qualquer ônus para a BBTS. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas.

8.2.3 Fica a CONTRATADA desobrigada de qualquer garantia sobre o material quando se constatar que o defeito decorre de mau uso dos mesmos ou negligência de prepostos do CONTRATANTE.

9. Condições de Garantia Técnica

9.1 A garantia técnica por período de até 36 (trinta e seis) meses, contada a partir da entrega da solução, compreende manutenção, atualização e garantia, que consiste em:

9.1.1 Evolução/upgrade do produto, repassando a BBTS toda e qualquer atualização, releases, fix packs, melhoria ou correção introduzida nos produtos que componham a solução, bem como a catalogação de novas versões (releases), que contenham, além de outras, as funções dos produtos em questão;
9.1.2 Manutenção da solução, assim entendida a correção de erros de funcionamento ou desempenho inconsistente com as especificações técnicas dos produtos;
9.1.3 Atuar na resolução de problemas de atualização da solução, upgrade, salvamento e restauração;
9.1.4 Fornecimento de toda e qualquer informação relativa ao funcionamento da solução, dirimindo as dúvidas ou problemas operacionais na sua utilização;
9.1.5 Assegurar a total disponibilidade e manter a solução em perfeitas condições de uso.

9.2 Em caso de alteração de versão de quaisquer softwares fornecidos na solução integrada que implique em deformação ou inabilitação das funcionalidades, o FORNECEDOR executará as alterações necessárias ao atendimento de todos os requisitos descritos neste documento, sem qualquer custo adicional para a BBTS.
9.3 A BBTS se reserva no direito de efetuar conexão da Solução a produtos de outros fornecedores, desde que tal iniciativa não implique incompatibilidade com a solução. A efetivação de tal medida não poderá, sob qualquer hipótese, servir como justificativa para desobrigação da prestação da garantia técnica;
9.4 O FORNECEDOR deverá prestar os serviços descritos para a totalidade de produtos e condições relacionados nesta especificação técnica.
9.5 O FORNECEDOR ficará desobrigado do cumprimento das metas de atendimento enquanto a prestação de serviços estiver prejudicada em função de impedimento ou retardo decorrente de responsabilidade comprovada da BBTS;
9.6 O FORNECEDOR deverá fornecer quaisquer atualizações e/ou correções de software em até 48 (quarenta e oito) horas após sua disponibilidade no mercado;
9.7 O FORNECEDOR deverá prover acesso ao ambiente de disseminação de conhecimento e atualização da solução, de preferência via internet, à equipe técnica da BBTS designada para essa atividade;
9.8 O FORNECEDOR deverá prestar serviços de atualização e suporte técnico, via e-mail, página WEB e serviço telefônico em território nacional, em horário de 24x7 (24 horas por 7 dias da semana) durante o período de vigência da garantia técnica;

9.9 Canais de Atendimento:
9.9.1 Deverá ser disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana através de site na Internet, canal telefônico em território nacional e e-mail;
9.9.2 O FORNECEDOR deverá possuir e informar, no momento da assinatura do contrato, página da Internet onde estejam disponíveis atualizações e instaladores da solução, manuais e demais informações técnicas dos softwares, sem restrições de acesso às pessoas autorizadas pela BBTS;
9.9.3 Os chamados de suporte técnico terão a seguinte classificação quanto à prioridade de atendimento:
9.9.4 Urgente: Indica total impossibilidade de uso do sistema ou falha em alguma funcionalidade crítica que impossibilite o uso da solução e/ou infecção generalizada:
9.9.4.1 Neste caso, o atendimento inicial por parte do FORNECEDOR deverá ocorrer no máximo 2 (duas) horas a partir do registro do chamado;
9.9.4.2 Após iniciado o atendimento a um chamado com Prioridade Urgente, o FORNECEDOR deverá prover tratamento ininterrupto do problema até o restabelecimento do serviço afetado;
9.9.4.3 Caso o problema não possa ser resolvido remotamente, o FORNECEDOR deverá colocar imediatamente à disposição da BBTS, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será do FORNECEDOR;
9.9.4.4 O atendimento de Prioridade Urgente não poderá ser interrompido até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;
9.9.4.5 O prazo máximo para resolução de problemas de prioridade urgente será de 12 horas contadas após registro do chamado.
9.9.5 Alta: Indica que a solução pode ser usada, porém com restrições severas nas operações e/ou fornecimento de informações que afetem seu funcionamento:

9.9.5.1 Neste caso, o atendimento inicial por parte do FORNECEDOR deverá ocorrer no máximo 12 (doze) horas a partir do registro do chamado;
9.9.5.2 Caso o problema não possa ser resolvido remotamente, o FORNECEDOR deverá colocar imediatamente à disposição da BBTS, um especialista devidamente habilitado e credenciado para a solução do problema, sendo que o ônus financeiro de tal providência será do FORNECEDOR;
9.9.5.3 O atendimento de Prioridade Alta não poderá ser interrompido até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;
9.9.5.4 O prazo máximo para resolução de problemas de prioridade alta será de 24 horas contadas após registro do chamado.
9.9.6 Médio: Problemas críticos que não afetem o funcionamento da solução, Atendimento de Dúvidas e Pedidos de Informações:
9.9.6.1 Neste caso, o atendimento inicial por parte do FORNECEDOR deverá ocorrer no máximo 24 (vinte e quatro) horas a partir do registro do chamado.
9.9.7 Baixo: Problemas não críticos que não afetem o funcionamento da solução, Atendimento de Dúvidas e Pedidos de Informações:
9.9.7.1 Neste caso, o atendimento inicial por parte do FORNECEDOR deverá ocorrer no máximo 48 (quarenta e oito) horas a partir do registro.

10. DA INSTALAÇÃO DOS BENS/MATERIAIS

10.1 A instalação inclui as seguintes atividades:
10.1.1 Plano de execução da instalação;
10.1.2 Instalação da solução;
10.1.3 Implementação da solução;
10.1.4 Teste da solução.
10.2 A CONTRATADA deverá apresentar ao CONTRATANTE, em até 7 (sete) dias corridos, prorrogáveis por igual período, após o aceite de entrega da solução, um plano contemplando as atividades para execução da instalação, implementação e testes da solução. O plano deverá ser validado em até 7 (sete) dias corridos, prorrogáveis por igual período, a partir da entrega, pelo CONTRATANTE.
10.3 O documento deverá conter cronograma, requisitos técnicos, ações a serem executados e todas as demais informações relevantes à instalação, implementação e testes nos ambientes de produção.
10.4 O CONTRATANTE poderá alterar o cronograma e o planejamento das atividades, caso julgue necessário e de comum acordo com a CONTRATADA.
10.5 As atividades de instalação, implementação e testes da solução deverão ser realizadas pela CONTRATADA no prazo de 90 (noventa) dias.

11. Homologação:

11.1 Deverão ser apresentados, junto da proposta comercial, Cadernos Técnicos apontando o atendimento a todos os itens especificados. A BBTS poderá, caso entenda necessário, exigir teste de bancada para as soluções apresentadas.

12. Condições de Pagamento:

12.1 O pagamento será creditado, em parcela única após a entrega, implantação e aceite das licenças, em conta corrente mantida preferencialmente no Banco do Brasil S.A., em nome da CONTRATADA, em 30 dias corridos, a contar da emissão da Nota fiscal, acompanhada do Documento Auxiliar da Nota Fiscal Eletrônica, relativo aos municípios em que o documento é exigido.

12.2 A nota fiscal deverá ser entregue à CONTRATANTE, em até 5 (cinco) dias úteis subsequentes a data de sua emissão, sendo entregue até o dia 21 (vinte e um) do mês de sua emissão, acompanhada do Documento Auxiliar da Nota Fiscal Eletrônica, relativo a prestação de serviços nos municípios em que o documento é exigido.

13. Multa:

13.1 Para efeito de aplicação de multas referentes ao descumprimento de obrigações contratuais, às infrações serão atribuídos graus, conforme as tabelas 1 e 2 a seguir:

TABELA 1	
GRAU	CORRESPONDÊNCIA
1	1,0% sobre o valor contratado
2	2,0% sobre o valor contratado

TABELA 2		
ITEM	DESCRIÇÃO DA OCORRÊNCIA	GRAU
1	Execução de serviços de forma incorreta, em desconformidade com as normas técnicas pertinentes, com padrão de qualidade inferior ou em prazos superiores à média de mercado, embasados em clara deficiência técnica do(s) profissional(is) envolvido(s) ou por falta de equipamento ou ferramenta adequados, por ocorrência, cumulativamente não superior a 10%.	2
2	Manter funcionário sem qualificação para a execução dos serviços; por ocorrência, cumulativamente não superior a 10%.	1
3	Executar serviço incompleto ou de caráter paliativo, ou deixar de providenciar recomposição complementar; por ocorrência, cumulativamente não superior a 10%.	1
4	Deixar de disponibilizar equipamentos, ferramentas ou aparelhos necessários à realização dos serviços do escopo do contrato; por ocorrência, cumulativamente não superior a 5%.	1
5	Deixar de repor ferramentas/equipamentos desgastados, avariados ou inoperantes que sejam de sua responsabilidade; por ocorrência, cumulativamente não superior a 5%.	1
6	Deixar de cumprir a programação periódica de manutenção preventiva; por item, por ocorrência, cumulativamente não superior a 10%.	1

14. Acordo de Nível de Serviço:

14.1 O FORNECEDOR estará sujeito a multa pelo descumprimento do prazo máximo para resolução de problemas durante o período da garantia, aplicados sobre o valor total da solução acionada no momento do descumprimento, por hora ou fração de hora de atraso, de acordo com os níveis de criticidade e os percentuais abaixo, limitado a 5% do valor total do contrato, conforme Sanções Administrativas previstas no Contrato.

PRIORIDADE	PRAZO MÁXIMO PARA RESOLUÇÃO DE PROBLEMSAS	EVENTO DE QUEBRA DA META (HORA OU FRAÇÃO)	PERSISTÊNCIA DE QUEBRA (HORA OU FRAÇÃO)
Urgente	12 (doze) horas	0,05%	0,025%
Alta	24 (vinte quatro) horas	0,03%	0,015%

14.2 Os percentuais a que se referem o item anterior serão apurados mensalmente e poderão ensejar a aplicação de multa no decorrer da vigência da garantia prestada pelo FORNECEDOR. Nenhuma sanção será aplicada sem o devido processo, assegurada a ampla defesa.

15. Aspectos de Segurança:

15.1 O acesso ao ambiente da CONTRATANTE, só serão realizados com acompanhamento do funcionário da BBTS e mediante assinatura de um termo de sigilo.

16. Vigência:

16.1 O contrato terá vigência de 36 (trinta e seis) meses, podendo ser prorrogado até o limite de 60 (sessenta) meses.

17. Repactuação de preços:

17.1 O valor será fixo e irreajustável durante toda a vigência do contrato.

18. Matriz de risco:

CATEGORIA DO RISCO	DESCRIÇÃO	CONSEQUÊNCIA	ALOCAÇÃO DO RISCO
Risco atinente ao Tempo da Execução	Atraso na execução do objeto contratual por culpa do Contratado.	Aumento do custo do produto e/ou do serviço.	Contratada
	Fatos retardadores ou impeditivos da execução do contrato próprios do risco ordinário da atividade empresarial ou da execução.	Aumento do custo do produto e/ou do serviço.	Contratada
	Fatos retardadores ou impeditivos da execução do contrato que não estejam na sua álea ordinária, tais como fatos do príncipe.	Aumento do custo do produto e/ou do serviço.	Contratante
Risco da Atividade Empresarial	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária.	Aumento ou diminuição do lucro do Contratado.	Contratada
	Variação da taxa de câmbio.	Aumento ou diminuição do custo do produto e/ou do serviço.	Contratada
	Violação de dados pessoais de TERCEIROS identificados e identificáveis por falha de segurança técnica e administrativa.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada
	Violação de dados pessoais de terceiros identificados e identificáveis por descumprimento das orientações do Contratante.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada
	Violação de dados pessoais de terceiros identificados e identificáveis por descumprimento das normas de proteção de dados.	Sujeito às penalidades contratuais por infringência à Lei Geral de Proteção de Dados.	Contratada
	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra.	Aumento do custo do produto e/ou do serviço.	Contratante

Risco Tributário e Fiscal (Não Tributário)	Responsabilização da CONTRATANTE por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa da CONTRATANTE.	Débito ou crédito tributário ou fiscal (não tributário).	Contratada

19. Qualificação Econômico-Financeira:

19.1 A qualificação econômico-financeira da CONTRATADA será avaliada de acordo com os seguintes critérios:

19.1.1 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da legislação em vigor, acompanhado do demonstrativo das contas de lucros e prejuízos que comprovem sua boa situação financeira.

19.1.1.1 No caso de Microempresa ou Empresa de Pequeno Porte, a apresentação dessa documentação servirá também para comprovação de enquadramento nessa condição, de acordo com o art. 3º da Lei Complementar nº 123, de 14.12.2006.

19.1.1.2 No caso de empresa constituída no exercício social vigente, será admitida a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

19.1.2 A comprovação da boa situação financeira da CONTRATADA será baseada também na obtenção de Índices de Liquidez Geral (LG), de Solvência Geral (SG) e de Liquidez Corrente (LC) resultantes da aplicação das fórmulas abaixo, sendo considerada habilitada a empresa que apresentar resultado maior que 1, em todos os índices aqui mencionados:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

19.1.3 Se a CONTRATADA apresentar qualquer dos índices relativos à boa situação financeira igual ou menor que 1,00 (um) deverá comprovar possuir patrimônio líquido igual ou superior a 10% do valor estimado da contratação, por meio da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, apresentados na forma da lei, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrados há mais de 3 (três) meses da data da apresentação da proposta.

20. Qualificação Técnica:

20.1 A qualificação técnica da CONTRATADA será avaliada de acordo com os seguintes critérios:

20.1.1 No mínimo 01(um) atestado de capacidade técnica comprovando fornecimento compatível em características, quantidades e prazos ao indicado no projeto básico.

20.1.1.1 O atestado deverá indicar o fornecimento de um quantitativo de bens não inferior a 50% do especificado no item 1 OBJETO.

20.1.2 A CONTRATADA deve disponibilizar, se solicitadas, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia simples do contrato que deu suporte à contratação, cópia das notas fiscais, endereço atual da CONTRATANTE e local em que foram prestados os serviços.

21. *Due Diligence*:

21.1 Considerando que a BB TECNOLOGIA E SERVIÇOS S.A. implementou a gestão de risco de fornecedores por meio de Due Diligence, e que a referida ferramenta permite aumentar a segurança nas contratações e na gestão, fica a CONTRATADA, ciente de que, a critério da BB Tecnologia e Serviços, deverá preencher, assinar e encaminhar o FQ415-042- Questionário de Due Diligence (Anexo IX) com as devidas evidências, no prazo máximo de 03 (três) dias úteis, contados da solicitação do envio, observando que a entrega do questionário e suas evidências respondido é fato determinante para a assinatura do contrato.

22. Garantia Financeira da Execução Contratual:

22.1 Será exigida garantia de 5% (cinco por cento) sobre o valor contratado, nos termos do artigo 70 da Lei nº 13.303/16.

22.2 A garantia deverá ser válida durante todo o período de vigência do contrato.

DOCUMENTO Nº 2 DO CONTRATO

DEMONSTRATIVO DO ORÇAMENTO DE CUSTOS/PROPOSTA

Item	Descrição	QTD.	PREÇO UNITÁRIO	PREÇO TOTAL
01	Aquisição de licença perpétua de solução EDR, para upgrade da solução McAfee antivírus, garantia de 36 meses. PN: MV6ECE	6.000	R$ 188,33	R$ 1.129.980,00
Valor Total				R$ 1.129.980,00

1. OBJETO:

1.1. Apresentamos nossa Carta-Proposta para prestação dos serviços de 6.000 licenças perpétuas, para upgrade da solução McAfee e garantia de 36 meses, conforme discriminado no ANEXO I do Edital que integra o instrumento convocatório da licitação em epígrafe. Aquisição de licença perpétua de solução EDR, para upgrade da solução McAfee antivírus, garantia de 36 meses. PN: MV6ECE.

2. PREÇO DO SERVIÇO

2.1. Pela prestação dos serviços, cobraremos, a importância total estimada de

R$ 1.129.980,00 (Um milhão, cento e vinte e nove mil, novecentos e oitenta reais) para 6.000 licenças perpétuas para upgrade da solução McAfee e garantia de 36 meses, sendo o valor unitário de R$ 188,33 (cento e oitenta e oito reais a trinta e três centavos).

2.2. O preço proposto contempla todas as despesas necessárias à plena execução do serviço, tais como de pessoal, de administração e todos os encargos (obrigações sociais, impostos, taxas etc.) incidentes sobre o serviço.

2.3. Desde já nos declaramos cientes de que a BB Tecnologia e Serviços S.A. procederá à retenção de impostos nas hipóteses previstas em lei.

3. CONDIÇÕES GERAIS

3.1. Declaramos conhecer os termos do instrumento convocatório que rege a presente licitação bem como seus anexos, incluindo a Minuta de Contrato.

3.2. Declaramos, sob as penas da lei, que não nos enquadramos nas situações previstas no item 3.6 do Edital.

3.3. O INTERESSADO declara, sob as penas da lei, que não possui em seu quadro societário empregado da BB Tecnologia e Serviços S.A., ainda que em gozo de licença não remunerada, ou membro da Administração dessa Instituição, mesmo subcontratado.

3.4. Não se Aplica na condição de ME, EPP.

3.5. As relações empregador/empregado, concernentes ao controle de frequência, disciplina, folha de pagamento e demais obrigações de Lei serão sempre de inteira e exclusiva responsabilidade desta empresa.

3.6. Quaisquer reclamações oriundas da prestação dos serviços deverão ser formalizadas por escrito e dirigidas ao nosso escritório, sito na rua SGAN 607, conjunto A, bloco A, sala 312.Asa Norte, Brasília – DF.

3.7. Preposto administrativo: Waldo Baptista Gomes
Cargo: Diretor de Marketing e Relacionamento
E-mail: waldo@netsafecorp.com.br
Tel.: (11) 98181-3786

Suite de produtos McAfee Protect Plus EDR - MV6

GERENCIAMENTO

McAfee MVISION ePO (SaaS)

McAfee ePolicy Orchestrator (ePO) for deployment on-premises or in Amazon Web Services (AWS)

McAfee Threat Intelligence Exchange (TIE)

McAfee Data Exchange Layer (DXL).

FUNCIONALIDADES INCLUSAS

MVISION EDR with guided investigations

McAfee Endpoint Security (ENS) for Windows

McAfee Adaptive Threat Protection (ATP) – requires ENS for Windows

McAfee Endpoint Security (ENS) for macOS

McAfee Endpoint Security (ENS) for Linux

McAfee MVISION Endpoint

McAfee MVISION Mobile (for Android & iOS)

McAfee Device Control

Command Line Scanner

McAfee Application Control for PCs

MVISION Insights for profiling "Top Attacks" with guidance to improve protection

Access to deploy McAfee Strategic Innovation Alliance (SIA) partner products.

INDICAÇÃO DOS SIGNATÁRIOS:

CONTRATANTE: BB TECNOLOGIA E SERVIÇOS S.A.

Nome: Sérgio Gonzaga Wenceslau
Cargo: Gerente de Divisão
CPF: [redacted]

Nome: Isaac Nicholas Siqueira Viana
Cargo: Gerente Executivo
CPF: [redacted]

CONTRATADA: NETSAFE CORP LTDA

Nome: Waldo Baptista Gomes
Cargo: Diretor de Marketing e Relacionamento
CPF: [redacted]

DOCUMENTO Nº 3 DO CONTRATO

TERMO DE HOMOLOGAÇÃO E ACEITE DOS SERVIÇOS CONTRATADOS

Por intermédio deste termo de homologação e aceite, a **CONTRATANTE** confirma o recebimento dos serviços contratados através do **Contrato de Prestação de Serviços,** firmado pelas partes em XXXXXXXXXXXX, que, foram verificados e testados quanto a sua conformidade perante à **CONTRATADA** e, dá nesta data, seu aceite e recebimento sem perda do direito da garantia e outras faculdades previstas no Contrato.

Brasília, _____/_____de 200_

CONTRATANTE **CONTRATADA**

*DOCU*MENTO Nº 4 DO CONTRATO

QUESTIONÁRIO DE DUE DILIGENCE (FQ415-042)

. Informações Cadastrais

1.1. Razão social:
1.2. Nome fantasia:
1.3. CNPJ:
1.4. Endereço:
1.5. CEP:
1.6. E-mail:
1.7. Website:
1.8. Telefone:
1.8.1 Telefone 1:
1.8.2 Telefone 2:
1.8.3 Telefone Celular:

1.9. Porte da Empresa:
☐ Microempresa – Faturamento menor ou igual a R$ 360 mil.
☐ Pequena empresa – Faturamento maior que R$ 360 mil e menor ou igual a R$ 4,8 milhões.
☐ Média empresa – Faturamento maior que R$ 4,8 milhões e menor ou igual a R$ 300 milhões.
☐ Grande empresa – Faturamento maior que R$ 300 milhões.

1.10. Ramo principal de atividade da empresa:
☐ Comercial
☐ Industrial
☐ Prestação de Serviço

1.11. Informar número de Empregados:

2. Eixo Gestão

2.1. A empresa possui Código de Ética, Guia de Conduta ou documentos correlatos que descrevem as condutas éticas que devam ser observadas pelos integrantes da Alta Administração, empregados próprios e/ou terceirizados?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

2.2. A empresa possui alguma política formal ou programa de responsabilidade empresarial que inclua aspectos ambientais, sociais e de saúde e segurança do colaborador?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

2.3. A empresa divulga publicamente relatório anual sobre sua atuação referente aos eixos financeiros, ambientais e sociais?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

2.4. Qual o faturamento da empresa nos últimos 3 anos?
2018:_____ 2019:_____ 2020: _____

2.5. A empresa possui algum certificado do sistema gestão? (ISO 9.001, 14.001, 16.001, 27.001, 37.001, OHSAS 18.001, entre outros)?

☐ Sim ☐ Não

Nota – Requer a apresentação de evidência (s).

2.6. A empresa promove ações de capacitação do público interno em questões relacionadas a gestão ambiental, diversidade, assédio, direitos humanos, anticorrupção, etc.?

☐ Sim ☐ Não

Nota – Requer a apresentação de evidência (s).

3. Eixo Social (Direitos Humanos)

3.1. A empresa possui compromisso formal com os Direitos Humanos?

☐ Sim ☐ Não

Nota 1 - Considerar compromissos relacionados: à erradicação do trabalho infantil, erradicação do trabalho forçado ou compulsório, combate à prática de discriminação em todas suas formas, prevenção do assédio moral e do sexual, valorização da diversidade, respeito à livre associação sindical e direito à negociação coletiva.
Nota 2: Requer apresentação de evidência (s).

3.2. A sua empresa responde ou respondeu, nos últimos 3 anos, processo judicial ou administrativo decorrente de práticas envolvendo trabalho forçado ou compulsório e/ou trabalho infantil, em suas próprias operações ou em sua cadeia de suprimentos?

☐ Sim ☐ Não

Nota: Se positivo, apresentar evidência (s) com o número do processo e instância.

3.3. A sua empresa responde ou respondeu, nos últimos 3 anos, processo judicial ou administrativo decorrente de práticas envolvendo assédio moral ou sexual e/ou discriminação em suas próprias operações ou em sua cadeia de suprimentos?

☐ Sim ☐ Não

Nota: Se positivo, apresentar evidência (s) com o número do processo e instância.

3.4. A sua empresa promove o engajamento do público interno, incluindo trabalhadores terceirizados, no combate a qualquer prática de discriminação em matéria de emprego e ocupação?

☐ Sim ☐ Não

Nota - Se positivo, apresentar evidência (s). Considerar iniciativas ou procedimentos relacionados: à seleção e contratação, promoção, acesso a treinamento, sensibilização dos funcionários diretos e trabalhadores terceirizados para o tema.

3.5. A empresa avalia a satisfação dos funcionários e implementa ações de melhoria contínua?

☐ Sim ☐ Não

Nota 1 - Em caso de resposta positiva, considerar que pelo menos um dos temas seguintes são atendidos: Clima organizacional (exposição a estresse, ambiente harmônico, cooperação entre funcionários, etc.); Carga de trabalho (horas trabalhadas, metas de produção e outros tipos de demandas); Remuneração compatível com a carga de trabalho; Benefícios.
Nota 2 - Requer apresentação de evidência (s).

3.6. A empresa tem políticas de melhoria da qualidade de vida dos funcionários?

☐ Sim ☐ Não

Nota 1 - Em caso de resposta positiva, considerar que pelo menos um dos temas seguintes são atendidos: Incentiva ações para a alimentação saudável, academia, ginástica laboral e outras atividades que promovam o bem estar e uma vida mais saudável (física e psíquica); Conscientiza, informa e estimula seus funcionários quanto a um estilo de vida saudável; Acompanha a situação de seus funcionários quanto a aspectos relacionados à sua qualidade de vida e estrutura programas que incentivem progressos em relação ao tema; Possui programas que incentivem a redução de horas-extras e equilíbrio entre carga horária disponível e demanda de trabalho.
Nota 2 - Requer apresentação de evidência (s).

3.7. A empresa busca, por meio de práticas cotidianas, construir um relacionamento com a comunidade local visando seu desenvolvimento?

☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

3.8. A empresa tem política de diversidade publicamente disponível que inclua fatores de diversidade como gênero, cor, etnia, orientação sexual, país de origem ou nacionalidade?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

3.9. Nos quadros da empresa tem mulheres ocupando cargo de gerência e/ou diretoria?
☐ Sim. Quantas? _____ ☐ Não

3.10. Nos quadros da empresa tem negros ocupando cargo de gerência e/ou diretoria?
☐ Sim. Quantos? _____ ☐ Não

3.11. Na empresa existe diferença na remuneração entre pessoas de gêneros diferentes ocupantes de cargos de gerência e/ou diretoria?
☐ Sim. Percentual médio da diferença_____ ☐ Não

3.12. Na empresa, as funcionárias que retornam de licença-maternidade permanecem por no mínimo 12 meses após o retorno?
☐ Sim ☐ Não.

3.13. Nos quadros da empresa tem pessoas com deficiência (PcD)?
☐ Sim. Quantas? ___ ☐ Não

3.14. A empresa adota medidas visando promover a empregabilidade de pessoas com deficiência(PcD)?
☐ Sim ☐ Não

Nota 1 - Considerar uma ou mais das seguintes medidas: investimento em meios de acessibilidade; investimento em tecnologias adequadas para a realização do trabalho; capacitação profissional; sensibilização e conscientização de seus funcionários para a recepção e boa convivência profissional.
Nota 2 - Se positivo, requer a apresentação de evidência (s).

3.15. A empresa disponibiliza plano de saúde para os funcionários?
☐ Sim ☐ Não

3.16. Qual o tempo médio de trabalho dos funcionários da empresa?
☐ De 1 a 5 anos
☐ De 5 a 10 anos
☐ Acima 10 anos

4. Eixo Ambiental

4.1. O monitoramento e a mitigação dos riscos socioambientais fazem parte da estratégia da empresa?
☐ Sim ☐ Não

4.2. A alta direção patrocina/acompanha as ações/estratégias ambientais?
☐ Sim ☐ Não

4.3. A empresa possui licença (s) ambiental (is) para o funcionamento? (Licença de Operação - LO ou equivalente)?
☐ Sim ☐ Não ☐ Não se aplica

Nota 1 - Caso seja aplicado à atividade da empresa a necessidade da licença ambiental.
Nota 2 – Requer a apresentação de evidência (s).

4.4. A empresa possui passivos ambientais?
☐ Sim ☐ Não

4.5. A empresa foi autuada, multada ou notificada nos últimos 10 anos por motivo de crime ou descumprimento da legislação ambiental?
☐ Sim ☐ Não

Nota 2: Se positiva apresentar evidência com o número do processo e órgão para verificação.

4.6. A empresa possui procedimentos estruturados para logística reversa, em conformidade com a Lei nº 12.305/2010?
☐ Sim ☐ Não ☐ Não se aplica

4.7. A empresa possui programa de Coleta seletiva implementado?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

4.8. A empresa emite relatório de emissão de GEE (Gases do efeito estufa) relacionados a sua atividade?
☐ Sim ☐ Não ☐ Não se aplica

Nota - Requer a apresentação de evidência (s).

4.9. A empresa possui política ambiental para redução da emissão de GEE (Gases do efeito estufa)?
☐ Sim ☐ Não ☐ Não se aplica

Nota - Requer a apresentação de evidência (s).

4.10 A empresa tem conhecimento da procedência dos insumos utilizados no seu processo produtivo e/ou prestação de serviço?
☐ Sim ☐ Não

4.11 A empresa possui programa de geração distribuída ou faz uso de outra matriz energética além da convencional?
☐ Sim Qual?_____ ☐ Não

4.12 A empresa possui ações/metas para redução do consumo de energia elétrica e água?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

5. Eixo Integridade

5.1. Nome, cargo e percentual de participação (quando aplicável) de seus proprietários, sócios controladores, conselheiros e diretores:

Nome	CPF	Cargo	% Participação (quando aplicável)

5.1.1 Percentual de participação societária da sua empresa em outras pessoas jurídicas na condição de controladora, controlada, coligada ou consorciada, bem como a razão social e o CNPJ das mesmas.

☐ Não se aplica

Razão Social	CNPJ	% Participação	Relacionamento Societário

5.2. A empresa ou sociedades controladoras, controladas, coligadas ou consorciadas estão localizadas ou realizam operações comerciais e financeiras nos seguintes locais:

Angola, Argentina, Bolívia, China, Colômbia, Gabão, México, Nigéria, Paraguai, Tanzânia, Venezuela, Ilhas Cayman, Cingapura, Mônaco, Panamá, Ilhas Virgens Britânicas, Nicarágua.

☐ Sim ☐ Não

5.3. A sua empresa é membro de alguma iniciativa nacional ou internacional de combate à corrupção?
☐ Sim. Qual? _____ ☐ Não

5.4. Algum integrante da Alta Administração[1] ou seus familiares[2] (até terceiro grau) ocupa ou é candidato a cargo eletivo ou cargo de confiança na administração pública?
☐ Sim ☐ Não

5.4.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Grau de Parentesco	Nome do Órgão/Entidade	Cargo	Período

[1] Ocupantes de cargo ou membros de colegiados posicionados hierarquicamente acima da linha gerencial média. Ex.: Membros do Conselho de Administração e da Diretoria Executiva, Sócios, Presidente, Vice-presidente, Diretor e/ou Gerente Executivo.
[2] Primeiro grau: pai, mãe e filhos; Segundo grau: irmãos, avós e netos; Terceiro grau: tios, sobrinhos, bisavós e bisnetos

5.5. Algum integrante da Alta Administração ou seus familiares (até terceiro grau) mantém negócios pessoais ou relacionamento próximo com algum agente público?
☐ Sim ☐ Não

5.5.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Nome do Órgão/Entidade	Cargo	Grau de Parentesco	Nome do empregado ou membro	Cargo do empregado ou membro

5.6. Algum integrante da Alta Administração é familiar (até terceiro grau) de algum empregado da BB Tecnologia e Serviços que ocupe função gerencial ou de algum membro da Diretoria Executiva ou Conselho de Administração da BBTS ou de funcionário que trabalhe diretamente com o processo de compra e contratação da BBTS?

☐ Sim ☐ Não

5.6.1. Em caso afirmativo, forneça os detalhes abaixo:

Nome	Grau de Parentesco	Nome do empregado ou membro	Cargo do empregado ou membro

5.7. A sua empresa possui regras específicas formalizadas para visitas e demais interações com entes públicos, com foco na Prevenção e Combate à Corrupção?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.8. Algum integrante da Alta Administração da sua empresa já foi preso, acusado, investigado (mesmo que em curso), processado ou condenado por fraude ou corrupção nos últimos 10 anos?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.9. A empresa, controladoras, controladas, coligadas ou consorciadas já foram acusadas, investigadas (mesmo que em curso), processadas ou condenadas por fraude ou corrupção nos últimos 10 anos?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.10. A empresa, controladora, controlada, coligada ou consorciada já entregou, ofertou, autorizou, acordou ou prometeu qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para angariar ou manter negócios, ou mesmo obter qualquer vantagem comercial, nos últimos 10 anos?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.11. Algum integrante da Alta Administração, empregado, agente ou terceiro representando a sua empresa já entregou, ofertou, autorizou, acordou ou prometeu qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para angariar ou manter negócios, ou mesmo obter qualquer vantagem comercial, nos últimos 10 anos?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.12. A empresa, controladora, controlada, coligada ou consorciada esteve submetida à investigação ou avaliação externa relacionada à fraude e/ou corrupção por algum órgão ou agência, nacional ou internacional (CGU, TCU, TCE, CVM, SEC, PF, etc.) nos últimos 10 anos?
☐ Sim ☐ Não
Nota – Se positivo fornecer evidência (s).

5.13. A empresa conhece a legislação anticorrupção a qual está sujeita?
☐ Sim ☐ Não

5.14. A empresa possui um Programa de Integridade estruturado com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira?
☐ Sim ☐ Não
Nota 1 - Caso a resposta desta questão seja "Sim", responder às Questões 5.15 e 5.16.
Nota 2 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu website.

5.15. A empresa possui uma estrutura hierárquica definida para coordenar e implantar o programa de integridade?
☐ Sim ☐ Não

5.16. O Programa de Integridade é revisado periodicamente pela Alta Administração?
☐ Sim. Qual periodicidade? ____ ☐ Não

5.17. A empresa possui unidade específica e independente para mapear e analisar os riscos aos quais está exposta e verificar o cumprimento da legislação pelos empregados?
☐ Sim ☐ Não

5.18. A empresa possui mapeamento dos riscos de ocorrência de fraude e corrupção?
☐ Sim ☐ Não

5.19. A empresa possui medidas para evitar atos de corrupção nas situações de risco identificadas?
☐ Sim ☐ Não

5.20. A empresa possui política anticorrupção ou documento equivalente, amplamente distribuída para colaboradores, gestores, diretores e conselheiros?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.21. A empresa possui normativos internos que determinem a proibição de qualquer tipo de pagamento ou benefício a qualquer autoridade governamental nacional ou estrangeira, para obter ou manter negócios ou vantagem comercial?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.22. A empresa possui normativos internos que determinem a proibição ou restrição, quanto ao oferecimento de presentes, brindes e hospitalidade a agentes públicos, clientes e parceiros comerciais?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.23. A empresa possui normativos internos que disponham sobre doação e/ou contribuição a instituições de caridade, programas sociais ou a partidos políticos?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.24. A empresa possui normativos internos de *Due Diligence* para a avaliação da reputação, idoneidade e das práticas de combate à corrupção de terceiros, tais como: fornecedores, distribuidores, agentes, consultores, representantes comerciais e/ou parceiros operacionais?
☐ Sim ☐ Não
Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.25. A empresa conhece os documentos da BB Tecnologia e Serviços, disponibilizados no site www.bbts.com.br, relacionados a Compliance, Ética e Integridade?
☐ Sim ☐ Não

https://www.bbts.com.br/index.php/canal-do-fornecedor-etica-integridade

5.25.1. Se afirmativo, informar quais documentos disponibilizados pela BBTS (www.bbts.com.br) sua empresa tem conhecimento:
☐ Política de Relacionamento com Fornecedores
☐ Código de Ética e Normas de Conduta
☐ Política de Prevenção e Combate à Corrupção, Lavagem de Dinheiro e ao Financiamento do Terrorismo
☐ Programa de Compliance

5.26. A empresa oferece e/ou recomenda treinamentos periódicos sobre Integridade e/ou sobre os aspectos da Lei Anticorrupção?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.26.1. Se afirmativo, informar para quais públicos a empresa oferece e/ou recomenda treinamentos e fornecer evidencias:
☐ Conselheiros ☐ Diretores ☐ Colaboradores ☐ Fornecedores

5.27. A empresa oferece e/ou recomenda treinamentos periódicos sobre o seu Código de Ética, Normas de Conduta?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.27.1. Se afirmativo, informar para quais públicos a empresa oferece e/ou recomenda treinamentos e fornecer evidencias:
☐ Conselheiros ☐ Diretores ☐ Colaboradores ☐ Fornecedores

5.28. A empresa dá conhecimento e solicita aos empregados, que se relacionam com a BB Tecnologia e Serviços, que respeitem os documentos da BBTS, disponibilizados no site www.bbts.com.br, relacionados a Compliance, Ética e Integridade?
☐ Sim ☐ Não

https://www.bbts.com.br/index.php/canal-do-fornecedor-etica-integridade

5.29. A empresa possui canal de denúncias relacionado à corrupção e a outros desvios de conduta, abertos e amplamente divulgados a todos os empregados próprios e/ou terceirizados?
☐ Sim ☐ Não

Nota 1 - Caso tenha canal de denúncia, responda à Questão 5.30.
Nota 2 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.30. O canal de denúncia garante o anonimato evitando qualquer tipo de perseguição ou retaliação ao denunciante?
☐ Sim ☐ Não

5.31. A empresa possui mecanismos de investigação de indícios de fraude e/ou corrupção e procedimentos que assegurem a interrupção/correção de irregularidade ou infração detectadas e a tempestiva remediação dos danos gerados?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.32. A empresa possui normativos internos que disponham sobre o monitoramento da efetividade e da eficiência do programa de integridade anticorrupção da sua empresa?
☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.

5.33. A empresa utiliza os serviços de terceiros, tais como agentes, consultores, representantes comerciais e/ou outros tipos de intermediários, sejam pessoas físicas ou jurídicas, com o objetivo de angariar novos negócios?
☐ Sim ☐ Não

5.33.1. Se afirmativo, informar o nome e/ou razão social dos agentes, consultores, representantes comerciais e/ou outros tipos de intermediários, sejam pessoas físicas ou jurídicas

Nome/Razão Social	CPF/CNPJ

5.34. A empresa realiza avaliação prévia de requisito de integridade, para mitigar o risco de estabelecer relação de negócios com fornecedores, parceiros e demais terceiros, eventualmente envolvidos em ato de corrupção?

☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

5.35. A empresa divulga o seu programa de integridade aos seus fornecedores, distribuidores, representantes comerciais, intermediários e/ou outros tipos de parceiros de negócios?

☐ Sim ☐ Não

5.36. A empresa solicita que seus fornecedores, distribuidores, representantes comerciais, intermediários e/ou outros tipos de parceiros de negócios declarem pleno conhecimento sobre os principais aspectos do seu programa de integridade?

☐ Sim ☐ Não

Nota - Requer a apresentação de evidência (s).

5.37. Nos contratos firmados há previsão de cláusulas que obrigue a contraparte a respeitar

☐ Programa de Integridade

☐ Código de Ética/Norma de Conduta

☐ Lei 12.846/2013 – Lei Anticorrupção

Nota 1 - Requer a apresentação de evidência (s), com o fornecimento de cópia da documentação que suporte a afirmação, ou indique onde os referidos documentos podem ser encontrados no seu *website*.
Nota 2 – Pode ser marcado mais de uma alternativa

6. Declaração de veracidade das informações

6.1. Declaro e atesto para os devidos fins que este formulário foi preenchido por pessoa com poderes outorgados para representar a empresa e que as informações fornecidas acima, bem como os documentos disponibilizados são verdadeiros e não ocultaram quaisquer dados. Se em algum momento as informações ou documentos apresentados neste questionário não representarem mais a realidade, comprometemo-nos a comunicar imediatamente à BB Tecnologia e Serviços.

Local e data:

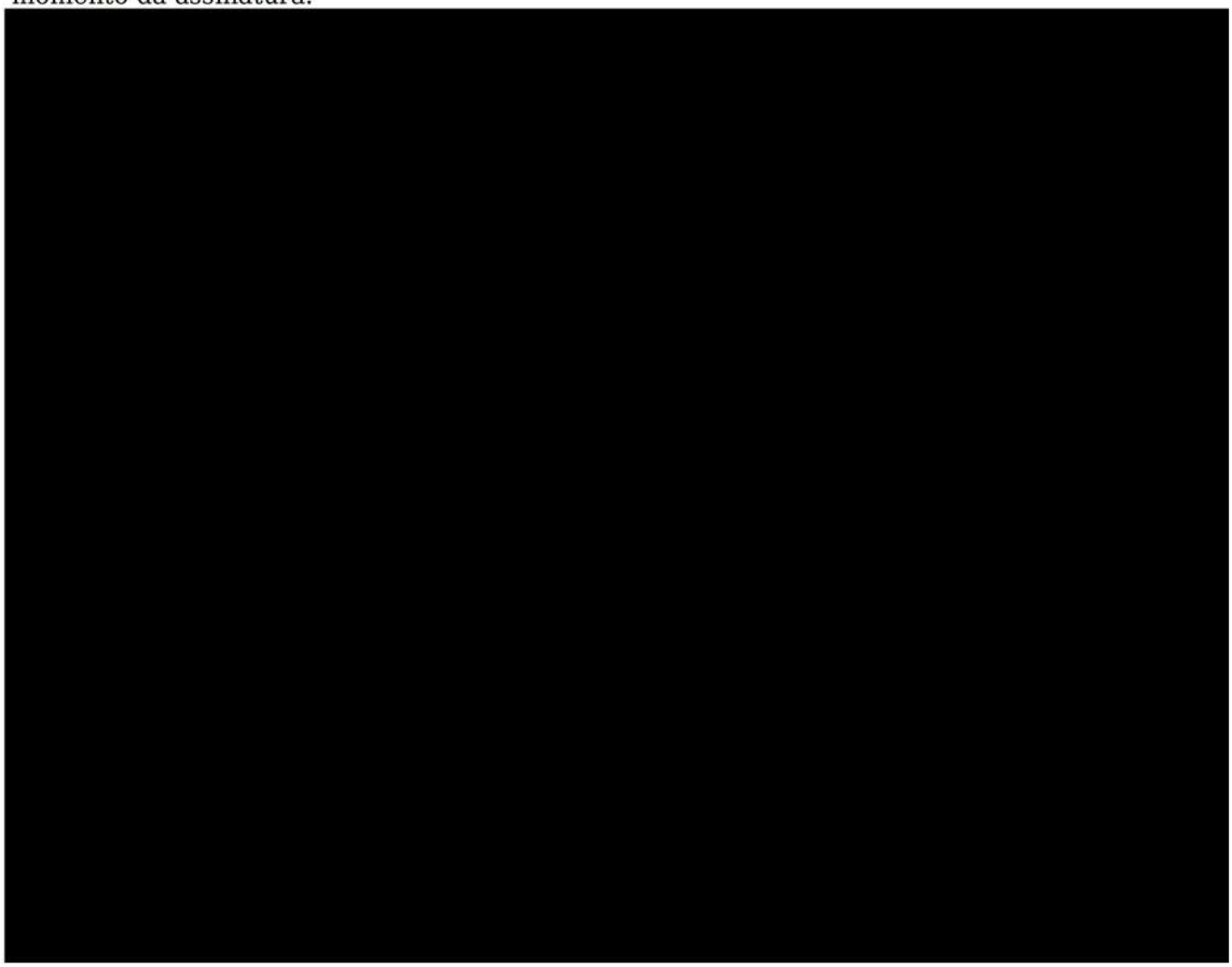
Assinatura:

Nome por extenso:

Cargo:

Signatário **Waldo Baptista Gomes** [redacted] registrou o documento abaixo no momento da assinatura:

Signatário **Waldo Baptista Gomes** [redacted] registrou o documento abaixo no momento da assinatura:



84 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 21 de julho de 2022, 11:26:14

[redacted]

CONTRATO DGCO 00185 2022 - NETSAFE pdf [redacted]

Assinaturas

Waldo Baptista Gomes [redacted]
Assinou como parte e apresentou documento com foto

PALOMA MACEDO PELLEGRINO [redacted]
Acusou recebimento

Paloma Macedo Pellegrino

Sérgio Gonzaga Wenceslau [redacted]
Assinou como parte

Isaac Nicholas Siqueira Viana [redacted]
Assinou como parte

PALOMA MACEDO PELLEGRINO [redacted]
Reconheceu

Paloma Macedo Pellegrino

Eventos do documento

20 Jul 2022, 09:41:48
Documento 943795c0-60db-4d19-8081-95b1dabd54a0 **criado** por PALOMA MACEDO PELLEGRINO (02cd307c-141a-4c54-91ec-dda1995cfdf5). Email: [redacted] - DATE_ATOM: 2022-07-20T09:41:48-03:00

20 Jul 2022, 09:48:09
Assinaturas **iniciadas** por PALOMA MACEDO PELLEGRINO (02cd307c-141a-4c54-91ec-dda1995cfdf5). Email: [redacted] DATE_ATOM: 2022-07-20T09:48:09-03:00

20 Jul 2022, 10:00:41
WALDO BAPTISTA GOMES **Assinou como parte** (76133467-cc17-4f3c-8cc2-21ca899f8cf2) - Email: [redacted]
DATE_ATOM: 2022-07-20T10:00:41-03:00

20 Jul 2022, 16:09:59
PALOMA MACEDO PELLEGRINO **Acusou recebimento** (02cd307c-141a-4c54-91ec-dda1995cfdf5) - Email:

[redacted]DATE_ATOM: 2022-07-20T16:09:59-03:00

20 Jul 2022, 17:32:50
SÉRGIO GONZAGA WENCESLAU **Assinou como parte** (751ced78-b15d-4933-88a8-f5a7284f97dd) - Email: [redacted]DATE_ATOM: 2022-07-20T17:32:50-03:00

20 Jul 2022, 19:43:28
ISAAC NICHOLAS SIQUEIRA VIANA **Assinou como parte** (21ec7a9a-fb12-4b30-b967-1b610b5de995) - Email: [redacted]DATE_ATOM: 2022-07-20T19:43:28-03:00

21 Jul 2022, 11:24:51
PALOMA MACEDO PELLEGRINO **Reconheceu** (02cd307c-141a-4c54-91ec-dda1995cfdf5) - Email: [redacted]ATE_ATOM: 2022-07-21T11:24:51-03:00

Hash do documento original
[redacted]

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign