Governo do Estado do Rio de Janeiro

Companhia Estadual de Águas e Esgotos do Rio de Janeiro

Diretoria Jurídica

CONTRATO NI NºCONTRATO 114/2022 (DAD)

CONTRATO CEDAE N.º 114/2022 (DAD)

que entre si celebram a **COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS – CEDAE** e a **NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.**

A **COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS (CEDAE)** , sociedade de economia mista, com sede nesta Cidade, na Av. Presidente Vargas, 2655, Cidade Nova, CEP 20.210-030, registrada na JUCERJA sob o n.º 5.000, em 14 de agosto de 1975, inscrita no CNPJ sob o n.º 33.352.394/0001-04, por meio de seus diretores ao final assinados, Sr. LEONARDO ELIA SOARES - Diretor-Presidente, e Sr. JULIO CESAR URDANGARIN BATISTA JUNIOR – Diretor Administrativo, doravante denominada **CEDAE**, e a **NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.**, sediada na ST SCN Quadra 05, Bloco A N, nº 50, sala 617, Edifício Brasília Shopping, Asa Norte, Brasília – DF, CEP: 70.715-900 , inscrita no CNPJ sob o n.º 09.137.728/0001-34, neste ato por meio de seu Sócia Administradora ao final assinada, Srª. PATRICIA ANGELINA DA CONCEIÇÃO, identidade nº 48.453.021-5 SSP/SP e CPF n. 346.994.838-01, têm entre si, justo e contratado o **"SERVIÇO DE PROTEÇÃO DE ESTAÇÕES DE TRABALHO E SERVIDORES COM SUBSCRIÇÃO DE LICENÇAS DE USO PARA SOLUÇÃO ANTIVÍRUS",** em conformidade com as especificações técnicas constantes do edital e da proposta da **CONTRATADA**, demais condições previstas no Edital de **Pregão Eletrônico nº 002/2021** e da **Ata de Registro de Preços nº 001/2022**, ao qual CEDAE adere na condição de carona, fazendo-o com fundamento no art. 66 da Lei 13.303/2016, no art. 21 do Regulamento Interno de Licitações e Contratos da CEDAE (RILC) e no Decreto Estadual do Rio de Janeiro n. 46.751/2019, que se regerá pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA: DO OBJETO

A presente contratação tem por objeto a "**CONTRATAÇÃO DE SERVIÇO DE PROTEÇÃO DE ESTAÇÕES DE TRABALHO E SERVIDORES COM SUBSCRIÇÃO DE LICENÇAS DE USO PARA SOLUÇÃO ANTIVÍRUS"** , conforme as condições estabelecidas **Ata de Registro de Preços nº 0001/2022,** bem como No Termo de Referência, autuado sob index 34519272 do Processo Administrativo SEI-150001/008347/2022.

	Item	Descrição	Quantidade
Lote 1	1	Subscrição de licenças de uso para solução Antivírus (Estação de trabalho)	2.600 unidades
	2	Subscrição de licenças de uso para solução Antivírus (Servidores)	300 unidades
	3	Serviço de treinamento para solução antivirus (Estação de trabalho e Servidores)	3 Turmas
	4	Serviço de suporte técnico para solução antivírus (Estações de trabalho e servidores) remoto 24 x 7	1 unidade

Parágrafo Único - A referida contratação foi aprovada pela Diretoria da CEDAE, em reunião datada do dia 22 de Setembro de 2022, autuado sob index 40020405 do Processo Administrativo SEI-150001/008347/2022.

CLÁUSULA SEGUNDA: DAS OBRIGAÇÕES DA CEDAE

Constituem obrigações da **CEDAE**:

a) realizar os pagamentos devidos à **CONTRATADA**, nas condições estabelecidas neste contrato;

b) fornecer à **CONTRATADA**S documentos, informações e demais elementos pertinentes à execução do contrato;

c) exercer a fiscalização do contrato; e

d) aceitar provisória e definitivamente o objeto do contrato nas formas aqui definidas.

CLÁUSULA TERCEIRA: DAS OBRIGAÇÕES DA CONTRATADA

Constituem obrigações da **CONTRATADA,** além daquelas previstas no Termo de referência autuado sob index 34519272 do Processo Administrativo de referência:

a) conduzir os serviços de acordo com as normas técnicas e legislação em vigor;

b) abster-se de transmitir a terceiros qualquer informação ou documento de que tenha conhecimento ou posse em razão destes serviços, orientando seus funcionários sobre a impossibilidade de concederem entrevistas faladas ou escritas em nome da CEDAE, salvo se expressamente autorizados por esta;

c) providenciar todos os documentos necessários para que seu pessoal possa executar legalmente os serviços especificados neste Contrato;

d) manter-se em compatibilidade com as condições de habilitação inicialmente exigidas para esta contratação;

e) prestar, sem quaisquer ônus, os serviços necessários à correção das falhas verificadas na

execução dos serviços, responsabilizando-se, perante terceiros e CEDAE, pelos prejuízos decorrentes;

f) providenciar, por sua conta exclusiva, todos os seguros exigidos por Lei, cuja vigência deverá observar o recebimento definitivo do objeto;

g) enviar representante, sempre que solicitado, para examinar e prestar esclarecimentos relacionados a problemas verificados com a execução do objeto contratado; caso em que sua convocação será feita com antecedência mínima de 48 (quarenta e oito) horas;

h) manter a **CEDAE** informada sobre o desenvolvimento dos serviços;

i) cumprir todas as obrigações e encargos, sociais e trabalhistas, decorrentes da prestação de seus serviços; e

j) Demonstrar, apenas se possuir empregados alocados a este contrato e em quantidade superior a 100 (cem), o cumprimento do regime de quotas previsto na Lei Federal n. 8.213/1991 e Lei Estadual n. 7.258/2016, observando os seguintes quantitativos: (1) até 200 empregados = 2%; (2) de 201 a 500 empregados = 3%; (3) de 501 a 1.000 empregados = 4%; e (4) de 1.001 em diante = 5%.

CLÁUSULA QUARTA: DO PRAZO DE VIGÊNCIA

O prazo de vigência deste contrato será de **36 (trinta e seis) meses**, contados a partir da data indicada na Ordem de Fornecimento, que poderá ser emitida pela **CEDAE** após a assinatura deste contrato.

Parágrafo Único – Esta contratação poderá ser prorrogada por iguais e sucessivos períodos até o limite de 05 (cinco) anos totais de vigência, desde que observados os requisitos constantes do art. 203 do RILC.

CLÁUSULA QUINTA: DA DOTAÇÃO ORÇAMENTÁRIA

As despesas com a execução do presente contrato correrão à conta das seguintes dotações orçamentárias relativas ao exercício financeiro de 2022, assim classificadas:

Conta Contábil: 411110305
Programa de Trabalho: 2200022016
Código Orçamentário: 33904006
Fonte de Recursos: 10
Central de Custo: DE05040000
Reserva Orçamentária: 2022000747.

CLÁUSULA SEXTA: VALOR DO CONTRATO

A presente contratação será realizada sob o regime de preço unitário, sendo o seu valor total de **R$ 2.614.982,99 (dois milhões, seiscentos e quatorze mil, novecentos e oitenta e dois reais e noventa e nove centavos),** conforme proposta de preço da **CONTRATADA**, autuada sob index 36755398 e tabela resumo abaixo:

	Item	Descrição	Quantidade	Unitário	Total
Lote 1	1	Subscrição de licenças de uso para solução Antivírus (Estação de trabalho)	2.600 unidades	R$ 560,4876	R$ 1.457.267,7600
	2	Subscrição de licenças de uso para solução Antivírus (Servidores)	300 unidades	R$ 3.704,9004	R$ 1.111.470,1200
	3	Serviço de treinamento para solução antivirus (Estação de trabalho e Servidores)	3 Turmas	R$ 15.294,7110	R$ 45.884,1330
	4	Serviço de suporte técnico para solução antivírus (Estações de trabalho e servidores) remoto 24 x 7	1 unidade	R$ 360,9828	R$ 360,9828
Valor Total Global (Lote 1) 36 meses					R$ 2.614.982,9958

Parágrafo Único – O preço ajustado nesta Cláusula inclui o lucro e todos os custos e tributos dos serviços, sejam estes diretos ou indiretos, responsabilizando-se a **CONTRATADA** por toda e qualquer despesa, ainda que não prevista textualmente neste Contrato; inclusive a que decorrer de ato ou fato que implique em transgressão ou inobservância de qualquer dispositivo legal ou regulamentar, federal, estadual ou municipal.

CLÁUSULA SÉTIMA: DA EXECUÇÃO E FISCALIZAÇÃO DO CONTRATO

O contrato deverá ser executado fielmente, de acordo com as cláusulas avençadas neste instrumento, no termo de referência e na legislação vigente, especialmente aquelas relacionadas à execução, fiscalização, fornecimento, aceitação, conservação, aplicação de penalidades, rescisão de contratos e pagamentos, respondendo o inadimplente pelas consequências da inexecução total ou parcial dos serviços.

Parágrafo Primeiro – A execução do contrato será acompanhada e fiscalizada por uma comissão constituída de 3 (três) membros devidamente habilitados.

Parágrafo Segundo – É facultado à **CEDAE** exercer ampla fiscalização sobre os serviços objeto do presente contrato, diretamente ou por intermédio de prepostos devidamente credenciados, aos quais a **CONTRATADA** prestará a assistência requerida, facultando-lhe o acesso, em qualquer fase, época e local onde se processem tarefas relacionadas com o desenvolvimento dos serviços.

Parágrafo Terceiro - A **CONTRATADA** deverá refazer aquilo que for rejeitado, obedecendo às determinações da Comissão de Fiscalização.

Parágrafo Quarto – O representante da **CEDAE**, sob pena de ser responsabilizado administrativamente, anotará em registro próprio as ocorrências relativas à execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

Parágrafo Quinto – A **CONTRATADA** declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações necessários.

Parágrafo Sexto – A fiscalização do serviço pela **CEDAE** não excluirá ou atenuará a responsabilidade da **CONTRATADA** quanto à qualidade dos serviços, ao cumprimento dos prazos e a quaisquer outras obrigações contratuais ou legais, nem a eximirá de manter fiscalização própria.

Parágrafo Sétimo– Quando existirem empregados alocados à contratação, os mesmos deverão trabalhar com Equipamento de Proteção Individual (EPI) adequado ao tipo do serviço que será desenvolvido. A Fiscalização poderá paralisar os serviços enquanto tais empregados não

estiverem protegidos. O ônus da paralisação correrá por conta da **CONTRATADA**, mantendo-se inalterado o prazo de execução dos serviços.

Parágrafo Oitavo – Quando aplicável, proceder-se-á à fiscalização do regime de cotas de que trata a alínea "j" da cláusula terceira, realizando-se a verificação do cumprimento da obrigação assumida no contrato.

CLÁUSULA OITAVA: DA RESPONSABILIDADE

A **CONTRATADA** será responsabilizada pelos danos causados à **CEDAE** ou a terceiros, a título de dolo ou culpa, quando decorrentes da execução deste contrato; não se eximindo dessa responsabilidade pela fiscalização da **CEDAE**.

Parágrafo Primeiro – A **CONTRATADA** será a única responsável pelos encargos trabalhistas (inclusive os decorrentes de acordos, dissídios e convenções coletivas), previdenciários, fiscais e comerciais oriundos da execução do contrato, podendo a **CEDAE**, a qualquer tempo, exigir a comprovação do cumprimento de tais encargos.

Parágrafo Segundo – Quando houver mão de obra alocada a esta contratação, a **CONTRATADA** se obrigará a cumprir as determinações da Lei nº 6.514, de 22 de dezembro de 1977 e da Portaria nº 3214, de 08 de julho de 1978 e suas Portarias Modificadoras, que aprovam as Normas Regulamentadoras do Capítulo V, título II, da CLT, relativas à Segurança e Medicina do Trabalho.

Parágrafo Terceiro - Mensalmente, juntamente com a fatura/nota fiscal dos serviços, deverão ser apresentados os seguintes comprovantes para o processamento dos pagamentos:

a. medição/detalhamento do serviço prestado;

b. declaração de que se encontra cumprindo o regime de quotas da Lei Estadual n. 7.258/2016; exigível somente quando a **CONTRATADA** estiver enquadrada na situação prevista na cláusula terceira, letra "j", deste instrumento; e
c. declaração de que se encontra em dia com o pagamento das verbas salariais, de FGTS e INSS, exigível apenas quando houver previsão de pessoal destacado à execução do serviço, mesmo que em caráter eventual, nas dependências da CEDAE.

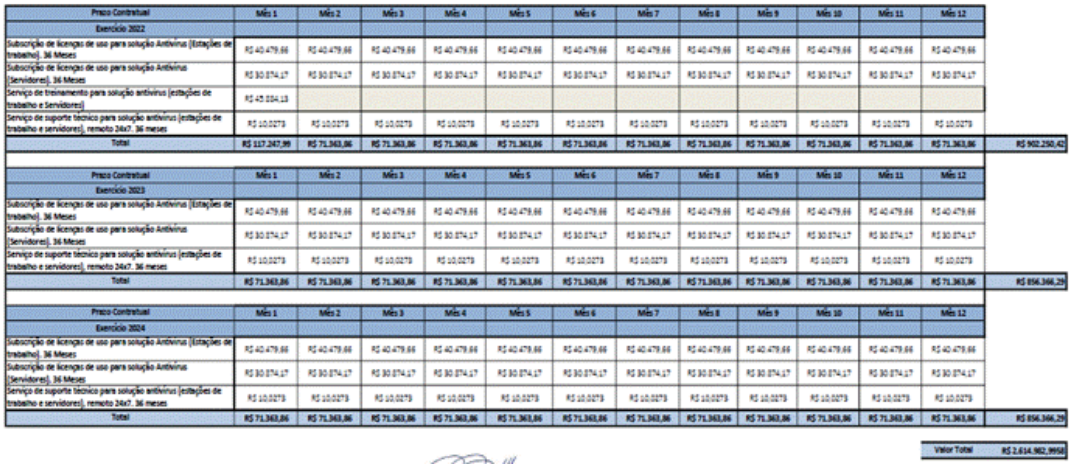
Parágrafo Quarto - A ausência de qualquer dos documentos mencionados no parágrafo anterior **impedirá a obtenção do recibo de adimplemento**, conforme art. 191 do RILC, e importará em notificação à **CONTRATADA** para, no prazo de 10 (dez) dias, apresentar defesa prévia e efetuar o cumprimento destas obrigações.

Parágrafo Quinto - Expirado o prazo constante do parágrafo acima sem que tenham sido tomadas as providências cabíveis, ou sendo rejeitados os argumentos apresentados em defesa pela **CONTRATADA,** será aplicada a ela penalidade de advertência. Permanecendo a inadimplência total ou parcial em virtude de ausência de qualquer dos documentos referidos, o contrato poderá ser rescindido com a aplicação da penalidade de suspensão prevista no item "iii" do parágrafo quinto da cláusula décima terceira.

Parágrafo Sexto – Todos os documentos mencionados nesta cláusula ficarão autuados no processo administrativo referente à contratação, bem como no processo de prestação de contas que deverá ser aberto em virtude da OS "E" nº 14.695/2017.

CLÁUSULA NONA: DAS CONDIÇÕES DE PAGAMENTO

A **CEDAE** pagará à **CONTRATADA** o valor dos total de **R$ 2.614.982,99 (dois milhões, seiscentos e quatorze mil, novecentos e oitenta e dois reais e noventa e nove centavos)**, de maneira parcelada e mensal para os serviços contínuos e integralmente para o serviço de treinamento sob demanda, juntamente com a parcela mensal do contrato referente aos demais itens, sendo efetuado diretamente na conta corrente da CONTRATADA, na forma do cronograma abaixo transcrito.



Preço Contratual	Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6	Mês 7	Mês 8	Mês 9	Mês 10	Mês 11	Mês 12	
Exercício 2022													
Subscrição de licenças de uso para solução Antivirus (Estações de trabalho), 36 Meses	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	
Subscrição de licenças de uso para solução Antivirus (Servidores), 36 Meses	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	
Serviço de treinamento para solução antivirus (estações de trabalho e Servidores)	R$ 45.054,13												
Serviço de suporte técnico para solução antivirus (estações de trabalho e servidores), remoto 24x7, 36 meses	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	
Total	R$ 117.247,99	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 902.250,42

Preço Contratual	Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6	Mês 7	Mês 8	Mês 9	Mês 10	Mês 11	Mês 12	
Exercício 2023													
Subscrição de licenças de uso para solução Antivirus (Estações de trabalho), 36 Meses	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	
Subscrição de licenças de uso para solução Antivirus (Servidores), 36 Meses	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	
Serviço de suporte técnico para solução antivirus (estações de trabalho e servidores), remoto 24x7, 36 meses	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	
Total	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 856.366,29

Preço Contratual	Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6	Mês 7	Mês 8	Mês 9	Mês 10	Mês 11	Mês 12	
Exercício 2024													
Subscrição de licenças de uso para solução Antivirus (Estações de trabalho), 36 Meses	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	R$ 40.479,66	
Subscrição de licenças de uso para solução Antivirus (Servidores), 36 Meses	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	R$ 30.874,17	
Serviço de suporte técnico para solução antivirus (estações de trabalho e servidores), remoto 24x7, 36 meses	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	R$ 10.027,9	
Total	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 71.363,86	R$ 856.366,29

Valor Total	R$ 2.614.982,99

Parágrafo Primeiro - Os pagamentos devidos em decorrência da execução do objeto deste contrato serão efetuados mediante crédito em conta bancária indicada pela **CONTRATADA** no banco **BRADESCO,** ficando autorizada a indicação de outra conta somente quando justificada tal impossibilidade.

Parágrafo Segundo – A **CONTRATADA** emitirá mensalmente as faturas/notas fiscais de seus serviços, cujos percentuais se limitarão aos valores reservados para esta contratação.

Parágrafo Terceiro – Os pagamentos à **CONTRATADA** serão feitos no prazo de **até 30 (trinta)** dias contados de cada período de **adimplemento**, assim considerado o cumprimento da etapa/parcela do serviço acompanhado da nota fiscal/fatura e da documentação mencionada na cláusula oitava. O adimplemento será confirmado por meio de recibo, nos termos da Ordem de Serviço n. 14.693/2017 e do art. 191 do RILC.

Parágrafo Quarto - De posse da documentação apresentada, a Comissão de Fiscalização, composta por 3 membros especialmente designados para esta contratação, **atestará mensalmente** (utilizando a forma prevista no art. 90, §3º da Lei Estadual n. 287/1979) a documentação e a qualidade do(s) serviço(s) desenvolvido(s) pela **CONTRATADA,** o que será feito como condição à realização do(s) pagamento(s) devido(s).

Parágrafo Quinto - A verificação de qualquer irregularidade no(s) serviço(s) prestado(s) ou na documentação encaminhada (ver cláusula oitava) **impedirá a concessão do atesto**, ficando consequentemente suspenso o prazo para pagamento, que somente voltará a correr após a solução do problema apontado.

Parágrafo Sexto – A suspensão do prazo para pagamento será efetuada na data em que ocorrer a notificação da **CONTRATADA** a respeito da irregularidade verificada, podendo se dar de forma simplificada, por e-mail.

Parágrafo Sétimo – Caso se faça necessário, a Comissão de Fiscalização, mensalmente, até o dia 30 (trinta) de cada mês, estabelecerá de comum acordo com a **CONTRATADA** a programação dos serviços que deverão ser realizados no mês seguinte, tendo por base as metas do cronograma físico-financeiro contratual e as necessidades dos serviços.

Parágrafo Oitavo- A **CEDAE** não se responsabilizará pelo pagamento de faturas de serviços executados em quantidades superiores às fixadas na Estimativa Orçamentária, salvo as expressamente determinadas pela Fiscalização.

Parágrafo Nono– Quando a contratação envolver alocação de mão de obra, a **CEDAE** poderá utilizar os créditos da **CONTRATADA** para efetuar os pagamentos dos salários e demais verbas trabalhistas e previdenciárias devidas por ela a seus empregados, fazendo-o diretamente ou por meio de aprovisionamento em conta vinculada, na forma prevista no art. 19-a, I, da IN/SLTI/MP 2/2008, com redação dada pela IN/SLTI/MP 6/2013, quando não for possível a realização dos pagamentos diretamente pela CEDAE.

Parágrafo Décimo - Os pagamentos eventualmente realizados com atraso, por culpa exclusiva da **CEDAE**, sofrerão a incidência de atualização financeira pelo IPCA/IBGE e juros moratórios de 0,5% (meio por cento) ao mês, calculados "pro rata die"; e aqueles pagos em prazo inferior ao estabelecido neste contrato serão feitos mediante desconto de 0,5% (dois por cento) ao mês, também calculados "pro rata die. ***Os juros e a atualização previstos neste parágrafo não correrão durante o período de suspensão do prazo para pagamento***.

CLÁUSULA DÉCIMA: DO REAJUSTE

O valor contratado poderá ser reajustado a cada 12 meses pelo IBGE/IPCA, iniciando-se a contagem deste prazo a partir da data da apresentação da proposta (I0), conforme a expressão matemática a seguir.

$$R = Po \left[\frac{I - Io}{Io} \right]$$

R = Valor do reajustamento

Po = Preço Contratual

I = Índice IBGE/ICA correspondente ao mês do reajustamento

Io = Índice IBGE/IPCA correspondente ao mês da data da apresentação da proposta.

a. Observada a periodicidade, a aplicação do reajustamento obedecerá ao cronograma de serviços em vigor.

b. O valor do reajustamento será objeto de fatura própria, separada daquela referente à medição dos serviços/obra.

PARÁGRAFO PRIMEIRO - A CONTRATADA terá o prazo máximo de 60 (sessenta) dias para iniciar o procedimento necessário ao reajuste de seus preços, contando-se este prazo a partir da divulgação do índice contratualmente ajustado. As anualidades que se completarem durante o curso da licitação/contratação deverão ser pleiteadas no mesmo prazo, contados da assinatura do contrato.

PARÁGRAFO SEGUNDO - O reajuste deverá ser formalmente solicitado por meio de e-mail ou de documento da CONTRATADA dirigido à Comissão de Fiscalização, registrado no Protocolo Geral da CEDAE, e deverá vir acompanhado dos cálculos, conforme art. 198, §1º do RILC.

PARÁGRAFO TERCEIRO - A inércia da CONTRATADA em iniciar o procedimento de reajuste no prazo acima fixado importará em decadência do seu direito de pleiteá-lo, relativo à correspondente anualidade.

PARÁGRAFO QUARTO - Consideram-se "anualidades" os sucessivos períodos de 12 (doze) meses, contados a partir da data da apresentação da propost (lo).

PARÁGRAFO QUINTO - O procedimento de reajuste seguirá o disposto no art. 194 e seguintes do RILC.

PARÁGRAFO SEXTO - As partes concordam, desde já, que o valor apurado a título de reajuste poderá ser negociado entre elas para permitir a aplicação de descontos em favor da CEDAE.

PARÁGRAFO SÉTIMO - A prorrogação de prazo por culpa da **CONTRATADA** impedirá que o período acrescido à execução do contrato seja considerado para fins de reajuste.

CLÁUSULA DÉCIMA PRIMEIRA – DA GARANTIA

Parágrafo Primeiro - A **CONTRATADA** deverá prestar garantia contratual, optando por uma das modalidades previstas no §1º do art. 70 da Lei 13.303/16.

Parágrafo Segundo - O comprovante deverá ser apresentado na Tesouraria da **CEDAE**, no 6º andar do prédio Sede, no prazo máximo de 10 (dez) dias úteis contados da assinatura do instrumento.

Parágrafo Terceiro - A garantia deverá ser prestada em percentual correspondente a 5% (cinco por cento) do valor do contrato, com exceção apenas da caução em dinheiro, que poderá ser prestada em percentual inferior, correspondente a 1,5% (um e meio por cento).

Parágrafo Quarto - A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

Parágrafo Quinto - A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

I. Todos os prejuízos advindos do não cumprimento do contrato;

II. Multas punitivas aplicadas à **CONTRATADA**;

III. Prejuízos diretos causados à **CONTRATANTE** decorrentes de culpa ou dolo durante a execução do contrato;

IV. Obrigações previdenciárias e trabalhistas não honradas pela **CONTRATADA**.

Parágrafo Sexto - Se a CONTRATADA optar pelo "seguro-garantia", deverá prestá-lo na modalidade "***Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviço***" para cobertura dos itens I a III do parágrafo anterior, em percentual correspondente a 1% (um por cento), complementada com a garantia adicional na modalidade ***"Seguro-Garantia de Ações Trabalhistas e Previdenciárias"*** para o item IV, em percentual de 4% (quatro por cento), sendo o parâmetro de ambas garantias o valor atualizado do contrato.

Parágrafo Sétimo - Se da contratação resultar a transferência da posse direta de bens da CEDAE à CONTRATADA, em valor total superior a **R$ 1.000.000,00 (um milhão de reais),** será exigido, ainda, o ***seguro multirriscos básico***, que conterá as seguintes coberturas adicionais mínimas: Danos Elétricos, Subtração de Bens e Mercadorias, Responsabilidade Civil de Operações, Responsabilidade Civil do Empregador, Equipamentos Estacionários e Móveis, cuja cobertura alcançará o valor total dos bens entregues.

Parágrafo Oitavo - A garantia somente poderá ser liberada após o recebimento definitivo do objeto, cabendo à **CONTRATADA** formular tal solicitação.

Parágrafo Nono - A garantia que não for prestada em dinheiro deverá ser firmada com prazo de validade superior à vigência do contrato administrativo em, no mínimo, 180 (cento e oitenta) dias.

Parágrafo Décimo - A **CONTRATADA** se declara ciente de que as alterações de valor e/ou de prazo efetuadas no contrato importarão na necessidade de reforço e/ou prorrogação da garantia prestada, não se eximindo a **CONTRATADA** desta responsabilidade mesmo quando silente o aditivo formalizado.

Parágrafo Décimo Primeiro - Nos casos em que os valores das multas vierem a ser descontados da garantia, seu valor original será recomposto no prazo de até 72 (setenta e duas) horas, sob pena de multa e/ou de rescisão administrativa do contrato.

Parágrafo Décimo Segundo - A garantia que for prestada na modalidade fiança bancária deverá ser apresentada conforme modelo constante do Anexo VII da OS n. 14.927/2017.

Parágrafo Décimo Terceiro – O atraso da **CONTRATADA** em prestar ou revalidar a garantia autorizará a CEDAE a promover o bloqueio dos pagamentos devidos até o limite máximo de 5% (cinco por cento) do valor do contrato. Uma vez prestada a garantia, esta substituirá o bloqueio.

Parágrafo Décimo Quarto - O bloqueio efetuado com base no parágrafo anterior não gerará direito a nenhum tipo de compensação financeira à **CONTRATADA**.

Parágrafo Décimo Quinto - A **CEDAE** se ressalva o direito de pleitear em juízo as perdas e danos que não puderem ser reparados através da garantia prestada.

CLÁUSULA DÉCIMA SEGUNDA - DA SUBCONTRATAÇÃO

Não será admitida a subcontratação nos serviços contratados.

CLÁUSULA DÉCIMA-TERCEIRA: DAS SANÇÕES ADMINISTRATIVAS

A inexecução dos serviços, total ou parcial, a execução imperfeita, a mora na execução ou qualquer inadimplemento ou infração contratual, sujeitarão a **CONTRATADA**, sem prejuízo da responsabilidade civil ou criminal que lhe couber, às penalidades seguintes:

a) advertência;

b) multa administrativa;

c) suspensão temporária da participação em licitação e impedimento de contratar com a CEDAE por prazo não superior a 2 (dois) anos;

Parágrafo Primeiro - A sanção administrativa deve ser determinada de acordo com a natureza e a gravidade da falta cometida.

Parágrafo Segundo - Todas as sanções previstas no caput serão impostas pelo Diretor responsável, na forma do art. 21, §1º, do Procedimento de aplicação de sanções da CEDAE.

Parágrafo Terceiro- A **multa administrativa**, prevista na alínea "b" do caput, será aplicada à CONTRATADA pelo descumprimento de suas obrigações acessórias, observando o que segue:

i) corresponderá ao valor de até 5% (cinco por cento), aplicada de acordo com a gravidade da infração e proporcionalmente às parcelas não executadas, a contar da data da infração;

i.1.) Nas infrações cometidas após o encerramento do contrato, a base de cálculo será o valor da contratação.

ii) nas reincidências específicas, deverá corresponder, no mínimo, ao dobro do valor da que tiver sido inicialmente imposta;

iii) O somatório das multas administrativas deverá observar o limite de 20% (vinte por cento) do valor do contrato ou do empenho.

iv) poderá ser aplicada cumulativamente a qualquer outra penalidade; e

v) não tem caráter compensatório, não se confundindo, portanto, com as multas por atraso, com a multa rescisória e com a multa prevista na cláusula décima oitava, que poderão ser aplicadas cumulativamente à multa administrativa.

Parágrafo Quarto - A suspensão temporária da participação em licitação e impedimento de contratar, prevista na alínea "c", do caput desta cláusula, será aplicada conforme as disposições do art. 9º do Procedimento de Aplicação de Sanções da CEDAE, observando o seguinte:

i. não poderá ser aplicada em prazo superior a 2 (dois) anos;

ii. sem prejuízo de outras hipóteses, **deverá** ser aplicada quando o adjudicatário faltoso, sancionado com multa, não realizar o depósito deste valor no prazo devido;

Parágrafo Quinto - A aplicação das penalidades acima referidas, em virtude das infrações contratuais retro mencionadas, não importará em renúncia, por parte da **CEDAE,** da faculdade de declarar rescindido o contrato, se assim entender conveniente ao interesse público.

Parágrafo Sexto - O atraso injustificado no cumprimento das obrigações contratuais sujeitará a **CONTRATADA** à **multa de mora** por dia útil que exceder ao prazo estipulado, conforme percentuais abaixo:

a) 0,33% (trinta e três centésimos por cento) por dia de atraso, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, correspondente a até 30 (trinta) dias de atraso; e

b) 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, calculado sobre o valor correspondente à parte inadimplente, quando o atraso ultrapassar 30 (trinta) dias, até o limite máximo de 20%.

Parágrafo Sétimo - As multas porventura aplicadas serão consideradas dívidas líquidas e certas, ficando a **CEDAE** autorizada a descontá-las das garantias prestadas, e caso estas sejam insuficientes, dos pagamentos devidos à **CONTRATADA;** ou ainda, quando for o caso, cobrá-las judicialmente, servindo para tanto, o instrumento contratual como título executivo extrajudicial.

Parágrafo Oitavo - A intimação do interessado deverá indicar o prazo e o local para a apresentação de defesa.

l) A defesa prévia do interessado será exercida no prazo de 10 (dez) dias úteis, na forma prevista no art. 26, §§ 3º e 5º do Procedimento de Aplicação de Sanções da CEDAE.

Parágrafo Nono - Será emitida decisão conclusiva sobre a aplicação ou não da sanção, pela autoridade competente, devendo ser apresentada a devida motivação, com a demonstração dos fatos e dos respectivos fundamentos jurídicos.

Parágrafo Décimo - Todas as multas previstas neste contrato, incluindo a rescisória e a prevista na cláusula décima oitava, serão somadas quando aplicadas cumulativamente, e terão como limite seus respectivos percentuais máximos.

CLÁUSULA DÉCIMA QUARTA– DA RESCISÃO DO CONTRATO

A inexecução total ou parcial do contrato poderá ensejar a sua rescisão com as consequências cabíveis.

Parágrafo Primeiro - A rescisão contratual poderá ocorrer por:

I - ato unilateral e escrito, quando verificada a ocorrência de qualquer das situações descritas no art. 222 do RILC;

II- acordo entre as partes, reduzido a termo no processo de contratação, desde que seja vantajoso à CEDAE; ou

III – decisão judicial ou arbitral.

Parágrafo Segundo - Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo administrativo que ensejou a contratação, sendo assegurado à **CONTRATADA** o direito ao contraditório e ampla defesa.

Parágrafo Terceiro - Quando a rescisão ocorrer por interesse exclusivo da CEDAE, sem que haja culpa da CONTRATADA, esta será ressarcida dos prejuízos que houver sofrido.

Parágrafo Quarto - A rescisão por ato unilateral da CEDAE, quando justificada no descumprimento de obrigações contratuais por parte da CONTRATADA, acarretará a aplicação de multa rescisória, no percentual de 10% (dez por cento) calculada sobre o saldo reajustado do contrato, bem como a execução da garantia contratual e/ou a utilização dos créditos decorrentes do próprio contrato.

Parágrafo Quinto - A CEDAE se reserva ao direito de cobrar indenização suplementar em juízo se ficar constatado que o prejuízo causado foi superior ao valor da multa rescisória aplicada, conforme autorização contida no art. 416, parágrafo único, *in fine,* do Código Civil.

Parágrafo Sexto - A rescisão contratual por acordo entre as partes será da competência da autoridade referida no art. 25 do RILC; enquanto a rescisão unilateral ficará a cargo do Diretor responsável pela contratação, conforme art. 15 do Procedimento Interno de Sanções da CEDAE.

Parágrafo Sétimo - A **CONTRATADA** manifesta previamente que, na hipótese de a CEDAE reduzir suas operações em face do Projeto de Universalização e Desestatização do Saneamento Básico no Estado do Rio de Janeiro, aceitará a redução qualitativa ou quantitativa proposta pela CEDAE ou ainda a rescisão unilateral, desde que mediante comunicação por escrito e com pelo menos 30 (trinta) dias de antecedência, renunciando a Contratada antecipadamente a qualquer

direito, nessas situações, à indenização ou compensação.

CLÁUSULA DÉCIMA-QUINTA: CASO FORTUITO OU DE FORÇA MAIOR

Se a **CONTRATADA** ficar temporariamente impedida de cumprir suas obrigações, no todo ou em parte, em consequência de caso fortuito ou de força maior, deverá comunicar o fato de imediato à Fiscalização da **CEDAE** e ratificar por escrito a comunicação, informando os efeitos danosos do evento.

Parágrafo Único – Constatada a ocorrência de caso fortuito ou de força maior, ficarão suspensas tanto as obrigações que a **CONTRATADA** ficar impedida de cumprir, quanto a obrigação da **CEDAE** em remunerá-las.

CLÁUSULA DÉCIMA-SEXTA: DA ALTERAÇÃO CONTRATUAL

Este contrato poderá ser alterado por acordo entre as partes, formalizado por meio de Termo Aditivo, com observância do disposto nos art. 209 a 211 do RILC.

Parágrafo Primeiro – As alterações que se fizerem necessárias nas quantidades ou qualidade do serviço contratado deverão observar os limites do §1º do art. 81 da Lei 13.303/2016.

Parágrafo Segundo – Quando a contratação trouxer previsão de matriz de risco haverá impedimento para a celebração de aditivo decorrente dos eventos ali previstos como de responsabilidade da **CONTRATADA**, conforme art. 196, §2º do RILC.

CLÁUSULA DÉCIMA-SÉTIMA: DA IMPOSSIBILIDADE DE MODIFICAÇÃO DO CONTRATO PELA SUPRESSIO

O atraso, a tolerância ou a omissão da **CEDAE** no exercício de suas prerrogativas jamais ensejará a modificação automática das cláusulas avençadas, não sugerindo qualquer renúncia de direitos por parte desta, que poderá exercê-los a qualquer tempo.

CLÁUSULA DÉCIMA-OITAVA: DO RECURSO AO JUDICIÁRIO

As importâncias decorrentes de quaisquer penalidades impostas à **CONTRATADA**, inclusive as perdas e danos ou prejuízos que a execução do contrato tenha acarretado, quando superiores à garantia prestada ou aos créditos que a **CONTRATADA** tenha em face da **CEDAE**, que não comportarem cobrança amigável, serão cobrados judicialmente.

Parágrafo Único – Caso a **CEDAE** tenha de recorrer ou comparecer a Juízo para haver o que lhe for devido, a **CONTRATADA** ficará sujeita ao pagamento, além do principal do débito, da pena convencional de 10% (dez por cento) sobre o valor do litígio, dos juros de mora de 1% (um por cento) ao mês, despesas de processo e honorários de advogado, estes fixados, desde logo, em 20% (vinte por cento) sobre o valor em litígio.

CLÁUSULA DÉCIMA-NONA: DOS CASOS OMISSOS

Os casos omissos serão resolvidos conforme disposto na Lei nº 13.303, de 30 de junho de 2016.

CLÁUSULA VIGÉSIMA: DA ACEITAÇÃO PROVISÓRIA

Aceitação Provisória ocorrerá ao término de cada exercício financeiro, mediante emissão de PARECER CIRCUNSTANCIADO PARA ACEITAÇÃO PROVISÓRIA (doc. ref. ANEXO VI da Ordem de Serviço n. 14.693/2017), que será assinado pelas partes atestando o cumprimento de todas as cláusulas contratuais.

Parágrafo Primeiro – A competência para a emissão do PARECER CIRCUNSTANCIADO PARA ACEITAÇÃO PROVISÓRIA será da Comissão de Fiscalização do Contrato, não se exigindo da **CONTRATADA** a comunicação acerca da entrega dos resultados dos serviços executados.

Parágrafo Segundo - Se a Comissão de Fiscalização do Contrato vier a constatar alguma incorreção nos serviços executados, deverá relatá-la no citado parecer e encaminhar uma cópia deste ao Gerente do Contrato, para adoção das providências necessárias.

Parágrafo Terceiro - O prazo para elaboração do parecer circunstanciado em questão será de 15 (quinze) dias após o encerramento de cada exercício financeiro.

Parágrafo Quarto – Somente no último mês/etapa/parcela de execução do Contrato é que a Comissão de Fiscalização e o Gerente do Contrato deverão obedecer ao procedimento necessário à emissão do **TERMO DE ACEITAÇÃO PROVISÓRIA** (doc. Ref. ANEXO I da Ordem de Serviço n. 14.693/2017), abaixo descrito:

I. A **CONTRATADA** deverá comunicar à **CEDAE**, por meio de carta redigida em papel timbrado, que o objeto pactuado se encontra em condições de ter sua posse transferida ou o resultado dos serviços executados entregues, mesmo que aquela entenda que existam ressalvas quanto ao cumprimento das obrigações contratuais por parte da **CEDAE**.

II. As ressalvas deverão ser consignadas na citada carta e encaminhada à **CEDAE**, juntamente com a fatura relativa à última medição realizada do contrato e com os documentos exigidos para realização do pagamento. O Representante da **CEDAE** não poderá conceder à contratada o recibo simplificado de adimplemento do último mês/etapa/parcela do cronograma físico-financeiro se não estiver acompanhada da respectiva carta.

III. Se após 10 (dez) dias contados a partir da conclusão do último mês/etapa/parcela a **CONTRATADA** se omitir ou se recusar a realizar a comunicação da condição de transferência de posse do objeto pactuado, ou o resultado dos serviços executados à **CEDAE**, o Gerente do contrato deverá notificá-la, por meio de carta registrada com aviso de recebimento, sobre a obrigação de manifestar-se pela efetiva comunicação, informando acerca do inadimplemento de suas obrigações e da consequente suspensão do prazo para pagamento.

IV. Persistindo a recusa da **CONTRATADA** em se manifestar por meio de carta redigida em papel timbrado quanto à notificação recebida, o prazo de pagamento referente à última fatura ficará suspenso.

V. A obrigação será considerada adimplida pelo cumprimento da etapa/parcela acompanhada dos documentos exigidos neste contrato para a realização do correspondente pagamento.

VI. O representante da **CEDAE**, após a conclusão de cada etapa/parcela, e no momento da apresentação de todos os documentos necessários ao pagamento da despesa, fornecerá à **CONTRATADA** recibo simplificado, com a listagem dos documentos recebidos. Na ausência de qualquer documento exigido no contrato, não será fornecido o referido recibo.

VII. De imediato, o representante da **CEDAE** encaminhará os documentos recebidos à Comissão de Fiscalização do Contrato, para que esta, no prazo de até 5 (cinco) dias úteis contados a partir da entrega do recibo à **CONTRATADA,** verifique a veracidade e a correção das informações neles contidas e, se for o caso, efetive o atesto da fatura. Qualquer incorreção nos documentos apresentados pela contratada ensejará a suspensão do prazo para pagamento da última fatura pela Comissão de Fiscalização.

VIII. A veracidade e a correção das informações contidas nos comprovantes de recolhimento de tributos e contribuições sociais serão verificadas no setor de Contas a pagar da **CEDAE** quando do encaminhamento da fatura para pagamento.

IX. Caberá à Comissão de Fiscalização do Contrato notificar a contratada quanto ao seu atraso nas providências necessárias à obtenção do adimplemento, fazendo-o ao menos uma vez, caso este supere 10 (dez) dias contados da conclusão da respectiva etapa. As notificações feitas pela **CEDAE** poderão ocorrer de modo simplificado, por correspondência eletrônica (e-mail) ou carta, exceto no último mês/etapa/parcela dos serviços, e deverão ser registradas no processo.

X. O procedimento de aceitação provisória poderá ser dispensado nos casos mencionados no art. 187 do Regulamento Interno de Licitações e Contratos da CEDAE (RILC), casos em que será substituído pela emissão de simples "recibo", conforme item 1.2.7.1 da Ordem de Serviço n. 14.693/2017, que permanece aplicável naquilo em que não confrontar com o referido art. 187 do RILC.

Parágrafo Quinto– A Comissão de Fiscalização deverá fornecer à **CONTRATADA**, se por ela solicitado, a Ordem de Serviço n. 14.693/2017, que disciplina o recebimento provisório e definitivo nos contratos da **CEDAE**.

CLÁUSULA VIGÉSIMA-PRIMEIRA: DA ACEITAÇÃO DEFINITIVA DOS SERVIÇOS

O serviço executado será recebido definitivamente ao final do contrato, da seguinte forma:

Parágrafo Primeiro – A aceitação definitiva do objeto pactuado será feita por meio de Comissão especificamente nomeada para este fim, mediante emissão do TERMO DE ACEITAÇÃO DEFINITIVA (doc. Ref. ANEXO VII da Ordem de Serviço n. 14.693/2017).

Parágrafo Segundo – A empresa contratada, após assinatura do Termo de Aceitação Provisória, no prazo máximo de 60 (sessenta), solicitará à **CEDAE**, por meio de carta redigida em papel timbrado, que o objeto pactuado seja aceito definitivamente.

Parágrafo Terceiro – De igual modo, a **CONTRATADA** deverá apresentar declaração de que a **CEDAE** possui ou não pendências de pagamento, dando-lhe a quitação financeira do contrato.

Parágrafo Quarto– No caso de omissão ou recusa da **CONTRATADA** em solicitar à **CEDAE** a aceitação definitiva do objeto contratado, o Gerente do contrato deverá notificá-la, por meio de carta registrada com aviso de recebimento, sobre a necessidade de se manifestar pela efetiva solicitação em, no máximo, 15 (quinze) dias contados a partir do recebimento da notificação.

Parágrafo Quinto– Persistindo a recusa da **CONTRATADA** em se manifestar, por meio de carta redigida em papel timbrado, quanto à notificação recebida, o Gerente do contrato reterá a garantia contratual, se houver.

Parágrafo Sexto- Compete ao Gerente do Contrato, quando couber, o acompanhamento e o controle dos prazos de vencimentos das apólices de seguro-garantia ou carta de fiança correspondente às garantias contratuais apresentadas pela **CONTRATADA**.

Parágrafo Sétimo- A inobservância do parágrafo anterior poderá ensejar apuração de responsabilidade, caso a perda da garantia contratual resulte em prejuízos para a **CEDAE**.

CLÁUSULA VIGÉSIMA-SEGUNDA – DAS MEDIDAS DE INTEGRIDADE – LEI ESTADUAL 7.753/2017

Parágrafo Primeiro - Na execução do presente Contrato é vedado às partes, dentre outras condutas:

a) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja;

b) criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Contrato;

c) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;

d) manipular ou fraudar o equilíbrio econômico-financeiro do presente Contrato; ou

e) de qualquer maneira fraudar o presente Contrato; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 (conforme alterada) ou de quaisquer outras leis ou regulamentos aplicáveis ("Leis Anticorrupção"), ainda que não relacionadas com o presente Contrato.

Parágrafo Segundo - A **CONTRATADA** compromete-se a respeitar, cumprir e fazer cumprir, no que couber, o **Código de Ética e Conduta da CEDAE, presente no link www.cedae.com.br/governancacorporativa.**

Parágrafo Terceiro - A violação aos parágrafos primeiro e segundo pelos administradores, empregados ou prestadores de serviços da **CONTRATADA**, a depender da gravidade da infração e dos danos causados à CEDAE, acarretará na aplicação das sanções administrativas previstas no contrato, rescisão unilateral e/ou ressarcimento de perdas e danos apurados.

Parágrafo Quarto - A comunicação imediata à CEDAE de eventual violação aos parágrafos primeiro e segundo, acompanhada das medidas tomadas pela **CONTRATADA,** suficientes para sanar a violação, desde que preservados os negócios da CEDAE, sua imagem e reputação, serão consideradas como atenuantes para o fim previsto no parágrafo anterior.

Parágrafo Quinto - A **CONTRATADA** se obriga a possuir e manter programa de integridade nos termos da disciplina conferida pela Lei Estadual n.° 7.753/2017 e eventuais modificações e regulamentos subsequentes, consistindo tal programa no "*conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública*".

Parágrafo Sexto - O programa de integridade será obrigatório nos contratos com prazo de vigência igual ou superior a 180 (cento e oitenta) dias cujo valor ultrapasse R$ 650.000,00 (seiscentos e cinquenta mil reais), para compras e serviços, ou R$ 1.500.000,00 (um milhão e quinhentos mil reais), para obras e serviços de engenharia; sendo facultativo nos demais casos.

Parágrafo Sétimo - A **CONTRATADA** que não possuir o programa de integridade já implantado

deverá constituí-lo no prazo de até 180 (cento e oitenta) dias contados da assinatura deste contrato.

Parágrafo Oitavo - O não atendimento ao disposto no parágrafo sétimo implicará na aplicação de multa moratória de 0,02%, por dia, incidente sobre o valor do contrato.

Parágrafo Nono - O montante correspondente à soma dos valores básicos das multas moratórias será limitado a 10% do valor do contrato.

Parágrafo Décimo - O não cumprimento da exigência durante o período contratual acarretará na impossibilidade da contratação da empresa com a Administração Direta e Indireta do Estado do Rio de Janeiro até a sua regular situação.

Parágrafo Décimo-Primeiro - O cumprimento da exigência da implantação não implicará ressarcimento das multas aplicadas.

Parágrafo Décimo-Segundo - Caberá ao Gerente do Contrato, sem prejuízo de suas demais atribuições, conforme estabelecido no artigo 11 da Lei Estadual 7.753 de 02/10/2017, fiscalizar a aplicabilidade de seus dispositivos.

Parágrafo Décimo-Terceiro - As ações e deliberações do Gerente do Contrato não poderão implicar interferência na gestão das empresas nem ingerência de suas competências, devendo ater-se a responsabilidade de aferir a implantação do Programa de Integridade por meio de prova documental emitida pela **CONTRATADA**."

Parágrafo Décimo-Quarto - A prática de atos de contra a Administração Pública Estadual sujeitará a **CONTRATADA** às sanções previstas na Lei Federal nº 12.846/2013, na forma do Decreto Estadual nº. 46.366/2018.

CLÁUSULA VIGÉSIMA-TERCEIRA: DA PUBLICAÇÃO

O extrato desta contratação será publicado no Diário Oficial do Estado, para fins de mera publicidade, e posteriormente divulgado no sítio eletrônico da **CEDAE**.

Parágrafo Único - Após a publicação no Diário Oficial, deverá ser observado o disposto na Deliberação TCE-RJ n. 312/2020 para o envio das informações nos casos exigidos.

CLÁUSULA VIGÉSIMA QUARTA – DA CONFIDENCIALIDADE E DA PROTEÇÃO DE DADOS PESSOAIS

A CEDAE e a CONTRATADA se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

a. o tratamento de dados pessoais venha a ocorrer de acordo com as bases legais previstas nas hipóteses dos artigos 7º, 11 e/ou 14 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular;

b. o tratamento seja limitado às atividades necessárias para o alcance das finalidades do serviço contratado ou, quando for o caso, ao cumprimento de obrigação legal ou regulatória,

no exercício regular de direito, por determinação judicial ou por requisição da ANPD;

c. Caso a coleta de dados pessoais dos usuários se faça indispensável ao cumprimento do próprio contrato, o seu acesso será solicitado diretamente pela CONTRATADA aos titulares, após prévia aprovação da CEDAE; responsabilizando-se a CONTRATADA pela sua gestão. Os dados coletados só poderão ser utilizados na execução do objeto especificado neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outras finalidades;

1. eventualmente, podem as partes convencionar formalmente que a CEDAE será responsável por obter o consentimento dos titulares.

d. os sistemas que servirão de base para armazenamento dos dados pessoais coletados sigam um conjunto de premissas, políticas, especificações técnicas, devendo estar alinhados com a legislação vigente e as melhores práticas de mercado; e

e. os dados obtidos em razão deste contrato sejam armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (*log*), adequado controle baseado em função (*role based access control*) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros.

Parágrafo Primeiro - A transferência internacional de dados pessoais pela CONTRATADA somente poderá ser realizada caso seja necessária para o atendimento do objeto deste contrato, desde que haja o compromisso com as seguintes garantias:

a. que a legislação do país para o qual os dados forem transferidos assegurem o mesmo nível de proteção que a legislação brasileira em termos de privacidade e proteção de dados, sob pena de encerramento da relação contratual em virtude das restrições previstas no ordenamento jurídico brasileiro;

b) que os dados transferidos sejam tratados em ambiente da CONTRATADA;

c) que o tratamento dos dados pessoais, incluindo a própria transferência, seja e continue a ser realizada de acordo com a legislação brasileira e com a do país receptor dos dados pessoais;

d) que existam garantias suficientes em relação às medidas de segurança técnicas e organizacionais, especificadas formalmente ao contratante, não se permitindo o compartilhamento de dados remetidos por terceiros;

e) que as medidas de segurança sejam adequadas para proteger os dados pessoais contra a destruição/perda acidental ou ilícita, a alteração, a divulgação ou o acesso não autorizado, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. As medidas de segurança deverão possuir um nível de segurança adequado em relação aos riscos que o tratamento representa e à natureza dos dados a proteger, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação;

f) que haja zelo no cumprimento das medidas de segurança;

g) que a legislação que lhe é aplicável não o impeça de respeitar as instruções recebidas pela CEDAE e as obrigações do contrato e que, no caso de haver uma alteração nesta legislação que possa ter efeito adverso substancial nas garantias e obrigações conferidas pelas cláusulas do

contrato, que haja comunicação imediatamente dessa alteração à CEDAE que, neste caso, poderá suspender a transferência de dados e/ou aplicar as penalidades cabíveis;

h) que a CEDAE seja imediatamente notificada sobre qualquer solicitação juridicamente vinculativa de divulgação de dados pessoais por uma autoridade fiscalizadora responsável pela aplicação da lei, a menos que haja dever legal de sigilo;

i) que as solicitações de informação formuladas pela CEDAE sejam respondidas rápida e adequadamente quando relacionadas ao tratamento dos dados pessoais objeto da transferência;

j) que a pedido da CEDAE sejam apresentadas as informações necessárias sobre o tratamento relacionado com os dados pessoais objeto da transferência, ou com as informações solicitadas pelas autoridades fiscalizadoras;

k) que a CEDAE seja previamente informada sobre a necessidade de subcontratação, cabendo-lhe anuir, ou não, expressamente acerca desta possibilidade. A subcontratação será executada de acordo com o disposto neste contrato;

k.1) Em qualquer caso, a subcontratação somente poderá ocorrer se a subcontratada comprovar que está adequada à LGPD.

l) que seja enviado imediatamente à CEDAE uma cópia de qualquer acordo de subcontratação que celebrar sobre o objeto deste contrato.

Parágrafo Segundo - A CONTRATADA dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula, inclusive no tocante à Política de Privacidade da CEDAE.

Parágrafo Terceiro - As partes cooperarão entre si no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas leis e regulamentos de proteção de dados em vigor e, também, no atendimento de requisições e determinações do Poder Judiciário, Tribunais de Contas, Ministério Público, ou quaisquer outros órgãos de controle administrativo.

Parágrafo Quarto - Uma parte deverá informar a outra, sempre que receber uma solicitação de um titular de dados, a respeito de dados pessoais da outra Parte, abstendo-se de responder qualquer solicitação, exceto nas instruções documentadas ou conforme exigido pela LGPD e Leis e Regulamentos de Proteção de Dados em vigor.

Parágrafo Quinto - O Encarregado pelo tratamento de dados pessoais da CONTRATADA manterá contato formal com o Encarregado da CEDAE no prazo de até 24 (vinte e quatro) horas contados da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que este possa adotar as providências devidas na hipótese de questionamento das autoridades competentes.

Parágrafo Sexto - A critério do Encarregado da CEDAE, a CONTRATADA poderá ser provocada a colaborar na elaboração do relatório de impacto à proteção de dados pessoais (RIPD), conforme sensibilidade e risco inerentes aos serviços objeto deste contrato, no tocante a dados pessoais.

Parágrafo Sétimo - Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sensíveis ou não, a CONTRATADA interromperá o tratamento e, em no máximo (30) dias, sob instruções e na medida do determinado pela CEDAE, eliminará

completamente os Dados Pessoais e todas as cópias porventura existentes (em formato digital, físico ou outro qualquer), salvo quando necessite mantê-los para cumprimento de obrigação legal ou outra hipótese legal prevista na LGPD.

Parágrafo Oitavo - Eventuais responsabilidades das partes, serão apuradas conforme estabelecido neste contrato e, também, de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

Parágrafo Nono - A CONTRATADA e seus empregados se obrigarão a manter, mesmo após o término da vigência contratual, a mais absoluta confidencialidade sobre dados e informações disponibilizados ou conhecidos em decorrência deste contrato.

Parágrafo Décimo - A CONTRATADA e seus empregados ficarão terminantemente proibidos de fazer uso ou revelação, sob nenhuma justificativa, a respeito de qualquer informação, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou elementos de propriedade da CEDAE, ou de seus Clientes, aos quais tiver acesso em decorrência do objeto desta contratação.

Parágrafo Décimo Primeiro - A CONTRATADA e seus empregados deverão obedecer às normas sobre confidencialidade e segurança adotadas pela CEDAE, além das cláusulas específicas constantes neste instrumento contratual.

Parágrafo Décimo Segundo - O descumprimento das obrigações relacionadas com a confidencialidade das informações, mediante ações ou omissões intencionais ou acidentais, determinará a responsabilização, na forma da lei, de seus dirigentes e empregados envolvidos durante ou após a vigência contratual.

CLÁUSULA VIGÉSIMA-QUINTA: DO FORO DE ELEIÇÃO

Fica eleito o Foro da Comarca da Capital do Rio de Janeiro para dirimir qualquer litígio decorrente do presente contrato que não possa ser resolvido por meio amigável, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

E, por estarem assim acordes em todas as condições e cláusulas estabelecidas neste contrato, firmam as partes o presente instrumento em via digital de igual forma e teor, depois de lido e achado conforme.

Rio de Janeiro, ____ de _____ de 2022 .

Pela **CEDAE:**

LEONARDO ELIA SOARES

Diretor Presidente

JULIO CESAR URDANGARIN BATISTA JUNIOR

Diretor Administrativo

Pela **CONTRATADA:**

PATRICIA ANGELINA DA CONCEIÇÃO
Sócia Administradora

Rio de Janeiro, 03 outubro de 2022

Documento assinado eletronicamente por **Patrícia Angelina da Conceição**, **Usuário Externo**, em 03/10/2022, às 18:02, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Julio Cesar Urdangarin Batista Junior**, **Diretor**, em 03/10/2022, às 21:00, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Leonardo Elia Soares**, **Presidente**, em 04/10/2022, às 17:51, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **40533482** e o código CRC **C7960820**.

Referência: Processo nº SEI-150001/008347/2022 SEI nº 40533482

Avenida Presidente Vargas, 2655 - Bairro Cidade Nova, Rio de Janeiro/RJ, CEP 20210-030
Telefone:

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de serviço de proteção de estações de trabalho e servidores com subscrição de licenças de uso para solução antivírus, contemplando instalação, configuração, atualização, treinamento, suporte e garantia, por um período de 36 meses, para proteção do ambiente de Tecnologia da Informação da CEDAE.

2. JUSTIFICATIVA

Observamos nos últimos anos um aumento nos crimes disparados contra usuários e empresas com objetivos diversos, entre eles o sequestro de dados em troca de resgate e a aquisição de informações bancárias para utilização em golpes.
Pesquisas apontam que, durante o ano de 2021, o cibercrime cresceu no Brasil mais de 20%.

Este aumento percebido em relação ao crime cibernético possui inúmeras causas, mas entre elas podemos destacar a mudança da cultura das organizações que se viram, em meio a pandemia, obrigadas a adotar novas formas para a execução das rotinas de trabalho, entre elas a adoção do Home Office.
Com a Empresa CEDAE não foi diferente, adotamos novas rotinas, implementamos novas soluções, facilitamos o acesso dos nossos funcionários.

Diante de todo este cenário e com a proximidade do termino do nosso atual contrato de solução de segurança de estações de trabalho e servidores, torna-se necessária a contratação de nova solução para continuarmos cumprindo com a defesa do nosso parque tecnológico e datacenter.

Atualmente é imprescindível a existência de uma solução de antivírus empresarial nos ambientes de informática devido ao grande aumento dos números de incidência de vírus, worms, spywares, malwares e trojans difundidos através da Internet e Correio Eletrônico. Pela grande facilidade e rapidez de disseminação e pela dificuldade em se manter controle sobre a transmissão de dados entre a Internet e a empresa, já que acessos web e e-mail são liberados, é de vital importância um sistema de proteção local em cada estação.

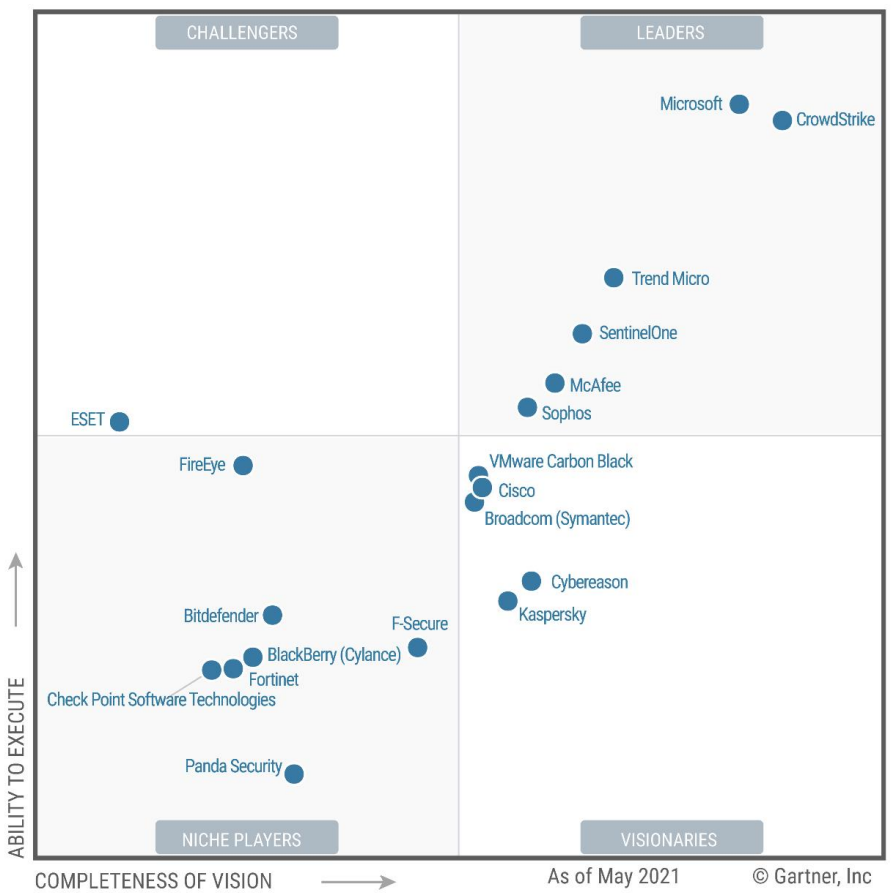
Uma vez instalado e atualizado nos microcomputadores e servidores, o sistema de antivírus age como uma barreira extra de segurança para os dados, softwares e ao próprio usuário, pois o número de

incidentes com roubo de informações bancárias (senhas, contas de banco, números de cartão de crédito, etc.) têm sido um dos principais fatores para a disseminação de softwares maliciosos. Garante também um melhor desempenho dos microcomputadores e da rede de dados que é bombardeada com geração de tráfego interno em casos de incidência de vírus e principalmente worms.

Buscamos com este processo modernizar nosso ambiente de proteção para estações de trabalho e servidores, e continuarmos com a manutenção desta importante linha de defesa, que em conjunto com outras soluções existentes sustentam os pilares da segurança da informação na CEDAE.

Nosso processo de pesquisa baseou-se em buscar fornecedores líderes de mercado, identificados pelo relatório do Gartner "Magic Quadrant for Endpoint Protection Platforms, Maio/2021".

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

3. ESPECIFICAÇÕES DO OBJETO

Para comprovação das funcionalidades descritas neste documento, será solicitado catálogo técnico da solução em português ou inglês, e documento constando análise ponto a ponto. Caso se faça necessário para comprovação, poderá ser solicitado ainda teste de bancada.

3.1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO ANTIVÍRUS

- A solução de segurança proposta deve ser fornecida por um único fabricante de modo que tanto o suporte à solução quanto as funcionalidades sejam inteiramente integradas, permitindo a correlação de eventos de segurança e gerenciadas através de uma única console de gerenciamento.
- Deverá atualizar a lista de ameaças cibernéticas conhecidas, pela rede, de preferência diariamente;
- Deverá proteger as estações de trabalho e servidores contra-ataques de criptografia (ransomware);
- Deverá fornecer manuais necessários à instalação, manutenção e utilização da solução, nos seguintes meios: papel, CD e ou Website em Inglês ou Português do Brasil;
- O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial;
- A solução deverá possuir filtro de reputação de websites e arquivos, ferramentas de varredura, detecção, análise e remoção de malware e riskware e demais formas de vírus e códigos maliciosos conhecidos, ameaças desconhecidas e ataques do tipo fileless (malware sem arquivo);
- Possuir console para monitoramento remoto com utilização de interface gráfica (GUI) ou browser para administração, monitoração e gerenciamento da solução ofertada que funcione em plataforma Windows.

3.2. FUNCIONALIDADES ESPECÍFICAS DA SOLUÇÃO ANTIVÍRUS

SUBSCRIÇÃO DE LICENÇAS DE USO PARA SOLUÇÃO ANTIVÍRUS (ESTAÇÕES DE TRABALHO)

- A solução deve atender os seguintes sistemas operacionais:
  - Windows 7 (Todas as versões);
  - Windows 8.1 (Standard, Pro e Enterprise);
  - Windows 10 (Todas as versões);
  - OS X 10.12 em diante;

- Funcionalidade de Administração e Gerência
  - A console de gerenciamento centralizado deverá estar disponível em nuvem e/ou on-premise;
  - Deve ser possível usar administração de forma híbrida;
  - Em caso de uso on-premise deve ser instalado em Windows 2012 Server ou superior, seja o servidor físico ou virtual;
  - Solução deve suportar base de dados Microsoft SQL Server;
  - A console de gerenciamento centralizado deve permitir a integração e correlação de eventos entre todos os componentes da solução ofertada;
  - A console de gerenciamento centralizada deve monitorar e administrar os módulos da solução descritos nos itens abaixo;
  - Deve gerenciar logs das atividades e eventos gerados pela solução;
  - Nas informações da política deve conter informações como nome, status, dono da política, horário e data da última alteração;
  - A gerência central deverá mostrar quais estações estão sem políticas;
  - Deve gerar relatório de compliance com informações de máquinas que nunca realizaram scan, políticas inconsistentes entre servidor/agente e componentes desatualizados;
  - Deve possuir integração com Microsoft Active Directory para acesso a console de administração;
  - Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de antimalware instalada;
  - Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
  - Deve permitir agrupamento automático de estações de trabalho da console de gerenciamento baseando-se no escopo do Active Directory ou IP;
  - Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
  - Deve permitir níveis de administração da console por usuários ou grupos de usuários;
  - Deve permitir a constituição de políticas genéricas aplicáveis a grupos de usuários ou máquinas;
  - Deve disponibilizar sua interface através dos protocolos http e https;
  - Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;
  - Deve gerar relatórios e gráficos pré-definidos nos formatos pdf, docx e xlsx;
  - Os relatórios devem conter informações de efetividade, ransomware, canais de infecção, principais usuários que receberam ameaças, vírus e spyware;
  - Deve permitir criação de modelos de relatórios customizados;

- Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;
- Deve permitir o controle individual de cada componente a ser atualizado;
- Deve permitir a definição de exceções por dias e horas para não realização de atualizações;
- Deve permitir ter como fonte de atualização um compartilhamento de rede em pelo menos um dos seguintes formatos: UNC, NFS e SMB;
- Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;
- Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;
- Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;
- Os métodos de envio suportados devem incluir ao menos duas das seguintes opções: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;
- Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;
- Deve permitir a escolha do intervalo de tempo necessário para que uma estação seja considerada off-line;
- Deve possuir a configuração do tempo de expiração da sessão dos usuários;
- Deve permitir a configuração do número de tentativas inválidas de login para o bloqueio de usuários;
- Deve possuir templates de acesso a console de gerenciamento;
- Deve permitir a configuração da duração do bloqueio;
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;
- Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;
- Deve permitir a criação de políticas de segurança personalizadas;
- Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;
- Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

- A solução deverá possuir um dashboard pré-configurado com informações sobre estações desatualizadas, usuários afetados, estações sem o antimalware instalado, estações afetadas, ameaças críticas tipo Ransomware, ameaças desconhecidas, vulnerabilidades e vazamento de dados;
- Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamento;
- A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;
- Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
- Deve possibilitar instalação "silenciosa";
- Deve permitir o bloqueio por nome de arquivo;
- Deve permitir o travamento de pastas e diretórios;
- Deve permitir o travamento de compartilhamentos;
- Deve permitir o travamento de portas via prevenção de epidemia;
- Deve permitir o rastreamento e bloqueio de infecções;
- Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho;
- Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
- Deve permitir a desinstalação através da console de gerenciamento da solução;
- Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
- Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;
- Deve permitir a deleção dos arquivos quarentenados;
- Deve permitir remoção automática da exibição na console de clientes inativos por determinado período de tempo;
- Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

- Deve registrar no sistema de monitoração de eventos da console de antimalware informações relativas ao usuário logado no sistema operacional;
- Deve prover ao administrador informações sobre quais estações de trabalho fazem parte do escopo de gerenciamento da console de antimalware e não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;
- Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;
- Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes;
- Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
- Deve permitir a criação de usuários locais de administração da console de antimalware;
- Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
- Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;
- Deve ser capaz de enviar eventos aos respectivos administradores de cada domínio definido na console de administração;
- Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
- Deve permitir atualização incremental da lista de definições de vírus;
- Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
- Deve permitir o rollback das atualizações das listas de definições de vírus e engines.

- Módulo de Proteção Anti-Malware
  - A solução de antimalware deve trabalhar de forma híbrida, fazendo uso de assinaturas, machine learning e detecção de comportamento para identificar malwares na estação de trabalho;
  - A solução deve possuir uma regra pré-definida para análise de malware consultando somente extensões comumente usadas por malware para otimizar o uso de recurso da estação de trabalho;

- Deve ser possível também definir quais extensões devem ser monitoradas de forma manual ou permitir ler todos os arquivos;
- Em caso de detecção a solução deve tomar uma das seguintes ações:
  - Liberar acesso;
  - Quarentenar;
  - Limpar;
  - Bloquear acesso;
  - Deletar;
  - Renomear;
- A solução deve permitir colocar pastas, programas ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso;
- Deve possuir a função SCAN CACHE, otimizando o scan nas máquinas armazenando informações dos arquivos que já são conhecidos como bons otimizando o uso de recurso;
- Deve ser possível alterar o período que o cache será armazenado para que seja criada uma nova base de assinaturas;
- Arquivos quarentemados devem ser possíveis de ser restaurados pela console central ou direto na estação de trabalho;
- Os arquivos quarentenados devem ser criptografados para evitar execução acidental e devem ser acessados com ferramenta provida pelo fornecedor;
- A solução deve permitir configurar scan baseado em assinaturas ou uso da inteligência na nuvem do fabricante;
- Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, ransomware e fileless, dentre outros;
- Em caso de cavalos de tróia a solução deve conseguir remover não só o malware mas também todos os processos criados por ele, recuperar alterações feitas em arquivos de sistema e deletar possíveis arquivos baixados pelo trojan;
- A solução deve permitir inspecionar o sistema operacional antes do boot em busca de malware “boot-type rootkits”;
- Para evitar falso positivos com spywares a solução deve permitir um modo de avaliação onde o administrador será notificado, porém as aplicações não são bloqueadas, permitindo criar uma whitelist antes de habilitar o bloqueio;

- Solução deve permitir conter surtos de malware na rede isolando a estação de trabalho infectada;
- O administrador deve ser notificado sobre surto na rede através do gerenciador central a partir de políticas definidas pelo administrador;
- A ação de isolamento da estação de trabalho deve ser executada pelo administrador na console central de gerenciamento;
- - Entre as ações tomadas pela contenção de surtos deve ser possível:
    - Limitar ou negar acesso a pastas compartilhadas;
    - Bloquear portas;
    - Negar escrita em arquivos e pastas;
    - Negar execução de arquivos executáveis (.exe);
- Deve ser possível notificar o usuário com uma mensagem customizada;
- A solução deve possuir um modulo de detecção de comportamento e análise de scripts, bloqueado ameaças conhecidas e potencialmente perigosas;
- Deve detectar scripts maliciosos mesmo quando executados por aplicações legítimas do Windows;
- A solução de antivírus deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos com a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
- Deve bloquear processos comuns associados a ransomware;
- Deve proteger contra exploits em arquivos executáveis e arquivos do pacote office;
- Deve realizar monitoramento da memória em tempo real para detecção de ataques fileless, sendo possível terminar os processos ou quarentenar para análise posterior;
- Deve realizar monitoramento de eventos na estação de trabalho que possam indicar um comportamento malicioso;
- Deve permitir monitorar ao menos os seguintes eventos:
    - Arquivos de sistema duplicados;
    - Modificação no arquivo hosts;
    - Novo plugin no Internet Explorer;
    - Alteração nas configurações do Internet Explorer;
    - Alteração nas políticas de segurança do Windows;
    - Injeção na biblioteca de programas;

- Modificação no shell;
- Novo serviço;
- Modificação em arquivo do sistema;
- Alteração na política de firewall;
- Alteração em processos do sistema;
- No programa na inicialização do sistema;

- Sempre que detectado um evento deve permitir no mínimo as seguintes opções:
  - Permitir;
  - Bloquear;
  - Perguntar quando necessário;
  - Avaliar;
- Deve ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas (zero-day) e suspeitas consultando modelos e características na nuvem do fabricante;
- O modulo de Machine Learning deverá funcionar em modo off-line caso o agente perca comunicação com a nuvem do fabricante, e deve retomar a conexão com a nuvem do fabricante de forma automática assim que tiver conexão disponível;
- Modulo de Machine Learning deve usar base do fabricante não sendo necessário que se faça uma base local nas estações de trabalho ou no servidor de gerenciamento centralizado visando reduzir o número de falso positivos;
- O modulo de Machine Learning deve monitorar arquivos e processos;
- O modulo de Machine Learning deve funcionar para análise estática o arquivo e em execução para evitar ofuscação de código malicioso;
- Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;
- Deve permitir configurar aos menos os seguintes tipos de varredura:
  - Manual;
  - Agendado;
  - Tempo-real;
- Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual e agendada;
- A solução deve possuir modulo de proteção contra alteração dos arquivos e serviços usados pelo agente de proteção.

- Funcionalidade de reputação web
  - A solução deve prover proteção web sem necessidade de instalação de plug-ins nos navegadores;
  - Deve suportar ao menos os seguintes navegadores:
    - Google Chrome;
    - Mozilla Firefox;
    - Microsoft Edge;
    - Safari
  - Solução deve detectar site malicioso através da reputação em nuvem do fabricante;
  - Solução deve permitir liberar ou bloquear acesso aos sites de baseado na pontuação atribuída pelo fabricante;
  - O modulo deve bloquear também tentativas de exploits através de sites maliciosos;
  - O modulo deve bloquear uso de scripts ou applets maliciosos através do navegador;
  - A pontuação do fabricante deve conter ao menos 3 níveis:
    - Sites perigosos;
    - Sites perigoso e altamente suspeitos;
    - Sites perigos, altamente suspeitos e suspeitos;
  - Deve ser possível bloquear sites que ainda não foram avaliados pelo fabricante;
  - A solução deve conseguir validar sites que usem protocolo HTTPS;
  - Deve ser possível criar uma whitelist para bypassar a análise do módulo de reputação web para evitar falsos positivos;
  - Deve ser possível habilitar um módulo de avaliação para evitar falsos positivos;
  - A solução deve detectar conexões com IPs conhecidos de C&C e bloquear a conexão em máquinas Windows;
  - Sempre que houver uma detecção de malware na estação de trabalho a solução deve fazer uma checagem para ver se o malware em algum momento se comunicou com uma C&C em máquinas Windows;

- Funcionalidade de controle de dispositivos e proteção de dados
  - Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, modificar, listar o conteúdo e bloqueio total;
  - Desejável possuir o controle a drives mapeados com as seguintes opções: acesso total, modificar, leitura e execução, apenas leitura e listar somente o conteúdo;

- Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com uma política aplicada;
- Possibilidade de adicionar novos dispositivos na lista de dispositivos permitidos utilizando “Class ID”, “Device ID” ou “Serial ID” do dispositivo;
- A solução deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;
- A proteção contra vazamento de dados deverá verificar o true file type a fim de impedir que o usuário tente burlar a segurança;
- Deve permitir a criação de modelos personalizados para identificação de informações;
- Deve permitir mais de uma ação para cada política, como: Apenas registrar o evento da violação, bloquear a transmissão, gerar alerta para o usuário, alertar na central de gerenciamento e solicitar uma justificativa para o usuário;
- A proteção contra vazamento de dados deve possuir a capacidade de realizar uma busca de arquivos baseado em computadores selecionados baseados em template.

- Funcionalidade de Host Firewall e HIPS
  - Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;
  - As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;
  - Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
  - Deve permitir ativar e desativar o produto sem a necessidade de remoção;
  - Deve permitir que os administradores habilitem ou desabilitem as regras de IPS;
  - Deverá possuir a possibilidade de configurar níveis diferentes de segurança para o firewall podendo ser eles alto, médio e baixo;
  - Deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Tiny Fragment Attack, Fragmented IGMP e Land Attack;
  - A funcionalidade de HIPS deverá possuir perfis pré-derteminados baseados em performance e segurança;
  - A funcionalidade de HIPS deverá possuir regras para proteger contra ameaças do tipo Ransomware;

- A funcionalidade de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

- Módulo para controle de aplicações
  - As regras de controle de aplicação devem permitir as seguintes ações: liberar e bloquear;
  - A regra com permissão de liberar aplicações deve possuir as seguintes funcionalidades: permitir a execução de processos externos, não permitir a execução de processos externos e herdar direitos de execução;
  - O módulo de controle de aplicações deve permitir importar e exportar regras;
  - As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
  - As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: Assinatura sha-1 e sha-256 do executável;
  - Atributos do certificado utilizado para assinatura digital do executável, Caminho lógico do executável, Base de assinaturas de certificados digitais válidos e seguros;
  - As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;
  - As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;
  - O modulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento;

- Funcionalidade de criptografia
  - Deve possuir as seguintes funcionalidades de criptografia para as estações de trabalho (desktops e notebooks): Disco completo (fde – full disk encryption);
  - Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;
  - A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;
  - Deve possuir suporte ao algoritmo de criptografia aes-256;
  - Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;
  - Deve possuir funcionalidade de criptografia por software ou hardware;
  - Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2;

- Deve possuir compatibilidade de autenticação por múltiplos fatores;
- Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;
- Deve possuir políticas por usuários, grupos e dispositivos;
- Deve possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;
- Deve possuir mecanismos para wipe (limpeza) remoto;
- Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);
- Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;
- Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;
- Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;
- Deve possibilitar que cada política tenha uma chave de criptografia única;
- Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:
- Chave do usuário: somente o usuário tem acesso aos arquivos;
- Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos
- Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;
- Deve possuir integração com o Gerenciamento Centralizado para visibilidade dos dispositivos criptografados e criação de política;

SUBSCRIÇÃO DE LICENÇAS DE USO PARA SOLUÇÃO ANTIVÍRUS (SERVIDORES)

- Deverá ser compatível com no mínimo os sistemas operacionais:
  - Windows:
    - Windows Server 2003 R2 SP2 (32/64-bit);
    - Windows Server 2008 (32/64-bit);
    - Windows Server 2008 R2 (64-bit);
    - Windows Server 2012 (64-bit);
    - Windows Server 2012 R2 (64-bit);
    - Windows Server Core 2012 (64-bit);

- Windows Server Core 2012 R2(64-bit);
- Windows Server 2016 (64-bit);
- Windows Server 2019 1809 (64-bit) e posteriores;

- Linux:
  - Red Hat Enterprise Linux 5 (32-bit);
  - Red Hat Enterprise Linux 6 (32/64-bit);
  - Red Hat Enterprise Linux 7 (64-bit);
  - Red Hat Enterprise Linux 8 (64-bit) e posteriores;
  - CentOS 5 (32/64-bit);
  - CentOS 6 (32/64-bit);
  - CentOS 7 (64-bit);
  - CentOS 8 (64-bit) e posteriores;
  - Oracle Linux 5 (32/64-bit);
  - Oracle Linux 6 (32/64-bit);
  - Oracle Linux 7 (64-bit);
  - Oracle Linux 8 (64-bit) e posteriores;
  - SUSE Linux Enterprise Server 11 (32/64-bit);
  - SUSE Linux Enterprise Server 12 (64-bit) e posteriores;
  - Ubuntu 10.04 LTS (64-bit);
  - Ubuntu 14 (64-bit);
  - Ubuntu 16 (64-bit);
  - Ubuntu 18.04 (64-bit);
  - Ubuntu 20.04 (64-bits) e posteriores;
  - Debian 7 (64-bit);
  - Debian 8 (64-bit);
  - Debian 9 (64-bit);
  - Debian 10 (64-bit) e posteriores;

- Deverá ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes:
  - Hyper-V
  - Vmware

- Red Hat Virtualization – RHV

- Deverá permitir gerenciar políticas de segurança em múltiplas plataformas e sistemas operacionais, para hosts físicos e virtuais, todos em uma única console centralizada e do mesmo fabricante;
- Deverá permitir no mínimo a aplicação de regras de IPS/IDS e antimalware para hosts gerenciados de Docker container;
- Deverá possuir gerenciamento de todos os eventos relativos aos hosts gerenciados possibilitando, além do armazenamento dos eventos na própria solução, o seu encaminhamento para uma solução de SIEM;
- Desejável ter a capacidade de se integrar com os principais softwares de SIEMs de mercado, no mínimo com: Ossim, IBMQradar, Splunk e ArcSight, de modo a permitir enviar os seus logs para essas soluções;
- Deverá possibilitar enviar logs para SYSLOG servers;
- Deverá suportar o uso de RESTful API para permitir a integração com outras aplicações;
- Deverá suportar o uso de RESTful API para permitir automatizações operacionais de tarefas;
- O uso de RESTful API deve suportar no mínimo as seguintes automatizações:
  - Executar tarefas de manutenção de rotina;
  - Configurar políticas e proteger servidores;
  - Pesquisar políticas por nome
- Configurações de proteção antimalware:
  - Definir as configurações da varredura antimalware em tempo real;
  - Configurar exclusões de diretório para uma configuração de varredura de malware;
  - Obter as configurações antimalware de todos os servidores;
  - Gerar relatório referente ao status do módulo;
- Configurações de proteção contra URLs maliciosas:
  - Ativar a proteção contra URLs maliciosas;
  - Definir configurações;
  - Gerar relatório referente ao status do módulo;
- Configurações de controle de firewall de host:
  - Configurar firewall;
  - Realizar pesquisa de regra de firewall por nome;
  - Gerar relatório referente ao status do módulo;

- Configurações de proteção contra exploração de vulnerabilidades:
  - Definir configurações de prevenção de intrusões;
  - Realizar busca para identificar regra de prevenção de intrusões para uma CVE;
  - Realizar busca para identificar regra servidores que não estão protegidos contra uma CVE;
  - Descobrir e aplicar automaticamente regras IDS/IPS que blindem exploração das vulnerabilidades existentes no sistema operacional e aplicações;
  - Gerar relatório referente ao status do módulo;
- Configurações do monitoramento de integridade e rastreabilidade:
  - Adicionar regras de monitoramento de integridade e rastreabilidade a uma política;
  - Gerar relatório referente ao status do módulo;
- Configurações da inspeção de log:
  - Adicionar regra de inspeção de log a uma política;
  - Criar uma regra de inspeção de log;
  - Gerar relatório referente ao status do módulo;
- Configurações de controle de aplicação:
  - Ativar controle de aplicações;
  - Bloquear softwares não reconhecidos;
  - Ativar o modo de manutenção;
  - Gerar relatório referente ao status do módulo;
  - Gerar relatório sobre o status do agente;
  - Gerar script de instalação do agente;
  - Autenticação – Log in e Log out;
  - Administração de Contas - Criação, edição e exclusão de contas de acesso;
  - Monitoração de Status - Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks;
- A solução deverá permitir a entrega de agentes por pelo menos uma dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet.

- Proteção antimalware
  - Deverá possuir proteção antimalware baseada em agente;

- Deverá possuir proteção antimalware com serviço de reputação externa através de nuvem de inteligência do próprio fabricante;
- Deverá possuir validação reputacional estendida com prevalência e contador de execuções;
- Deverá possuir proteção antimalware convencional com padrões locais;
- Deverá suportar proteção antimalware sem agente baseado em Vmware API (NSX-V);
- Deverá possibilitar realizar a varredura de arquivos sem utilização de agente, evitando a varredura de conteúdos duplicados (VMware Scan Cache);
- Deverá possibilitar configurar cache de varredura e exclusões para varreduras sem agente;
- Deverá ser compatível com no mínimo os seguintes sistemas operacionais: Windows Server 2008 (32/64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit); Windows Server 2012 R2 (64-bit); Windows Server 2016 (64-bit) e Windows Server 2019.
- A solução deve possuir um cache dos arquivos verificados de modo a evitar a redundância da varredura;
- O cache de arquivos verificados deverá estar disponível para varredura sob demanda e varredura em tempo real;
- Deverá possibilitar ao administrador liberar os arquivos quarentenados tanto no modo sem agente quanto no modo com agente;
- Deverá possuir proteção em tempo real;
- Deverá possibilitar diferentes configurações de detecção (varredura ou rastreamento):
  - Manual;
  - Agendado;
- Deverá possibilitar configurar o modo de I/ O para proteção em tempo real:
  - Escrita / leitura;
  - Somente escrita;
  - Somente leitura;
- Deverá possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar impactos de performance no host;
- Deverá possuir análise de comportamento visando identificar ameaças desconhecidas;
- Deverá possuir proteção contra ransomware utilizando de gatilhos do sistema em tentativas de criptografia;
- Deverá realizar backup dos arquivos afetados por tentativas de criptografia, possibilitando a restauração assim que o sistema for limpo;

- A solução deve ter capacidade de monitorar processos legítimos contra realizações de ações que não são tipicamente realizadas pelos mesmos, a fim de detectar e bloquear ameaças;
- Deverá realizar varredura de arquivos de pré-execução utilizando machine learning;
- Deverá identificar CVE de dia zero em documentos office e PDF;
- Deverá possuir proteção contra spyware;
- Deverá realizar varredura de arquivos comprimidos;
- Deverá ser possível configurar os níveis de camadas de compressão para a varredura de arquivos comprimidos;
- Deverá ser possível configurar no mínimo 5 (cinco) camadas;
- Deverá realizar varredura de arquivos comprimidos do tipo OLE, sendo possível configurar as camadas de compressão;
- Deverá realizar a varredura de pastas de rede;
- A solução deverá possibilitar a criação de listas de inclusão para que o processo do antivírus execute a varredura de determinados diretórios e arquivos;
- A solução deverá possibilitar a criação de listas de exclusão para que o processo do antivírus não execute a varredura de determinados diretórios e arquivos;
- Deverá permitir configurar o consumo de CPU que será utilizado para varredura manual e/ou agendada;
- Deverá suportar processamento multitarefa;

- Proteção contra URL`s maliciosas
  - Deverá possuir proteção baseada em agente contra acesso a URLs maliciosas utilizando classificação de reputação;
  - Deverá suportar proteção contra URLs maliciosas antimalware sem agente baseado em Vmware API(NSX-V);
  - Deverá possuir limiares configuráveis para bloquear o controle de sensibilidade;
  - Deverá possuir porta configuráveis para controle de atividade da web;
  - Deverá possibilitar criar blacklist e whitelist de URLs:
    - Domínio;
    - URL;
    - Palavras-chaves;
  - Deverá possuir serviços de reputação configuráveis para lidar com solicitações (global ou local);

- O serviço de reputação e a base de reputação devem ser do mesmo fabricante que provê a solução de proteção de servidores;
- Deverá possibilitar configurar a engine:
  - Inline;
  - Tap – possibilitando realizar testes;

- Firewall de host
  - Deverá trabalhar como firewall de host, através da instalação de agente nos servidores protegidos;
  - Deverá ter a capacidade de controlar o tráfego baseado no endereço MAC, frame types, tipos de protocolos, endereços IP e intervalo de portas;
  - Deverá ter a capacidade de definir regras distintas para interfaces de rede distintas;
  - Deverá ter a capacidade de controlar conexões TCP baseado nas Flags TCP;
  - Deverá ser capaz de reconhecer e possibilitar o bloqueio de endereços IP que estejam realizando network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint;
  - Deverá ter a capacidade de implementação de regras em determinados horários, customizados pelo administrador;
  - Deverá ter a capacidade de definição de regras para contextos específicos;
  - Deverá ter a capacidade de realização de varredura de portas nos servidores;
  - As regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
  - As regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
  - Para facilitar a criação e administração de regras de firewall, as mesmas poderão ser baseadas em objetos que podem ser lista de IPs e lista de portas;
  - Deverá ser stateful bidirecional;
  - Deverá permitir liberar ou apenas logar eventos;
  - Deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
  - Deverá possuir as seguintes ações, ou equivalentes: permitir, apenas logar, bloquear, bypass e forçar permissão;

- Deverá utilizar o conceito de regras implícitas para as regras de permissão, negando o tráfego para todo o restante que não estiver liberado;
- As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
- Deverá realizar pseudo stateful em tráfego UDP;
- Deverá logar a atividade stateful;
- Deverá permitir limitar o número de conexões de entrada e o número de conexões de saída de um determinado servidor;
- Deverá prevenir ack storm;
- Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
- Poderá atuar no modo inline para proteção contra ataques ou modo escuta para monitoração e alertas;

- Proteção contra exploração de vulnerabilidades
  - Deverá possuir proteção contra exploração de vulnerabilidades baseada em agente;
  - Desejável suportar proteção contra exploração de vulnerabilidades e sem agente baseado em Vmware API (NSX-V); não sendo nesse caso, necessário inspecionar tráfego de entrada SSL;
  - Deverá detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e aplicações;
  - Deverá realizar auditoria automática do servidor protegido (agendada e manual), detectando o tipo e versão do sistema operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem exploração das vulnerabilidades existentes no sistema operacional e aplicações.
  - Deverá definir e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (no caso de a vulnerabilidade já ter sido solucionada, a regra deverá ser removida automaticamente; e vice-versa). As regras deverão ser ativadas para as vulnerabilidades recém-descobertas e sistema sendo protegido por patch virtual.
  - Deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;
  - Deverá detectar conexões maliciosas, com a possibilidade de bloquear esta conexão.

- A opção de detecção e bloqueio deverá possibilitar ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;
- Deverá possuir regras de defesa para blindagem de vulnerabilidades e ataques que explorem os sistemas operacionais supracitados e regras para aplicações/serviços padrões de mercado, incluindo Microsoft IIS, DNS, SQL Server, Microsoft Exchange, Oracle Database,PostgreSQL, Adobe Acrobat, Tomcat,Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Red Hat Jboss, JAVA, PHP, Wordpress, Weblogic, soluções de backup, bibliotecas linux, Citrix, e Web Server Apache;
- Deverá realizar o armazenamento do pacote capturado quando detectado um ataque;
- Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações próprias;
- Deverá detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e mensagens instantâneas;
- Deverá detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting.
- Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
- Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
- Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- Deverá possibilitar permitir ou bloquear métodos utilizados por Webservers por regras de IPS;
- As regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- As regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
- Deverá ser capaz de inspecionar tráfego de entrada SSL;
- Deverá apresentar informações detalhadas das regras de proteção contra vulnerabilidades, contendo links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante e CVE relacionado;

- Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
- Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
- Deverá possibilitar habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para realizar análise;
- As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- Deverá ser possível configurar o modo de detecção, possibilitando apenas detectar ou bloquear os eventos que violem as regras, de modo que o administrador possa optar por qual ação tomar;
- As regras de proteção de vulnerabilidade deverão:
- Apresentar severidade baseada em CVE's;
- Apresentar CVE relacionado a vulnerabilidade e/ou a regra de IPS;
- Ter capacidade de LOG desabilitado;
- Quando disparadas poderão ter a possibilidade de emitir um alerta;
- Ser atualizadas automaticamente pelo fabricante;
- Deverá ser possível configurar o modo de detecção, possibilitando atuar no modo em linha para proteção contra ataques e modo escuta para monitoração e alertas;

- Monitoramento de integridade e rastreabilidade
  - Deverá possuir monitoramento de integridade e rastreabilidade baseada em agente;
  - Desejável suportar monitoramento de integridade e rastreabilidade sem agente baseado em Vmware API (NSX-V);
  - Desejável que a solução permita o monitoramento de integridade de arquivos na máquina virtual (VMWARE) a ser monitorada;
  - O monitoramento de integridade e rastreabilidade deverá ser realizado em tempo real;
  - Deverá detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações terceiras;
  - Deverá detectar mudanças no estado de portas em sistemas operacionais Linux;

- Deverá monitorar o status de serviços e processos do sistema operacional;
- Deverá monitorar mudanças efetuadas no registro do Windows;
- Deverá possibilitar customização de regras para monitoramento de integridade e rastreabilidade em chaves de registro, diretórios e subdiretórios;
- Deverá possibilitar customização de XML para criação de regras monitoramento de integridade avançadas;
- Deverá realizar auditoria no sistema operacional e aplicações (agendada e manual), para destacar e atribuir automaticamente a regra relevante para monitoramento de integridade de acordo com o resultado dessa auditoria;
- Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);
- Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
- A solução deverá monitorar modificações em arquivos, pastas, registros, processos, serviços e portas;
- Deverá possibilitar o rastreamento de arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;
- Deverá possibilitar gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;
- Deverá ser possível gerar relatório de todas as modificações que ocorram nos objetos monitorados;
- Deverá classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- Deverá possibilitar definir o diretório onde o arquivo será monitorado, possibilitando inclusão ou não de determinados tipos de arquivos dentro desse mesmo diretório;
- As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- Deverá possibilitar classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

- Inspeção de Logs
  - Deverá monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, armazenando uma cópia desses logs em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
  - Deverá realizar auditoria no sistema operacional e aplicações (agendada e manual), para destacar e atribuir automaticamente a regra relevante para inspeção de logs de acordo com o resultado dessa auditoria;
  - Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);
  - Deverá permitir customização de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
  - Deverá permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
  - Deverá possuir inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente e/ou do servidor;
  - Deverá permitir modificar as regras por severidade de ocorrência de eventos;
  - Deverá suportar sintaxe OSSEC padrão aberto;
  - Deverá suportar tipos comuns de log de eventos (log de eventos, snort, syslog e outros ...)
  - Deverá possuir decodificadores predefinidos para tipos comuns de log de eventos com base no regex;

- Controle de Aplicações
  - Deverá realizar inventário de softwares instalados e criar um conjunto de regras local e/ou um conjunto de regras compartilhado via API;
  - Deverá possuir as seguintes configurações ou semelhante:
  - Bloqueio: possibilitando o bloqueio de aplicações, impedindo a execução de todos os softwares novos ou alterados, a menos que sejam expressamente permitidos;
  - Permitido: possibilitando que aplicações sejam executadas por padrão, a menos que que sejam expressamente bloqueadas;
  - Deverá possuir lista de permissões de inventário, ou seja, ao ativar o controle de aplicações, todos os softwares atualmente instalados devem ser adicionados à lista de permissões do inventário do servidor e pode ser executado;

- Deve ser possível configurar modo de manutenção possibilitando instalar ou atualizar a lista de softwares permitidos na lista de inventário;
- Deverá monitorar continuamente o servidor quanto as alterações. Devendo ser integrado ao kernel e ao sistema de arquivos, monitorando todo o servidor, incluindo o software instalado pelas contas root e de administrador.
- Deverá detectar novos softwares, comparando hash, tamanho do arquivo, nome do arquivo e pasta;
- Deve também realizar o controle de aplicativos em:
- Aplicações Windows (.exe, .com, .dll, .sys), bibliotecas Linux (.so) e outros binários e bibliotecas compilados
- Arquivos Java .jar e .class e outro código de bytes compilado
- Scripts PHP, Python e shell, além de outros aplicativos e scripts da web que são interpretados ou compilados em tempo real
- Scripts do Windows PowerShell, batch (.bat) e outros scripts específicos do Windows (.wsf, .vbs, .js)
- Deverá exibir todos os softwares não reconhecidos, ou seja, softwares que não estão na lista de permissões de inventário de um servidor e não possuem uma regra de controle de aplicação correspondente, possibilitando tomar a ação de "Permitir" ou "Bloquear".

- Funcionalidades de Gerenciamento
  - A solução deverá ser gerenciada por console Web, devendo suportar certificado digital para gerenciamento;
  - O gerenciamento da console web deverá suportar no mínimo os navegadores Firefox, Internet Explorer, Microsoft Edge, Google Chrome e Apple Safari;
  - Em ambiente on-premises, a console de gerenciamento deverá ser compatível de instalação no mínimo nos seguintes sistemas operacionais:
    - Windows 2008 R2
    - Windows 2012
    - Windows 2012 R2
    - Windows 2016
    - Windows 2019
    - RHEL 5
    - RHEL 6

- RHEL 7
- RHEL 8

- A console de gerenciamento deverá disponibilizar os pacotes de instalação de agentes para todos os sistemas operacionais suportados, provendo inclusive scripts de instalação de agents (power shell script e bash script);
- Deverá permitir o envio de notificações via SMTP;
- Deverá permitir o envio de registros de logs a um servidor remoto;
- Deverá suportar o envio ao menos nos seguintes formatos: Raw Syslog, CEF e LEEF;
- Deverá suportar integração com serviços de terceiros baseando-se em SAML 2.0 para serviços como ADFS, Okta, PingOne entre outros;
- Desejável suportar APIs abertas para integração com serviços de terceiros;
- A comunicação entre a console de gerenciamento e componentes de proteção deverá ser criptografada;
- Deverá armazenar os eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;
- Deverá permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;
- A console de gerenciamento deverá permitir alta disponibilidade em nível de aplicação, através da criação de várias consoles, de modo que na ausência da principal, os agentes automaticamente se comuniquem com a secundária e com todas as configurações preservadas;
- Quando operadas em modo alta disponibilidade, as consoles devem compartilhar o mesmo banco de dados;
- Deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
- A console deverá ter a capacidade de se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;
- A console deverá permitir que os usuários recebam determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

- Quando o acesso for configurado em modo parcial, este deve permitir que um usuário possa gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível editar ou criar novas políticas de segurança;
- Deverá permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;
- Deverá armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados:
  - PostgreSQL
  - Microsoft SQL Server
  - Oracle database;
- Deverá permitir a definição de permissionamento, no mínimo, para os modos de visualização e edição de políticas;
- Deverá permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;
- Deverá possuir dashboards para facilidade de monitoração, as quais poderão ser customizados pelo usuário em quantidade de dashboards e período de monitoração;
- Deverá ser possível criar políticas de forma global para todas os servidores, por perfis e individualmente para cada host;
- Deverá permitir a criação/utilização de tags pré-definidas para o agrupamento e aplicação de políticas aos hosts segundo características comuns;
- Deverá permitir o envio de eventos da console via SNMP;
- Permitir o rollback de atualização de regras pela console de gerenciamento;
- Deverá gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- Deverá possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;
- Deverá classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.
- Deverá permitir o gerenciamento agrupando os hosts em pastas inteligentes, possibilitando organização de grupos de hosts para a aplicação de políticas. O agrupamento de hosts deverá ser no mínimo pelos seguintes parâmetros:
  - Hostname;
  - Sistema Operacional;

- Docker Host;
- Política de Configurações;
- Active Directory Name/Folder.

3.3. SERVIÇO DE TREINAMENTO PARA SOLUÇÃO ANTIVÍRUS

- O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela contratada;
- O treinamento deverá englobar a realização de laboratórios práticos, fornecidos pela CONTRATADA, para configuração e execução de exercícios práticos na mesma versão dos produtos ofertados;
- O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, administração, backup e restauração de configuração, gerenciamento, resolução de problemas, utilização da solução e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE;
- Deverá contemplar todos os recursos e configurações existentes na solução ofertada;
- O treinamento será direcionado aos técnicos da CONTRATANTE, deverá ser focado na solução adotada, de forma que haja transferência do conhecimento dos recursos, configurações existentes e sua utilização;
- Deverá ser entregue para a contratante a proposta com o conteúdo do treinamento;
- É de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou indiretas;
- O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso;
- A carga horária será de até 40 (quarenta) horas para até 1 turma de até 8 (oito) alunos;
- Os treinamentos deverão ser realizados em dias úteis e não poderão exceder o horário comercial;
- Os horários e datas dos treinamentos serão definidos pela equipe técnica da Contratante e comunicados a Contratada com antecedência de 10 (dez) dias;
- A Contratante reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo, caso não seja satisfatório;
- Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração emitida pelo fabricante;
- Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

3.4. SERVIÇO DE SUPORTE TÉCNICO PARA SOLUÇÃO ANTIVÍRUS - REMOTO 24X7

- O suporte técnico será remoto, com período de disponibilidade de 24 horas por dia, 7 dias por semana;
- Em caso de interrupção ou indisponibilidade do serviço, a contratada se compromete a realizar as correções necessárias à reativação do serviço e a prevenção de novas interrupções, respeitando os prazos de atendimento;
- Entende-se por "indisponibilidade total" quando os serviços não estão acessíveis, e "indisponibilidade parcial" quando há degradação dos serviços;
- A abertura de chamados de suporte deve possibilitar, no mínimo, os seguintes métodos: via telefone, e-mail, website do fornecedor;
- Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail, website do fornecedor;
- Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais ao CONTRATANTE, além do contratado, salvo se o problema não estiver relacionado ao objeto do contrato;
- Entende-se por manutenção corretiva uma série de procedimentos destinados a recolocar a solução em pleno estado de funcionamento, removendo definitivamente os defeitos apresentados;
- Entende-se por manutenção evolutiva o fornecimento de novas versões e/ ou releases corretivas e/ou evolutivas de softwares que compõem a solução corporativa do software, lançadas durante a vigência do contrato;
- Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;
- A CONTRATADA deverá manter registro de todo o serviço de manutenção e garantia executado, que poderá ser solicitado a qualquer tempo pela contratante;
- A contratante poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A contratada deverá possuir contrato de suporte técnico com o fabricante do produto oferecido, a fim de garantir o serviço prestado;
- Todos os chamados abertos, por qualquer meio, deverão ser registrados via sistema, e ao final de cada mês será emitido um relatório gerencial e um relatório técnico com todas as informações sobre os atendimentos realizados;
- A contratada deverá manter histórico de cada atendimento de suporte realizado, contendo a identificação do problema, providências adotadas e demais informações pertinentes;

- A contratada será responsável por possíveis migrações para novas versões da solução oferecida, sempre que demandadas pelo contratante.
- Não haverá limitação imposta para a quantidade de horas e a quantidade de chamados abertos, podendo a CONTRATANTE abrir quantidade ilimitada de requisições para a CONTRATADA ao longo do contrato.
- Quando não houver possibilidade de acesso remoto, ou que este não possibilite a execução das atividades necessárias, o atendimento deverá ser realizado nas instalações da CONTRATANTE.

4. INSTALAÇÃO E CONFIGURAÇÃO

- A CONTRATADA deve realizar, nas dependências da CONTRATANTE, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) em conjunto com as áreas de Segurança da Informação e infraestrutura da Contratada para definir o Plano de Trabalho de instalação e configuração da solução;
- Após a reunião de kick-off deve ser produzida uma ata, assinada por todos os participantes da CONTRATADA e da CONTRATANTE presentes, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da equipe do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratada;
- Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, se assim for o caso;
- A etapa de instalação e configuração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE;
- Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de testes, implantação e migração, definidos pela CONTRATANTE;
- As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana;
- Durante a etapa de instalação e configuração, os produtos fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção;

- A CONTRATADA deverá, com a supervisão e aprovação da CONTRATANTE, planejar e realizar a instalação e configuração dos softwares com total interoperabilidade no ambiente atual da CONTRATANTE, sem impacto no ambiente de produção;
- Durante a implantação e integração, caso seja necessário, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança;
- Para instalação e configuração devem ser consideradas as seguintes premissas:
- Caberá a CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação dos PRODUTOS;
- Caberá a CONTRATADA disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.
- A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação e ao pleno funcionamento do ambiente de produção.

5. ESPECIFICAÇÃO DO SERVIÇO

Item	Código IFS	ESPECIFICAÇÃO DO SERVIÇO	UNID	QUANT
01	**2110010075**	*Subscrição de licença de uso para solução Antivírus (estações de trabalho) Fornecimento: 36 meses*	UN	2600
02	**2110010076**	*Subscrição de licença de uso para solução Antivírus (Servidores) Fornecimento: 36 meses*	UN	300
03	**2110010077**	*Serviço de suporte técnico para solução Antivírus (Estações de trabalho e Servidores), remoto 24x7 Fornecimento: 36 meses*	UN	1
04	**2110010070**	*Serviço de treinamento para solução Antivírus (Estações de trabalho e Servidores)*	Turma	3

6. CRITÉRIO DE JULGAMENTO DA PROPOSTA

- Será considerado vencedor o licitante que apresentar o menor valor total para o objeto deste Termo de Referência

7. TIPO DE CONTRATAÇÃO E REGIME/FORMA DE EXECUÇÃO/FORNECIMENTO

7.1. (_X_) SERVIÇO:

- **(_X_) de natureza contínua;**
- **(_X_) sem mão de obra alocada;**
- **(_X_) Regime de execução por preço global;**

8. PRAZO DA PRESTAÇÃO DO SERVIÇO

- O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir do dia seguinte da autorização expressa expedida pela CEDAE (Ordem de Início), que será emitida após a publicação do extrato do instrumento no Diário Oficial.
- O prazo de vigência do contrato poderá ser prorrogado, observando-se o limite previsto no art.71, da Lei nº 13.303/16.

9. LOCAL DE EXECUÇÃO

- Os softwares deverão ser instalados no CPD do Prédio Sede da CEDAE, localizado na Av. Presidente Vargas, nº 2.655 - Térreo, Cidade Nova - Rio de Janeiro, RJ no horário das 08:00 às 17:00 h.
- Os serviços serão executados no endereço acima mencionado.

10. CONDIÇÕES DE RECEBIMENTO:

- Será observada, no que couber, a Ordem de Serviço "E" nº 14.693 de 23 de maio de 2017, que estabelece os procedimentos para a emissão provisória e definitiva para os contratos administrativos celebrados com a CEDAE, cujas cláusulas se encontram estabelecidas no edital de licitação.

11. GARANTIA:

- A garantia do fabricante será de 36 (trinta e seis) meses contados a partir da data da entrega das licenças da solução de segurança;
- A garantia do fabricante dos produtos fornecidos deverá obrigatoriamente prover:
    - Atualização dos softwares fornecidos, se novas versões forem disponibilizadas.
    - Atualização dos softwares, se houver lançamento de novos softwares em substituição aos fornecidos, o mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.
- As atualizações acima referidas devem ser implementadas mediante aprovação da contratante;
- A solução completa que atenda a este item e sua garantia devem ser de um único fabricante, de forma a garantir a integração, padronização e prover a otimização dos recursos de gerenciamento necessários.

12. FORMA E CONDIÇÕES DE PAGAMENTO

- A CEDAE pagará mensalmente, em 36 parcelas, à CONTRATADA, o valor dos serviços contínuos executados no período, de acordo com o cronograma físico financeiro do contrato, na forma e demais condições estabelecidas no edital
- A CONTRATADA deverá encaminhar a fatura para pagamento à CEDAE, dando entrada pelo Protocolo do mesmo.
- O prazo de pagamento será de até 30 (trinta) dias, a contar da data final do período de adimplemento de cada parcela.
- O Pagamento do Treinamento dar-se-á, 30 dias após a emissão da nota fiscal e devidamente atestada pela comissão de fiscalização;

13. OBRIGAÇÕES DA CONTRATADA

- Manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da execução dos serviços, objeto desta contratação.
- Responsabilizar-se por todos os ônus referentes aos serviços.
- Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CEDAE.
- Responsabilizar-se por qualquer prejuízo caudado à CEDAE, a seus prepostos ou a terceiros, provocados por ação ou omissão da CONTRATADA, em decorrência de falhas ou imperfeições na execução dos serviços.
- Responsabilizar-se pelos eventuais danos ou desvios causados aos bens que lhe forem confiados, devendo efetuar o ressarcimento correspondente, imediatamente após o recebimento da notificação expressa da Administração, sob pena de glosa de qualquer importância que tenha direito a receber.
- Garantir absoluto sigilo sobre todos os processos, informações e quaisquer outros dados disponibilizados pela CEDAE, em função das peculiaridades dos serviços a serem prestados.

- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades, objeto deste projeto básico, sem prévia autorização da CEDAE.
- Esclarecer em tempo hábil eventuais dúvidas e indagações da CEDAE.
- Comunicar ao gestor do contrato, designado formalmente pela CEDAE, qualquer fato extraordinário ou anormal que ocorra durante a vigência do contrato.
- Exigir dos seus empregados, quando em serviço nas dependências da CEDAE, o uso obrigatório de uniformes e crachás de identificação.
- Apresentar as informações detalhadas dos serviços disponibilizados e as restrições porventura existentes.
- Refazer os serviços que foram executados de maneira incorreta ou insatisfatória, sem ônus para a CEDAE.
- Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, os componentes, como também o equipamento em que se verificarem vícios, defeitos ou incorreções resultantes da fabricação, da execução do serviço de assistência técnica ou de materiais empregados.

14. OBRIGAÇÕES DA CONTRATANTE

- Cumprir com os compromissos financeiros assumidos com a empresa a ser CONTRATADA, de acordo com o contrato, mediante as notas fiscais/faturas devidamente atestadas comprovando a correta prestação do serviço.
- Fornecer e colocar à disposição da CONTRATADA, todos os elementos e informações que se fizerem necessários à prestação do serviço, conforme especificado neste equipamento.
- Notificar, formal e tempestivamente, a CONTRATADA sobre quaisquer irregularidades observadas na prestação dos serviços.
- Notificar a CONTRATADA, por escrito e com antecedência mínima de 72 horas sobre multas, penalidades e quaisquer débitos de sua responsabilidade.
- Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com os termos de sua proposta comercial, do contrato e do edital de licitação.
- Permitir o livre acesso dos empregados da CONTRATADA às dependências da CEDAE para execução dos serviços.

- Prestar as informações e os esclarecimentos relativos ao objeto do contrato, que venham a ser solicitados pela CONTRATADA.
- Promover, caso necessário, auditoria técnica e operacional do ambiente e recursos utilizados pela CONTRATADA, por meio de pessoal próprio ou equipe de terceiros.
- Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando estiverem em conformidade com os padrões de informação e qualidade exigidos no contrato.

15. VISITA TÉCNICA

- Não se aplica.

16. ACORDO DE NÍVEIS DE SERVIÇO

- Estão estabelecidos Níveis de Serviço com a finalidade de aferir e avaliar diversos fatores relacionados aos serviços contratados, bem como orientar o pagamento por resultados obtidos.
- A contratada deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros abaixo:

NÍVEL DE SEVERIDADE DOS CHAMADOS		
Categoria	**Nível**	**Descrição**
Urgente	1	Serviços totalmente indisponíveis. Falha em servidor de produção que deixe indisponíveis os recursos do mesmo (serviço parado). Impacto a múltiplos usuários e/ou falha em servidor de produção que afete operações críticas da Contratante.
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Normal	3	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.

TABELA DE PRAZOS DE ATENDIMENTO AO SUPORTE				
Modalidade	**Prazos de Atendimento**	**Níveis de Severidade**		
		1. Urgente	**2. Crítico**	**3. Normal**
On site, Remoto, e-Mail, Fax ou Telefone	Início	30 minutos	45 minutos	60 minutos
	Término	2 horas	4 horas	8 horas
Atualizações e aplicações diversas	Início	Após a disponibilização pelo fabricante		
	Termino	24h após a atualização da solução		
Indisponibilidade	Total	1h para o restabelecimento do serviço		
	Parcial	3h para o restabelecimento do serviço por completo		

- Ocorrerá aplicação de glosas por motivo de descumprimento de nível de serviço exigido, conforme valores a seguir:
    - 0,15% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “normal” não atendida;
    - 0,25% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “crítico” não atendida;
    - 0,50% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “urgente” não atendida;
    - 3% no valor da fatura do grupo correspondente do mês de referência, por até 15 dias de não cumprimento do item categorizado como “Atualizações e aplicações diversas”;
    - 5% no valor da fatura do grupo correspondente do mês de referência, por mais de 15 dias no mês corrente de não cumprimento do item categorizado como “Atualizações e aplicações diversas”;
    - 2% no valor da fatura do grupo correspondente do mês de referência, por hora de indisponibilidade total, após o vencimento do prazo indicado na tabela;
    - 1% no valor da fatura do grupo correspondente do mês de referência, por hora de indisponibilidade parcial, após o vencimento do prazo indicado na tabela;
- Os descontos relativos à redução por não cumprimento do nível de serviço deverão ser aplicados na fatura do mês corrente;
- Os descontos relativos à redução por não cumprimento do nível de serviço não serão aplicados para demandas não rotineiras, no caso, por exemplo, de novas instalações;

17. FORMALIZAÇÃO DO CONTRATO

17.1. Deverá haver a formalização do contrato.

18. PROPOSTAS DE PREÇO

18.1. A proposta de preço deverá informar o preço unitário, o valor da parcela mensal e o valor anual, em moeda nacional, para a prestação do serviço objeto deste documento, segundo o modelo contido no Anexo I;

19. ASSINATURAS

Paulo Pompei de L e S Junior
Coordenador de Segurança da Informação
GTI-7.2 - CEDAE

Ricardo Batista Moreira
Chefe de Departamento de Suporte, Infraestrutura e Segurança da Informação
GTI-7.2 - CEDAE

ANEXO I

MODELO DE PROPOSTA DE PREÇOS

PROPOSTA DE PREÇOS

Serviço de Proteção de Estações de Trabalho e Servidores						
Item	**Descrição**	**Referência**	**Preço Unitário**	**Qtd.**	**Preço Mensal**	**Preço Anual**
1	*Subscrição de licença de uso para solução Antivírus (estações de trabalho)*			2600		
2	*Subscrição de licença de uso para solução Antivírus (Servidores)*			300		
3	*Serviço de suporte técnico para solução Antivírus (Estações de trabalho e Servidores), remoto 24x7*			1		
4	*Serviço de treinamento para solução Antivírus (Estações de trabalho e Servidores)*			3		

	Mensal	**Anual**
Valores Globais		

ANEXO V

PROPOSTA DE PREÇOS LOTE 1

SERVIÇO PÚBLICO ESTADUAL	PREGÃO ELETRÔNICO - PE-RP Nº 002/2020
Companhia Estadual de Águas e Esgotos do Rio de Janeiro – CEDAE RJ	A realizar-se em: 14/12/2021 às 14:00 horas
PROPOSTA DE PREÇOS	
ANEXO V - LOTE 1	Processo Nº SEI - 120211/000548/2020
A firma ao lado mencionada propõe fornecer ao PRODERJ - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro, pelos preços abaixo assinalados, obedecendo rigorosamente as condições estipuladas no EDITAL PE-RP Nº 002/2020	NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA CNPJ:09.137.728/0001-34 END. SCN Qd. 05 Bl. A TORRE NORTE SALA 617 Ed. BRASÍLIA SHOPPING CEP 70715-900 BRASÍLIA - DF **CARIMBO**

Registro de Preços para subscrição de licenças de software para solução Antivírus, incluindo console de Gerenciamento, suporte, instalação, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 meses, conforme especificações e condições constantes no Termo de Referência - Anexo I do Edital e seus anexos						VALOR R$	
	Item	ID SIGA	Descrição	U.F	Qtde	Unitário	Total
Lote 1	1	167761	Subscrição de licenças de uso para solução Antivírus (Estações de trabalho)	U.N	2600	R$ 560,4876	R$ 1.457.267,7600
	2	167762	Subscrição de licenças de uso para solução Antivírus (Servidores).	UN	300	R$ 3.704,9004	R$ 1.111.470,1200
	3	167764	Serviço de treinamento para solução antivirus (estações de trabalho e Servidores)	Turma	3	R$ 15.294,7110	R$ 45.884,1330
	4	167766	Serviço de suporte técnico para solução antivírus (estações de trabalho e servidores), remoto 24x7.	UN	1	R$ 360,9828	R$ 360,9828
Valor Total Global (Lote 1) 36 meses							R$ 2.614.982,9958
Valor total por extenso: Dois milhões, seiscentos e quatorze mil, novecentos e oitenta e dois reais e noventa e nove centavos.							

Dados do Banco Bradesco do Licitante:	
Agência (Nome/nº): 01228	
Conta Corrente: 0290352-0	
OBSERVAÇÕES:	
1ª - A PROPOSTA DE PREÇOS deverá:	Prazo de execução: Conforme o TR
Conter os preços em algarismos e por extenso, por unidade, já incluídas as despesas de fretes, impostos federais ou estaduais e descontos especiais; e	Validade da PROPOSTA: Preços válidos por 60 (sessenta) dias.
2ª - O Proponente se obrigará, mediante devolução da PROPOSTA DE PREÇOS, a cumprir os termos nela contidos.	Local de entrega desta Proposta: Rua da Conceição nº 69/24º andar - Centro - Rio de Janeiro - RJ.
3ª - A licitação poderá ser anulada no todo, ou em parte, de conformidade com a legislação vigente.	Declaramos inteira submissão ao presente termo e legislação vigente.
	Em, 01 de julho de 2022.
	Assinatura do Responsável PATRICIA ANGELINA DA CONCEICAO:34699483801 Assinado de forma digital por PATRICIA ANGELINA DA CONCEICAO:34699483801 Dados: 2022.07.01 14:29:11 -03'00'
	Ntsec Soluções em Teleinformática Ltda.

Os preços contemplam todos os custos de acordo com as condições estabelecidas no Termo de Referência.

A proposta de preços engloba todas as despesas relativas ao objeto do contrato, bem como os respectivos custos diretos e indiretos, tributos, remunerações, despesas fiscais e financeiras e quaisquer outras necessárias ao cumprimento do objeto desta Licitação, salvo expressa previsão legal. Nenhuma reivindicação adicional de pagamento de preços será considerada.

Validade da proposta: 60 (sessenta) dias contados da data de abertura da sessão.

Brasília, 01 de julho de 2022.

PATRICIA ANGELINA DA CONCEICAO:34699483801
Assinado de forma digital por PATRICIA ANGELINA DA CONCEICAO:34699483801
Dados: 2022.07.01 14:29:28 -03'00'

Patrícia Angelina da Conceição

ticas organizacionais que contribuam para a implementação dos princípios e das diretrizes de governança pública;
IV - analisar e propor medidas para garantia da coerência das práticas de gestão às políticas públicas;
V - incentivar e monitorar a aplicação das melhores práticas de governança no âmbito da administração pública estadual;
VI - acompanhar a evolução da aplicação de suas recomendações e das iniciativas de aprimoramento da governança.

Parágrafo Único - O Comitê de Governança e Gestão (CGG) elaborará atas das reuniões com a pauta abordada e os itens discutidos.

Art. 5º - As pastas da Administração Direta e as entidades da Indireta envolvidas na implantação do Gestão.gov.br deverão designar responsáveis pela condução dos processos e das funções relacionadas aos objetivos da governança, da integridade corporativas e priorizar as atividades e demandas do Comitê, bem como a produção de informações consolidadas e as estatísticas que alimentarão a base de dados para o aperfeiçoamento reiterado da gestão estratégica.

Art. 6º - As demais atribuições do de Governança e Gestão do Gestão.gov.br estão definidas no Projeto de Implantação do Modelo de Governança e Gestão - Gestão.gov.br e no Guia do Instrumento de Maturidade da Gestão - IMG.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 7º - Os membros do Comitê não receberão qualquer espécie de remuneração por sua atuação, sendo o exercício de suas atividades considerado de relevante interesse público.

Art. 8º - Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro, 01 de novembro de 2022

ANTONIO PEDREGAL
Secretário de Estado de Envelhecimento Saudável

Id: 2435380

Secretaria de Estado de Transformação Digital

ADMINISTRAÇÃO VINCULADA

**SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL
CENTRO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO**

**DESPACHOS DO ORDENADOR DE DESPESAS
DE 01/11/2022**

PROCESSO Nº SEI-430002/000019/2022 - Com base no Parecer 476/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 4.887,55 (quatro mil oitocentos e oitenta e sete reais e cinquenta e cinco centavos), competência de dezembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan),conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435975

PROCESSO Nº SEI-150016/001314/2022 - Com base no Parecer 446/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 4.887,55 (quatro mil oitocentos e oitenta e sete reais e cinquenta e cinco centavos), competência de novembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan), conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435976

PROCESSO Nº SEI-430002/000074/2022 - Com base no Parecer 487/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 20.199,84 (vinte mil cento e noventa e nove reais e oitenta e quatro centavos), competência de novembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan), conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435977

PROCESSO Nº SEI-430002/000075/2022 - Com base no Parecer 479/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 20.199,84 (vinte mil cento e noventa e nove reais e oitenta e quatro centavos), competência de dezembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan),conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435978

PROCESSO Nº SEI-430002/000237/2022 - Com base no Parecer 489/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 15.599,80 (quinze mil quinhentos e noventa e nove reais e oitenta centavos), competências de novembro e dezembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan), conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435979

PROCESSO Nº SEI-430002/000163/202 - Com base no Parecer 482/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 66.315,45 (sessenta e seis mil trezentos e quinze reais e quarenta e cinco centavos), competência de novembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan), conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435980

PROCESSO Nº SEI-430002/000164/2022 - Com base no Parecer 488/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 66.315,45 (sessenta e seis mil trezentos e quinze reais e quarenta e cinco centavos), competência de dezembro de 2021, em favor da Claro S/A. - CNPJ nº 40.432.544/0062-69, referente à despesa com prestação de serviços de comunicação de dados de longa distância (wan),conexão internet para rede governo e serviços complementares de tecnologia da informação e comunicação para o governo do estado do Rio de Janeiro.

Id: 2435981

PROCESSO Nº SEI-150016/000616/202 - Com base no Parecer 323/2022/PRODERJ/ASSJUR, **RECONHEÇO** a dívida de exercício anterior no valor Total de R$ 15.375,00 (quinze mil trezentos e setenta e cinco reais), competência de dezembro de 2021, em favor da Extreme Digital Consultoria e Representações Ltda. - CNPJ nº 14.139.773/0001-68, referente à despesa com prestação de serviços de assistência técnica especializada, destinada a atender as demandas de suporte técnico das Secretarias e Órgãos do governo do Estado do Rio de Janeiro e para sustentação da infraestrutura de tecnologia da infomação e comunicação TIC da rede governo, por meio de ações proativas, preventivas, preditivas e corretivas, além do pianejamento e execução do projeto de implementação do novo data conter '' do Proderj.

Id: 2435982

Procuradoria Geral do Estado

PROCURADORIA GERAL DO ESTADO

**DESPACHO DO PROCURADOR-GERAL
DE 26.10.2022**

PROCESSO Nº SEI-140001/033397/2022 - À luz do presente processo, **HOMOLOGO** o termo de autocomposição celebrado entre o Estado do Rio de Janeiro, por meio da Procuradoria Geral do Estado, e LAURO DA GAMA E SOUZA JUNIOR, constante do documento 41485626, para que produza seus regulares efeitos, nos termos do artigo 12, § 2º, da Resolução PGE nº 4.710/21, e do artigo 12, da Lei Estadual nº 9.629/22.

Id: 2436056

AVISOS, EDITAIS E TERMOS DE CONTRATOS

Secretaria de Estado da Casa Civil

SECRETARIA DE ESTADO DE ESTADO DA CASA CIVIL

EXTRATO DE TERMO ADITIVO

INSTRUMENTO: 3º Termo Aditivo ao Contrato n° 003/2020.
PARTES: Estado do Rio de Janeiro, através da Secretaria de Estado da Casa Civil, e a EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS.
OBJETO: Prorrogar por mais 12 (doze) meses o prazo de vigência do contrato, totalizando 36 (trinta e seis) meses.
PRAZO: 12 (doze) meses, a contar de 29/12/2022.
VALOR: R$ 15.000,00 (quinze mil reais).
NOTA DE EMPENHO: 2022NE01771.
DATA DE ASSINATURA: 10/10/2022.
FUNDAMENTO: Art. 57, II da Lei nº 8.666/93 e suas alterações.
PROCESSO Nº SEI-150001/005675/2020.

Id: 2435786

EXTRATO DE TERMO

INSTRUMENTO: Termo de Cessão de Uso, lavrado no SEI-040196/000292/2021; índice 34164933.
PARTES: Estado do Rio de Janeiro e o Município de Itaperuna.
OBJETO: Imóvel, parcela correspondente aos 2° e 3° pavimentos, da Rua Cardoso Moreira, n°. 294, Município de Itaperuna/RJ.
FUNDAMENTO DO ATO: Utilização em suas atividades institucionais.
PRAZO: 20 anos.
DATA DA ASSINATURA: 11 de outubro de 2022.
PROCESSO Nº SEI-040196/000292/2021.

Id: 2435986

ADMINISTRAÇÃO VINCULADA

IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato de locação.
FUNDAMENTO: Lei Federal nº 8.245/1991, Lei nº 8.666/1993, Lei nº 13.303/16 e demais legislações aplicáveis.
PARTES: IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO e TERMINAL GARAGEM MENEZES CÔRTES S.A.
OBJETO: O presente contrato tem por objeto a locação das sobrelojas 221/222/223 e 224, do imóvel localizado na Rua São José, nº 35, com numeração suplementar pela Avenida Erasmo Braga, nº 278 - Centro - Rio de Janeiro.
PRAZO: O prazo de vigência do contrato será de 5 (cinco) anos, com início em 01.11.2022 e término em 31.10.2027.
VALOR: Dá-se a este contrato o valor estimado de R$ 937.165,20 (novecentos e trinta e sete mil cento e sessenta e cinco reais e vinte centavos).
PROGRAMA DE TRABALHO: 2151.22.122.0002.2016
NATUREZA DA DESPESA: 00100.3104.015
FONTE DE RECURSO: 230
DATA DE ASSINATURA: 31/10/2022
PROCESSO Nº SEI-150015/002761/2022.

Id: 2436066

IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO

EXTRATO DE TERMO

INSTRUMENTO: Termo de Rerratificação ao Contrato nº 21/2022.
PARTES: IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO e PPN TECNOLOGIA E INFORMATICA LTDA.
OBJETO: Constitui objeto do presente instrumento a retificação da Cláusula Segunda, que passará a contar com a seguinte redação:
CLÁUSULA SEGUNDA: DO PRAZO - O prazo de vigência do contrato será de 12 (meses) meses, ressaltando-se a garantia on-site de 5 anos, contados a partir da assinatura, desde que posterior à data da publicação do extrato deste instrumento no D.O., valendo a data de publicação do extrato com termo inicial de vigência, caso posterior à data convencionada nesta cláusula.
DATA DE ASSINATURA: 26/10/2022.
FUNDAMENTO: Processo nº SEI-150015/000521/2022.

Id: 2436069

IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO

EXTRATO DE TERMO ADITIVO

INSTRUMENTO: Termo Aditivo nº 01 ao Contrato nº 15/2021.
FUNDAMENTO: Art. 71, da Lei Federal nº 13.303/2016.
PARTES: Imprensa Oficial do Estado do Rio de Janeiro e Daniel Araujo da Silva Construções EIRELI - ME.
OBJETO: Constitui objeto do presente instrumento a prorrogação pelo período de 12 (doze) meses do prazo de vigência do Contrato nº 15/2021, relativo à contratação de empresa especializada para prestação de serviços técnicos de manutenção preventiva e corretiva de toda a rede elétrica e equipamentos elétricos da IOERJ - SEDE, através de 03 (três) técnicos especializados em eletrotécnica, incluindo a substituição de peças e materiais, caso necessário, que correrão por conta da contratante, conforme especificado e quantificado no Termo de Referência (Anexo I) e na Proposta Detalhe (Anexo II) do Edital de Pregão Eletrônico nº 07/2021.
VALOR ESTIMADO: R$ 252.000,00 (duzentos e cinquenta e dois mil reais).
PROGRAMA DE TRABALHO: 2151.22.122.0002.2016.
NATUREZA DE DESPESA: 00100.3104.082.
FONTE DE RECURSO: 230.
DATA DE ASSINATURA: 01/11/2022.
PROCESSO Nº SEI-150015/001559/2021.

Id: 2436067

IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO

AVISO

PROCEDIMENTO LICITATÓRIO INOMINADO Nº 002/2022 - PRESENCIAL.
OBJETO: Alienação de uma unidade de (Impressora ROTATIVA - PRES-LINE, identificada pelo patrimônio físico n º 8959 e Patrimônio - JDE nº 4907), conforme especificado e quantificado no Termo de Referência (Anexo I) e na Proposta Detalhe (Anexo II). **DATA:** 23/11/2022.
HORÁRIO: 09h30min.
LOCAL: Rua Professor Heitor Carrilho, nº 81, Centro, Niterói - RJ.O edital se encontra disponível no Sistema Eletrônico de Informações - SEI/RJ, no endereço eletrônico http://www.fazenda.rj.gov.br/sei e no portal da IOERJ (http://www.ioerj.com.br/portal/), ou por via impressa, na COMISLIP, situada à Rua Professor Heitor Carrilho, nº 81, Centro, Niterói - RJ, de segunda a sexta-feira, em dias úteis, no horário de 10 às 15 horas, telefone (21) 2717-4040.
PROCESSO Nº SEI-150015/002892/2021.

Id: 2436068

**SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS**

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 110/2022 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE - e a SODEXO PASS DO BRASIL SERVIÇOS E COMÉRCIO S.A.
OBJETO: "CONTRATAÇÃO REMANESCENTE DO SERVIÇO DE FORNECIMENTO DE VALE ALIMENTAÇÃO E DE VALE REFEIÇÃO AOS EMPREGADOS DA CEDAE".
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 70.000.000,00 (setenta milhões de reais).
DATA DE ASSINATURA: 03/10/2022.
FUNDAMENTO: Processo n° SEI-E12/800.435/2020 (Dispensa de Licitação - DL nº 011/2022 DPR).

Id: 2430217

**SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS**

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 114/2022 (DAD).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE - e a NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.
OBJETO: "CONTRATAÇÃO DE SERVIÇO DE PROTEÇÃO DE ESTAÇÕES DE TRABALHO E SERVIDORES COM SUBSCRIÇÃO DE LICENÇAS DE USO PARA SOLUÇÃO ANTIVÍRUS".
PRAZO: 36 (trinta e seis) meses.
VALOR TOTAL: R$ 2.614.982,99 (dois milhões, seiscentos e quatorze mil, novecentos e oitenta e dois reais e noventa e nove centavos).
DATA DE ASSINATURA: 04/10/2022.
FUNDAMENTO: Processo nº SEI-150001/008347/2022 (Pregão Eletrônico - PE nº 002/2021 e da Ata de Registro de Preços nº 001/2022).

Id: 2430218

**SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS**

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 116/2022 (DTP).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE - e a BARRA NOVA ENGENHARIA LTDA-EPP.
OBJETO: "COMPLEMENTAÇÃO DAS OBRAS DE CONTENÇÃO DO TALUDE (UT) TUNEL IV - PARACAMBI".
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 4.309.000,00 (quatro milhões, trezentos e nove mil reais).
DATA DE ASSINATURA: 05/10/2022.
FUNDAMENTO: Processo n° SEI-E-12/800.597/2020 (Procedimento Licitatório - LI 002/2021).

Id: 2430219

**SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS
ASSESSORIA DE LICITAÇÕES**

AVISO

MODALIDADE DE LICITAÇÃO: LI nº 009/2022.
OBJETO: "Serviços contínuos de manutenção, reparos, limpeza e operação assistida em poços tubulares profundos em diversas localidades de atuação da Diretoria do Interior - DRI".
PROCESSO CEDAE Nº SEI-150001/002717/2022.

A Assessoria de Licitações comunica que se encontra à disposição dos interessados no endereço www.cedae.com.br/licitacoes a Errata 02 com as alterações efetuadas no edital da licitação em epígrafe e informa, ainda, que a licitação teve sua realização adiada para o dia 29/11/2022, no mesmo local e horário anteriormente divulgados.

Id: 2435792

**SECRETARIA DE ESTADO DA CASA CIVIL
INSTITUTO RIO METRÓPOLE**

EXTRATO DE TERMO

INSTRUMENTO: Termo de Ajuste de Contas nº 01/2022.
PARTES: INSTITUTO RIO METRÓPOLE - IRM e IMPRENSA OFICIAL DO ESTADO DO RIO DE JANEIRO.
OBJETO: indenização referente aos serviços de publicação de atos oficiais, realizados pela Imprensa Oficial do Rio de Janeiro, no período entre 1º de janeiro de 2022 a 06 de junho de 2022, no valor de R$ 12.985,37 (doze mil, novecentos e oitenta e cinco reais e trinta e sete centavos).
DATA DA ASSINATURA: 06/10/2022.
FUNDAMENTO: Lei nº 8.666/93.
PROCESSO Nº SEI-120228/000118/2022.

Id: 2436062

INSTITUTO DE SEGURANÇA PÚBLICA

EXTRATO DE TERMO

INSTRUMENTO: Acordo de Cooperação Técnica nº 013/2022. PARTES: Estado do Rio de Janeiro, pelo Instituto de Segurança Pública - ISP e a Secretaria de Estado de Polícia Civil do Estado do Rio de Janeiro. OBJETO: o presente acordo tem por finalidade estabelecer o compartilhamento e intercâmbio de informações atinentes à segurança pública entre as instituições envolvidas. PRAZO DE VIGÊNCIA: o presente Acordo de Cooperação Técnica terá vigência por 24 (vinte e quatro) meses, a contar de sua publicação em Diário Oficial, podendo ser prorrogado, até o prazo máximo de 60 (sessenta) meses, com a devida anuência dos partícipes, mediante termo aditivo. VALOR: Não envolve a transferência de recursos entre os partícipes. DATA DA ASSINATURA: 26 de outubro de 2022. FUNDAMENTO: Processo nº SEI-360036/000208/2021.

Id: 2435805