PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

# CONTRATO N. 031/2018-CJF

PROCESSO N. CJF-ADM-2017/00320

PREGÃO ELETRÔNICO N. 14/2018-CJF

| DADOS DA CONTRATADA |
|---|
| **CONTRATADA: ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA.** |
| **CNPJ/MF:** 21.547.011/0001-66 |
| **ENDEREÇO:** SCN Quadra 1, Bloco F, Salas 501 a 503, Edifício América Office Tower, Asa Norte. CEP.: 70.711-905. |
| **TELEFONE:** (61) 3344.0236 |
| **E-MAIL:** mrossetto@alltechsolucoes.com.br;jribeiro@alltechsolucoes.com.br |
| **SIGNATÁRIO CONTRATADA:** MURILO ROSSETTO-Diretor |
| **SIGNATÁRIO CJF:** MÁRCIA DE CARVALHO/Diretora Executiva de Administração e de Gestão de Pessoas |

| DADOS DO CONTRATO |
|---|
| **OBJETO:** contratação de solução de segurança para proteção de *endpoint* e *datacenter*, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico. (Ata de Registro de Preços n. 015/2018 - CJF) |
| **FUNDAMENTAÇÃO LEGAL**: Lei n. 10.520/2002, Decreto n. 5.450/2005, Decreto n. 7.892/2013, e legislação correlata, aplicando-se, subsidiariamente, no que couberem, a Lei Complementar n. 123/2006 e alterações, regulamentada pelo Decreto n. 8.538/2015, Lei n. 8.666/1993 e alterações, Lei n. 12.846/2013 e, em conformidade com as informações constantes do Processo n. CJF-ADM-2017/00320. |
| **VIGÊNCIA:** 4 meses (entrega/configuração/treinamento)<br>60 meses (suporte técnico) |
| **VALOR DO CONTRATO: R$ 1.028.130,50** |
| **UNIDADE FISCALIZADORA: STI** |
| OBS.: Garantia contratual - 5% - cláusula 12ª<br>Vigência: 4 meses (entrega/configuração/treinamento) 60 meses (suporte técnico) cláusula 7ª |

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

**CONTRATO N. 031/2018-CJF**

Contrato que entre si celebram, o **CONSELHO DA JUSTIÇA FEDERAL** e a **ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA,** para a contratação de solução de segurança para proteção de *endpoint* e *datacenter*.

**CONTRATANTE:** **CONSELHO DA JUSTIÇA FEDERAL,** Órgão integrante do Poder Judiciário, CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília - DF, neste ato representado por sua Diretora Executiva de Administração e de Gestão de Pessoas, CPF/MF n. 152.491.231-04, Carteira de Identidade n. 451.499 SSP/DF, residente em Brasília - DF.

**CONTRATADA:** **ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA**, pessoa jurídica de direito privado, CNPJ/MF n. 21.547.011/0001-66, com sede no SCN Quadra 1, Bloco F, Salas 501 a 503, Edifício América Office Tower, Asa Norte, Brasília – DF, CEP: 70.711-905, neste ato representada por seu Diretor, o Senhor **MURILO ROSSETTO**, CPF/MF n. 036.031.821-54, Carteira de Identidade n. 2.485.039 SSP/DF.

As partes celebram o presente Contrato com fundamento na Lei n. 10.520, de 17 de julho de 2002, no Decreto n. 5.450, de 31 de maio de 2005, no Decreto n. 7.892, de 23 de janeiro de 2013, e legislação correlata, aplicando-se, subsidiariamente, no que couberem, a Lei Complementar n. 123, de 14 de dezembro de 2006 e alterações, regulamentada pelo Decreto n. 8.538, de 6 de outubro de 2015, na Lei n. 8.666, de 21 de junho de 1993 e alterações, na Lei n. 12.846, de 1º de agosto de 2013 e, em conformidade com as informações constantes do Processo n. CJF-ADM-2017/00320, mediante as cláusulas e condições seguintes:

## CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O objeto deste Contrato consiste na contratação de solução de segurança para proteção de *endpoint* e *datacenter*, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do CONTRATANTE, de acordo com as especificações técnicas contidas no Módulo I-Termo de Referência, do edital, na proposta comercial e tudo que consta do Pregão Eletrônico n. 14/2018-CJF, que ficam fazendo parte integrante do presente Contrato, independentemente de sua transcrição.

1.2. O detalhamento do objeto é apresentado no Módulo I-Termo de Referência e seus anexos.

## CLÁUSULA SEGUNDA - DO FORNECIMENTO

2.1. Os fornecimentos/serviços serão prestados em estrita observância às determinações, forma e condições constantes no Edital do Pregão Eletrônico n. 14/2018 seus Módulos e na proposta da CONTRATADA.

2.2. A entrega dos *softwares* e acessórios da solução e a realização dos serviços previstos neste Contrato deverão ser realizados na sede do CONTRATANTE, situada no Setor de Clubes Esportivos Sul - SCES - Trecho III, Polo 8, Lote 9, CEP 70200-003, Brasília - DF.

2.3. A solução de segurança é composta por *softwares* com garantia de 60 meses, serviços de instalação e configuração, serviço de transferência de conhecimento e serviço de suporte técnico por 60 meses, contados a partir da emissão do Termo de Recebimento Definitivo.

2.4. O quadro demonstrativo da situação atual de licenças - Solução Trend Micro, constam no subitem 3.1. E, o detalhamento do ambiente tecnológico consta no Anexo II do Módulo I - Termo de Referência.

2.5. O quantitativo do objeto é o constante do item 5 do Módulo I - Termo de Referência.

## CLÁUSULA TERCEIRA - DA EXECUÇÃO DO OBJETO

3.1. A solução de segurança para *endpoint* e *datacenter* deverá operar de forma integrada, ou seja, os *softwares* fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir desempenho, disponibilidade e funcionalidades adequados aos requisitos do CONTRATANTE.

3.2. Todas as soluções, independentemente do fabricante, deverão atender as condições, características e especificações técnicas previstas no Módulo I - Termo de Referência e demais itens não previstos que possam influir direta ou indiretamente no ambiente computacional do CONTRATANTE.

3.3. Caso algum *software* que compõe a solução conste em lista *de end-of-support, end-of-engineering-support ou end-of-life* do fabricante, durante o período de vigência das licenças de uso, a CONTRATADA deverá fornecer, configurar e promover a substituição por novo *software* equivalente, que atenda as especificações técnicas descritas no Módulo I - Termo de Referência e que não impacte na perda de funcionalidade da solução.

3.4. Os *softwares* deverão ser fornecidos em sua versão mais atualizada.

3.5. Caso a solução a ser fornecida, utilize *software* de proteção de *endpoint* diferente do atualmente instalado no CONTRATANTE, a CONTRATADA deverá providenciar a desinstalação automática de todas as cópias instaladas do *software* em estações e servidores e a instalação do novo *software* em um único processo.

3.6. A CONTRATADA deverá iniciar a execução das atividades de entrega, instalação e configuração dos *softwares* da solução de acordo com os prazos definidos no Anexo III do Módulo I - Termo de Referência, contados a partir da emissão da Ordem de Serviço do CONTRATANTE.

3.7. Até o 3º (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na sede do CONTRATANTE, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução de segurança para proteção de *endpoints* e *datacenter*.

3.8. A CONTRATADA deverá apresentar um Plano de Implantação, em até 10 (dez) dias da emissão da Ordem de Serviço do CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos *softwares* que compõem a solução.

3.8.1. O Plano de Implantação deverá dispor sobre o cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo os itens descritos nas alíneas "a/g", do subitem 7.2.4 do Módulo I - Termo de Referência.

3.9. A CONTRATADA deverá entregar todos os *softwares* e acessórios, no prazo máximo de até 15 (quinze) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.

3.10. Juntamente com o *software*, deverão ser entregues todos os documentos comprobatórios de garantia e de suporte técnico indicados nos itens **Erro! Fonte de referência não encontrada.** e **Erro! Fonte de referência não encontrada.** do Módulo I -Termo de Referência e toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.

3.11. Para a execução dos serviços e fornecimento dos *softwares* a CONTRATADA deverá cumprir os demais requisitos constantes no Módulo I - Termo de Referência e seus anexos.

## CLÁUSULA QUARTA – OBRIGAÇÕES DA CONTRATADA

4.1. A CONTRATADA obriga-se ao cumprimento de todas as disposições constantes do Item 7 do Módulo I - Termo de Referência e seus anexos e, ainda, a:

a) realizar a transferência de conhecimento conforme descrito no subitem 7.3 do Módulo I - Termo de Referência;

b) prestar garantia e suporte técnico conforme descrito no subitem 7.4 e 7.5, respectivamente do Módulo I - Termo de Referência;

c) iniciar a execução das atividades de entrega, instalação e configuração dos *softwares* da solução de acordo com os prazos definidos no cronograma, contados a partir da emissão de Ordem de Serviço do CONTRATANTE;

d) fornecer os *softwares* da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CONTRATANTE, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração;

e) entregar todos os *softwares* e acessórios no prazo máximo de até 15 (quinze) dias, a contar da data de emissão da Ordem de Serviço do CONTRATANTE;

f) não subcontratar, no todo ou em parte, o objeto deste Contrato;

g) manter durante todo o período de vigência deste Contrato as condições de habilitação e qualificação exigidas para a contratação, comprovando-as, a qualquer tempo, mediante solicitação do CONTRATANTE;

h) assumir a responsabilidade por danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE;

i) responsabilizar-se por todos os ônus referentes aos serviços/fornecimentos objeto deste Contrato, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício de sua atividade;

j) acatar, nas mesmas condições ofertadas, nos termos do § 1º do art. 65 da Lei n. 8.666/1993, as solicitações do CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto;

k) sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo às reclamações fundamentadas, caso venham a ocorrer;

l) substituir, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado, devidamente justificado;

m) dar ciência aos seus empregados acerca da obediência ao Código de Conduta do Conselho da Justiça Federal, nos termos da Resolução n. 147, de 15 de abril de 2011 (http://www.cjf.jus.br/codigo-de-conduta).

## CLÁUSULA QUINTA - OBRIGAÇÕES DO CONTRATANTE

5.1. O CONTRATANTE obriga-se a cumprir todas as obrigações constantes do termo de referência e, ainda, a:

a) acompanhar e fiscalizar a execução do objeto contratual;

b) determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual;

c) informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados;

d) comunicar formalmente qualquer anormalidade ocorrida na execução dos

serviços pela CONTRATADA;

e) avaliar todos os serviços prestados pela CONTRATADA;

f) responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA, após a apresentação de nota fiscal;

g) indicar os seus representantes para fins de contato e demais providências inerentes à execução do Contrato;

h) permitir o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações no período de garantia. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive quanto à identificação, trânsito e permanência em suas dependências.

## CLÁUSULA SEXTA – DA CONFIDENCIALIDADE

6.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do Contrato, todas as informações relativas à:

6.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de *hardware* e *software* decorrentes.

6.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e em atendimento aos itens de segurança constantes dos objetos instalados.

6.1.3. Qualquer informação do CONTRATANTE que venha tomar conhecimento em razão da execução dos serviços.

6.2. A CONTRATADA deverá entregar assinado por seu representante legal e com firma reconhecida, o Termo de Confidencialidade e Sigilo da CONTRATADA, Anexo IV do Módulo I - Termo de Referência deste Contrato.

## CLÁUSULA SÉTIMA – DA VIGÊNCIA

7.1. A vigência do Contrato será de:

7.1.1. **4 (quatro) meses**, contados da assinatura do Contrato, para a execução, mediante a emissão da Ordem de Serviços, da entrega, instalação, configuração, transferência de conhecimento e recebimento definitivo.

7.1.2. **60 (sessenta) meses**, contados da data de emissão do Termo de Recebimento Definitivo, referente aos serviços de garantia e suporte técnico da solução de segurança para proteção de *endpoint* e *datacenter*, relativo aos serviços de natureza contínua da contratação.

## CLÁUSULA OITAVA – DO PREÇO E DO VALOR DO CONTRATO

8.1. O preço que o CONTRATANTE se obriga a pagar à CONTRATADA, nos termos do presente Contrato, é de **R$ 1.028.130,50 (um milhão, vinte e oito mil, cento e trinta reais e cinquenta centavos)**, conforme especificado no Módulo II - Planilha de Preços e do qual serão feitas as glosas e retenções legais.

8.2. Nos valores estabelecidos nesta cláusula estão incluídos todos os tributos, contribuições fiscais e parafiscais previstos na legislação em vigor, incidentes, direta ou indiretamente, bem como despesas de quaisquer naturezas decorrentes da execução do presente Contrato.

## CLÁUSULA NONA – DOS RECURSOS FINANCEIROS

9.1. As despesas com a execução do presente Contrato correrão à conta de recursos orçamentários da União destinados ao CONTRATANTE consignados no Programa de Trabalho 085322, nos Elementos de Despesa 449040, 3390.40, com a respectiva emissão de notas de empenho: 2018NE000649, 2018NE000650 e 2018NE000651.

9.2. Observada as limitações constantes do § 1° do art. 65 da Lei n. 8.666/1993, poderá o CONTRATANTE promover alterações no objeto do presente Contrato.

## CLÁUSULA DÉCIMA – DO ACOMPANHAMENTO DO CONTRATO

10.1. A autoridade competente designará a equipe de gestão e fiscalização deste Contrato com as seguintes atribuições:

10.1.1. **Gestor do Contrato**: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual.

10.1.2. **Fiscal Técnico do Contrato**: servidor representante da Área de Tecnologia da Informação para fiscalizar tecnicamente o Contrato.

10.1.3. **Fiscal Administrativo do Contrato**: servidor representante da Área Administrativa para fiscalizar o Contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

10.1.4. **Fiscal Requisitante do Contrato**: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o Contrato do ponto de vista funcional da solução.

## CLÁUSULA DÉCIMA PRIMEIRA – DO RECEBIMENTO E DO PAGAMENTO

11.1. Será emitido Termo de Recebimento Provisório (TRP) após a entrega dos *softwares*, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no Anexo III do Módulo I-Termo de Referência.

11.2. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA. O recebimento provisório realizar-se-á no prazo máximo de 3 (três) dias corridos, contados da comunicação da CONTRATADA, desde que não haja pendências a cargo da mesma.

11.3. A CONTRATADA deverá concluir no prazo de 15 (quinze) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação, entrega das licenças de uso e configuração da solução, realizando todas as atividades programadas para esta etapa.

11.4. Será emitido Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega,

licenciamento, instalação e configuração dos *softwares* da solução. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da CONTRATADA, desde que não haja pendências a cargo da mesma.

11.5. O pagamento dos *softwares* da solução, garantia por 60 (sessenta) meses, serviços de instalação, configuração e transferência de conhecimento, será efetuado por ordem bancária, em até 10 (dez) dias úteis, após recebimento da cópia do Termo de Recebimento Definitivo, conforme previsto no Anexo III do Módulo I - Termo de Referência e, atesto do Gestor do Contrato, mediante a apresentação de notas fiscais/faturas, devendo ser emitidas obrigatoriamente pelo CNPJ que conste no Contrato e correspondente aos respectivos produtos/serviços.

11.6. Na hipótese de o valor a ser pago enquadrar-se no § 3º do art. 5º da Lei n. 8.666/1993, o prazo para pagamento será de até 5 (cinco) dias úteis, contados da apresentação da fatura.

11.7. O pagamento do serviço de **suporte técnico** será efetuado **mensalmente**, sendo iniciado somente após o Recebimento Definitivo da Solução, mediante envio da nota fiscal/fatura pela CONTRATADA.

11.8. O CONTRATANTE descontará do valor devido à CONTRATADA, as retenções previstas na legislação tributária vigente à época do pagamento.

11.9. Os documentos de cobrança deverão ser emitidos eletronicamente e encaminhados ao Setor de Protocolo do Conselho da Justiça Federal, pelo e-mail: protocolo@cjf.jus.br e serão pagos com os recursos consignados ao CONTRATANTE no Orçamento Geral da União.

11.10. Os pagamentos serão efetuados após o recebimento definitivo. Esse caracterizar-se-á pelo recebimento circunstanciado do atesto da nota fiscal, que ficará a cargo do Gestor do Contrato. Após o recebimento definitivo, o crédito será realizado em conta corrente, por meio de ordem bancária, a qual será emitida até o décimo dia útil.

11.10.1. O servidor indicado para a fiscalização terá o prazo de 5 (cinco) dias para atestar a nota fiscal, após a data de apresentação do referido documento ao CONTRATANTE.

11.11. O depósito bancário produzirá os efeitos jurídicos da quitação da prestação devida.

11.12. Por ocasião do pagamento a CONTRATADA deverá comprovar a regularidade de sua situação para com o recolhimento das contribuições devidas ao INSS e ao FGTS, mediante apresentação das certidões respectivas.

11.13. A nota fiscal deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas, nos termos do item 13 do Módulo I - Termo de Referência, Anexo deste Contrato.

## CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA CONTRATUAL

12.1. Para o integral cumprimento de todas as obrigações contratuais assumidas, nos termos do § 1º do art. 56 da Lei n. 8.666/1993, a CONTRATADA deverá entregar ao

CONTRATANTE, no prazo máximo de 20 (vinte) dias, contados da ordem de serviço, garantia correspondente a 5% do valor total contratado.

12.2. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ou até mesmo restrinjam-lhe a cobertura ou a sua eficácia, sem que haja previsão ou autorização expressa no instrumento convocatório ou contratual.

12.3. A garantia deve cobrir os seguintes riscos atinentes à:

a) indenização pelos prejuízos advindos do não cumprimento do objeto contratado e do inadimplemento das demais obrigações nele previstas;

b) prejuízos causados ao CONTRATANTE ou a terceiro, decorrente de culpa ou dolo, durante a execução deste Contrato;

c) aplicação de multas moratórias e compensatórias;

d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA.

12.4. O CONTRATANTE poderá descontar da garantia o valor que a CONTRATADA passar a dever em virtude da ocorrência de qualquer das situações expressamente previstas neste Contrato e na legislação pertinente.

12.5. Caso haja aditamento deste Contrato ou redução do valor da garantia, a CONTRATADA deverá apresentar garantia complementar ou substituí-la, de modo a preservar o montante estabelecido nesta cláusula, no prazo máximo de 2 (dois) dias úteis.

12.6. Caso o valor da garantia venha a ser utilizado em pagamento de qualquer obrigação, a CONTRATADA obriga-se a efetuar a respectiva reposição no prazo máximo de 72 (setenta e duas) horas, a contar da data do recebimento da notificação do CONTRATANTE.

12.7. O CONTRATANTE reserva-se no direito de somente liberar a garantia contratual no prazo de 3 (três) meses, contado do término da vigência deste Contrato, caso haja adimplemento total de todos os ônus e encargos advindos da contratação, ficando estabelecido que a vigência da garantia se estende até o prazo estabelecido nesta cláusula.

12.8. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expiração do vencimento, alteração por aumento no valor do Contrato ou outra necessidade indispensável.

12.9. O termo da garantia será restituído à CONTRATADA após o cumprimento integral de todas as obrigações contratuais.

## CLÁUSULA DÉCIMA TERCEIRA – DA GARANTIA E DO SUPORTE TÉCNICO DA SOLUÇÃO

13.1. O prazo de garantia e direito a atualização dos *softwares* que compõe a solução é de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo.

13.1.1. Os custos relativos ao serviço de garantia da solução já devem estar incluídos no preço dos próprios itens.

13.1.2. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento e na integração entre os componentes da solução, mediante a substituição de versões dos *softwares* ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nas páginas e manuais de suporte e normas técnicas específicas.

13.1.3. O direito a atualização dos *softwares* obriga a CONTRATADA a disponibilizar a atualização dos *softwares* fornecidos e que compõem a solução tão logo ocorra o lançamento de novos *softwares* em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos *softwares* fornecidos.

13.2. Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

13.2.1. Cessões de direito de uso perpétuo dos *softwares* fornecidos ou subscrição. Os termos de licenciamento de todos os *softwares* fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direitos pertencentes ao CONTRATANTE.

13.2.2. Conjunto de direitos de atualização de versão, pelo período de 60 (sessenta) meses de garantia, de todos os *softwares* fornecidos. Abrangerá todos os *softwares* e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão direito pertencente ao patrimônio do CONTRATANTE.

13.3. A CONTRATADA deverá garantir todo o descrito no subitem 7.4 do Módulo I - Termo de Referência.

13.4. O serviço de suporte técnico *on-site* deverá ser executado pela CONTRATADA durante o prazo de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos *softwares* da solução.

13.5.O serviço de suporte técnico da solução consiste em:

13.5.1. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte:

13.5.1.1. No local de instalação da solução, visando a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação.

13.5.1.2. Por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

13.5.2. Realizar visitas técnicas preventivas no local de instalação da solução (*on-site*), com frequência mensal, e com duração de pelo menos 4h a cada visita, visando assegurar o melhor desempenho da solução.

13.6. Quando da abertura de chamado técnico de suporte, os chamados deverão ser categorizados em 4 (quatro) níveis, da seguinte forma:

| Criticidade | Descrição | Prazo máximo para início de atendimento (contados a partir da abertura do chamado) | Prazo máximo para restauração de serviço (contados a partir da abertura do chamado) |
|---|---|---|---|
| Severidade 1 (Alta) | Atuação ON-SITE visando sanar problemas que tornem a solução inoperante, causando alto impacto nas operações do CJF. | Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE. | Em até 6 (seis) horas |
| Severidade 2 (Média/Alta) | Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não tornem a solução inoperante, causando impacto no ambiente de produção ou restrição de funcionalidade. | Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato. | Em até 12 (doze) horas |
| Severidade 3 Média/Baixa | Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução de segurança não gerando impacto ao negócio. | Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato. | Em até 24 (vinte e quatro) horas |
| Severidade 4 (Baixa) | Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração. | Em até 12 (doze) horas um técnico da CONTRATADA entra em contato. | Em até 72 (setenta e duas) horas |

13.6.1. O CONTRATANTE realizará a abertura de chamados técnicos de suporte por meio de ligação telefônica ou via Internet, em período integral, 24h por dia, 7 (sete) dias por semana.

13.6.2. A CONTRATADA deverá informar o procedimento para a abertura de chamado técnico de suporte no documento Plano de Implantação.

13.6.3. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24h por dia, 7 (sete) dias por semana.

13.6.4. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

13.6.5. A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

13.6.6. A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de

instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

13.6.7. A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos *softwares* que compõe a solução de segurança, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

13.7. As visitas técnicas preventivas deverão ser realizadas por técnicos plenamente qualificados, devendo possuir certificação emitida pelos fabricantes dos *softwares* da solução ofertada. As visitas técnicas serão prestadas com acompanhamento da equipe técnica do CONTRATANTE.

13.8. A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo da solução, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança.

13.9. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

## CLÁUSULA DÉCIMA QUARTA – DAS PENALIDADES

14.1. A CONTRATADA, pela inexecução total ou parcial das obrigações assumidas neste Contrato e observado o regular procedimento administrativo, assegurado o contraditório e a ampla defesa, ficará sujeita às seguintes penalidades, sem prejuízo das demais previsões legais:

14.1.1. **Advertência**, sempre que forem observadas irregularidades de pequena monta para as quais tenha concorrido.

14.1.2. **Multa** no percentual correspondente a:

14.1.2.1. 0,05% calculada sobre o valor total da contratação, por dia de atraso na entrega do Plano de Implantação, além do prazo máximo definido no Anexo III do Módulo I - Termo de Referência, até o limite de 30 (trinta) dias corridos.

14.1.2.2. 0,1% calculada sobre o valor total da contratação, por dia de atraso na **entrega de todos os *softwares* e acessórios da solução**, além do prazo máximo definido no Anexo III do Módulo I - Termo de Referência, até o limite de 30 (trinta) dias corridos, caracterizando inexecução total do Contrato.

14.1.2.3. 0,1% calculada sobre o valor total da contratação, por dia de atraso na **conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no Anexo III do Módulo I - Termo de Referência, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do Contrato.

14.1.2.4. 0,5% calculada sobre o valor total do serviço de transferência de conhecimento, por dia de atraso, na conclusão do serviço de transferência de conhecimento, além do prazo máximo definido no Anexo III do Módulo I - Termo de Referência, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do Contrato.

14.1.2.5. 20% calculada sobre o valor do suporte técnico mensal, no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, caracterizando inexecução parcial do Contrato.

14.1.2.6. 0,20% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual disposta no item 19.1 do Módulo I - Termo de Referência, no caso de atraso injustificado na sua entrega.

14.1.2.7. 10% sobre o valor total da contratação, no caso de inexecução total do Contrato.

14.1.3. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual e a aplicação da multa, no percentual de 10% sobre o valor da parte não entregue ou não executada.

14.1.4. A não manutenção das condições de habilitação da CONTRATADA, ao longo da execução do Contrato, ensejará a rescisão contratual unilateral pelo CONTRATANTE, após regular procedimento administrativo e garantido o direito ao contraditório e à ampla defesa, e, ainda, a aplicação de multa de 5% sobre o valor da contratação.

14.1.5. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos arts. 87 e 88 da Lei n. 8.666/1993.

14.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE ou cobrado judicialmente.

14.3. A reincidência da aplicação de multa ou advertência dará direito ao CONTRATANTE à rescisão contratual unilateral.

14.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores/SICAF.

14.5. **Impedimento de licitar e contratar com a União**, pelo prazo de até 5 (cinco) anos, nos termos do art. 7º da Lei n. 10.520/2002 c/c o art. 28 do Decreto n. 5.450/2005.

14.6. **Suspensão temporária**, por prazo não superior a 2 (dois) anos, nos termos inciso III do art 87 da Lei n. 8666/1993, conforme Acórdão 2242/2013/TCU Plenário.

14.7. **Declaração de Inidoneidade** para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

14.8. Fica estabelecido que os casos omissos serão resolvidos entre as partes contratantes, respeitados o objeto do presente Contrato, a legislação e demais normas reguladoras da matéria, em especial as Leis n. 8.666/1993 e 10.520/2002, aplicando-lhes,

quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

14.9. Nos termos do § 3° do art. 86 e do § 1° do art. 87 da Lei n. 8.666/1993, a multa, caso aplicada após regular processo administrativo, será descontada do pagamento eventualmente devido pelo CONTRATANTE ou ser recolhida ao Tesouro por GRU (Guia de Recolhimento da União) no prazo máximo de 5 (cinco) dias úteis, contados da notificação ou, ainda, quando for o caso, cobrada judicialmente, em conformidade com a legislação específica.

14.10. A aplicação das sanções previstas nesta cláusula será feita mediante procedimento administrativo específico. O CONTRATANTE comunicará à CONTRATADA sua intenção de aplicação da penalidade, assegurando-lhe o direito ao contraditório e à defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir do recebimento da comunicação.

14.11. Decidida pelo CONTRATANTE a aplicação de sanção, fica assegurado à CONTRATADA o uso dos recursos previstos em lei.

## CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO

15.1. O presente Contrato poderá ser rescindido a juízo do CONTRATANTE, com base nos arts. 77 a 80 da Lei n. 8.666/1993, especialmente quando este entender que a CONTRATADA não está cumprindo de forma satisfatória as avenças estabelecidas neste Contrato, independentemente da aplicação das penalidades estabelecidas.

## CLÁUSULA DÉCIMA SEXTA – DA PUBLICAÇÃO

16.1. De conformidade com o disposto no parágrafo único do art. 61 da Lei n. 8.666/1993, o presente Contrato será publicado no Diário Oficial da União, na forma de extrato.

## CLÁUSULA DÉCIMA SETIMA – DAS DISPOSIÇÕES GERAIS

17.1. As partes contratantes ficarão exoneradas do cumprimento das obrigações assumidas por este Contrato, quando ocorrerem motivos de força maior ou caso fortuito, assim definidos no parágrafo único do art. 393 do Código Civil, enquanto tais motivos perdurarem.

17.2. Os casos omissos serão resolvidos à luz das disposições contidas na Lei n. 8.666/1993, bem como dos princípios de Direito Público.

17.3. É defeso à CONTRATADA utilizar-se deste Contrato para caucionar qualquer dívida ou títulos por ela emitidos, seja qual for a natureza dos mesmos.

17.4. A CONTRATADA assumirá, de forma exclusiva, todas as dívidas que venha a contrair com vistas a cumprir com as obrigações oriundas do presente Contrato, ficando certo, desde já, que o CONTRATANTE não será responsável solidário pelas mesmas.

17.5. Na contagem dos prazos será observado o disposto no art. 110 da Lei n. 8.666/1993.

17.6. A documentação necessária para pagamento, pedido de prorrogação de prazo, recursos, defesa prévia e outros de qualquer espécie que dependam de registro da data de entrega e protocolo, para contagem de prazo e demais efeitos legais, deverá ser entregue no

Setor de Clubes Esportivos Sul – SCES, Trecho III, Polo 8, Lote 9, Brasília/DF, CEP 70.200-003, no Setor de Protocolo/SETPEX, e-mail: protocolo@cjf.jus.br .

**CLÁUSULA DÉCIMA OITAVA – DO FORO**

18.1. O Foro do Juízo Federal da Seção Judiciária do Distrito Federal é competente para dirimir qualquer dúvida oriunda do presente Contrato, com renúncia expressa a qualquer outro que as partes tenham ou venham a ter, por privilegiado ou especial que seja.

E para firmeza e como prova de assim haverem ajustado, foi lavrado o presente Termo em 2 (duas) vias de igual teor, uma das quais destinada à CONTRATADA, o que, depois de lido e achado conforme, vai assinado pelos representantes das partes contratantes.

Brasília-DF, 19 de dezembro de 2018.

**MARCIA DE CARVALHO**
Diretora-Executiva de Administração e
de Gestão de Pessoas do Conselho da Justiça Federal

**MURILO ROSSETTO**
Diretor da Alltech Soluções em Tecnologia Ltda.

# CONTRATO N. 031/2018-CJF

## MÓDULO I – TERMO DE REFERÊNCIA

1. OBJETO

Registro de preços para eventual contratação de solução de segurança para proteção de *endpoint* e datacenter, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do Conselho da Justiça Federal - CJF, de acordo com as especificações técnicas contidas no Termo de Referência.

2. JUSTIFICATIVA

Em 2016 o CJF realizou a contratação de solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra-ataques avançados, com garantia de 24 meses, tendo sido assinado o termo de recebimento definitivo CJF-TRM-2016/00482 em 1 de julho de 2016. A solução então fornecida pela empresa Global IP era composta de 550 licenças para proteção de endpoints do tipo estação de trabalho Windows, 50 licenças para estações de trabalho Linux, 10 licenças para estações de trabalho Mac, 150 licenças para servidores de rede Windows, 300 licenças para servidores de rede Linux, 2 licenças para Storage, 1 solução para proteção para o serviço de e-mail e a console de gerência da solução.

Considerando que a solução implantada em 2016 atende as necessidades de segurança da informação previstas pela área de segurança das redes, verificou-se durante a fase de análise de viabilidades a possibilidade de se manter a solução atualmente implantada por meio da renovação de licenças dos produtos em utilização. No entanto, a experiência comprova que, ainda que see pudesse justificar a contratação nominada da solução implantada, a participação de outros fabricantes resulta num custo de aquisição mais baixo em comparação com renovação, em que ocorre a participação de apenas um fabricante. A competição entre diversos fabricantes acaba por reduzir o preço final da contratação e, no mínimo, força o fabricante da atual solução a baixar seus preços, o que normalmente não ocorre com a renovação nominada sem a concorrência com outros fabricantes.

Consoante ao termo de referência utilizado no procedimento licitatório prévio, foram exigidas proteções contra diversos tipos de programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, dentre outros, bem como as proteções virtual patch e controle de aplicações tanto para o ambiente de estações de trabalho quanto de datacenter. Em relação a última contratação, foi suprimida a contratação de proteção para o serviço de e-mail pois no contrato n. 047/2017 – CJF, para atendimento da solução para proteção contra-ataques avançados, a empresa contratada forneceu também produto para a proteção de serviço e-mail. Desta forma, objetivando a economicidade da presente contratação, o item não foi previsto. Ademais, alguns produtos que não chegaram a ser demandados em Ordem de Serviço por ainda não serem utilizados no CJF, tal como proteção para Mac e para smartphones, também foram suprimidos.

Assim, s.m.j, acredita-se que as proteções vislumbradas nesta contratação, somadas as demais proteções já existentes, são economicamente e tecnicamente adequadas para fazer frente aos avanços tecnológicos dos ataques realizados por criminosos cibernéticos ao CJF. Destes pode-se salientar os ataques de "dia zero", nome utilizado na indústria de segurança da informação para ataques utilizados por meio da exploração de uma vulnerabilidade anteriormente desconhecida que afeta de maneira adversa programas, dados, computadores e redes. Códigos maliciosos que exploram tais vulnerabilidades não podem ser detectados pelo método tradicional de assinatura utilizado pela solução ora em uso. Desta forma, são necessárias outras formas de detecção, como o uso de métodos heurísticos de análise, emulação de código e virtualização.

Não obstante o valor agregado ao uso de tecnologias de gerenciamento de eventos e segurança de informação (SIEM – Security Information and Event Management) na análise em tempo real de alertas

de segurança gerados pelo *hardware* de rede, segurança e aplicações, optou-se pela não inclusão de componente de SIEM na presente solução pela inerente complexidade em sua aquisição, implementação e uso, bem como a relativa falta de maturidade e de pessoal especializado na organização que viabilizasse seu eficaz uso.

Tendo em vista que esta contratação se trata de serviço de natureza contínua, que é de fundamental importância para a proteção do maior bem do CJF, suas informações, que o contrato atual finda em 1 de julho de 2018, torna-se urgente a presente contratação.

3. DESCRIÇÃO DOS PRODUTOS

3.1. Quadro demonstrativo da situação atual de licenças – Solução Trend Micro:

| Nome do produto | Licenças |
|---|---|
| Deep Security - Network Security per CPU (Socket) | 18 |
| Deep Security Anti-Malware per CPU (Socket) | 18 |
| ServerProtect EMC Component | 510 |
| Serverprotect For Netapp | 510 |
| Cloud App Security for Office 365 Advanced Threat Protection Service | 510 |
| Control Manager Advanced | 510 |
| Enterprise Security for Endpoints - DLP Plug-in | 510 |
| Im Security For Lcs 1.0 | 510 |
| IMSVA 9.X including Base Product, Pre-filter, SPS/ERS, and DLP | 510 |
| InterScan Web Security as a Service | 510 |
| InterScan Web Security Virtual Appliance 6.x English version with DLP | 510 |
| OfficeScan 11.x Multilingual Full Feature | 510 |
| PortalProtect 2.x, Anti-Malware, Content Filter, Advanced DLP,WTP | 510 |
| ScanMail for Exchange Suite with DLP Version 11 | 510 |
| ScanMail for Lotus Domino suite version 5.x with Advanced DLP for Windows and Linux | 510 |
| ServerProtect Linux | 510 |
| Serverprotect Multiplataforma 5X | 510 |
| Trend Micro Endpoint Application Control - Full Package | 510 |
| Trend Micro Endpoint Encryption - Full Disk Encryption and File Encryption | 510 |
| Trend Micro Hosted Email Security 2.0 - ENGLISH | 510 |
| Trend Micro Mobile Security 9.x | 510 |
| Trend Micro Security for Mac 2.0 | 510 |
| Virtual Device Infrastructure Plugin for OfficeScan | 510 |
| Vulnerability Protection 2.0 | 510 |
| Worry-Free Business Security Services ver 3.x | 510 |

3.2. O detalhamento do ambiente tecnológico do CJF está descrito no ANEXO II.

4. DO FORNECIMENTO

4.1.1. O fornecimento dos bens e serviços, descritos neste Termo de Referência, poderá ser composto conforme os seguintes subitens podendo ser composta conforme os seguintes subitens:

4.1.2. Renovação e complementação das licenças atualmente instaladas no CONTRATANTE (subitem 3.1); ou

4.1.3. Substituição da solução de segurança atualmente implantada no CJF.

4.2. Independentemente das opções descritas acima, as soluções ofertadas devem atender integralmente as especificações técnicas deste Termo de Referência e possuir licenciamento para a completa proteção do ambiente tecnológico descrito no subitem 5.1.

## 5. QUANTITATIVOS

5.1. O objeto da contratação é uma solução de segurança, composta por *softwares* com garantia por 60 meses, serviços de instalação e configuração, serviço de transferência de conhecimento e serviço de suporte técnico por 60 meses, contados a partir da emissão do Termo de Recebimento Definitivo.

| Item | Descrição | Quantidade |
|---|---|---|
| **1** | **Solução para proteção de *endpoint*** | |
| 1.1 | Licenciamento da solução para estações de trabalho Windows | 550 |
| 1.2 | Licenciamento da solução para estações de trabalho Linux | 30 |
| 1.3 | Licenciamento da solução para armazenamento centralizado de dados – *Storage* | 2 |
| 1.4 | Serviço de instalação e configuração da solução | 14 |
| 1.5 | Serviço de suporte técnico (mensal) para até 582 licenças | 60 |
| **2** | **Solução de segurança para *datacenter*** | |
| 2.1 | Licenciamento da solução de segurança para datacenter | 32 hosts (64 sockets) ou 750 VMs |
| 2.1 | Serviço de instalação e configuração da solução. | 1 |
| 2.2 | Serviço de suporte técnico (mensal) para até 32 hosts. | 60 |
| **3** | **Transferência de conhecimento (por pessoa).** | 4 |

## 6. DA EXECUÇÃO DO OBJETO

6.1. A solução de segurança para endpoint e datacenter deverá operar de forma integrada, ou seja, os *softwares* fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir gerenciamento integrado, desempenho, disponibilidade e funcionalidades adequados aos requisitos do Conselho.

6.2. Todas as soluções, independentemente do fabricante, deverão atender as condições, características e especificações técnicas previstas neste Termo de Referência e demais itens não previstos que possam influir direta ou indiretamente no ambiente computacional do CONTRATANTE.

6.3. Caso algum *software* que compõe a solução conste em lista de *end-of-support*, *end-of-engineering-support* ou *end-of-life* do fabricante, durante o período de vigência das licenças de uso, a CONTRATADA deverá fornecer, configurar e promover a substituição por novo *software* equivalente, que atenda as especificações técnicas descritas neste Termo e que não impacte na perda de funcionalidade da solução.

6.4. Os *softwares* deverão ser fornecidos em sua versão mais atualizada.

6.5. Caso a solução a ser fornecida, utilize *software* de proteção de *endpoint* diferente do atualmente instalado no CJF, a CONTRATADA deverá providenciar a desinstalação automática de todas as cópias instaladas do *software* em estações e servidores e a instalação do novo *software* em um único processo.

## 7. OBRIGAÇÕES DA CONTRATADA

### 7.1. Obrigações Gerais

7.1.1. Fornecer os *softwares* da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CJF, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

7.1.2. Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

7.1.3. Submeter à prévia aprovação da CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

7.1.4. Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

7.1.5. Sujeitar-se à fiscalização do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

7.1.6. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos *softwares* que compõem a solução.

7.1.7. Não utilizar pessoal técnico já alocado em contratos ou projetos em execução no CONTRATANTE para prestar as atividades objeto da licitação, devendo compor equipe exclusiva para este fim.

7.1.8. Credenciar devidamente um Representante Técnico para, em todas as questões relativas ao cumprimento do objeto, representar a CONTRATADA.

7.1.9. O profissional indicado atuará desde o início da execução do contrato até a conclusão da implantação como Gerente de Projeto, devendo possuir certificação PMP (Project Management Professional).

7.1.10. Realizar a migração de todas políticas, regras e customizações configuradas no CJF em caso de atualização de versão ou troca de produto.

7.1.11. Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

7.1.12. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício de sua atividade.

7.1.13. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridas.

7.1.14. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

7.1.15. Guardar inteiro sigilo dos dados que vier a ter acesso, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

7.1.16. Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado devidamente justificado.

7.1.17. Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1°, da Lei n. 8.666/93, as solicitações do CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado.

7.1.18. Assumir a responsabilidade por danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE.

7.1.19. Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

7.1.20. Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

7.1.21. Corrigir as falhas detectadas pela Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE.

7.1.22. Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO III – Cronograma de Implantação, após a emissão de Ordem de Serviço pelo CONTRATANTE.

7.2. Quanto à entrega, instalação e configuração dos *softwares* da solução.

7.2.1. Iniciar a execução das atividades de entrega, instalação e configuração dos *softwares* da solução de acordo com os prazos definidos no cronograma, contados a partir da emissão de Ordem de Serviço pelo CONTRATANTE.

7.2.2. Até o 3° (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na sede do CONTRATANTE, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução de segurança para proteção de *endpoints* e *datacenter*.

7.2.3. A CONTRATADA deverá apresentar um Plano de Implantação, em até 10 (dez) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos *softwares* que compõe a solução.

7.2.4. O Plano de Implantação deverá dispor também sobre o cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

a) detalhar os procedimentos para entrega e conferência dos *softwares* e acessórios entregues;

b) detalhar informações sobre as etapas de instalação, conexões lógicas necessárias, definição de nomes e de endereçamento de IP;

c) elaborar e documentar topologia lógica de rede, interligando os elementos de conectividade fornecidos aos existentes no CJF;

d) elaborar atividades de teste de operação da solução;

e) elaborar planos de testes para os diversos componentes da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos *softwares* da solução;

f) planejamento para atualização da solução atual ou migração de todas políticas, regras de exceção e todas as demais configurações de proteção atuais para a nova solução;

g) transferência de conhecimento.

7.2.5. Entregar todos os *softwares* e acessórios no prazo máximo de até 15 (quinze) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.

7.2.6. Entregar os *softwares*, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.

7.2.7. Entregar todos os documentos comprobatórios de garantia e suporte técnico indicados nos itens **Erro! Fonte de referência não encontrada.** e **Erro! Fonte de referência não encontrada.**.

7.2.8. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.

7.2.9. Instalar os *softwares* nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica do CONTRATANTE.

7.2.10. A equipe da CONTRATADA deverá possuir certificação emitida pelos fabricantes dos *softwares* da solução ofertada.

7.2.11. Aceitar que as atividades de entrega, instalação e configuração dos *softwares* da solução deverão ocorrer localmente nas dependências do CJF, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O CJF poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção.

7.2.12. Aceitar que o processo de entrega, instalação e configuração dos *softwares* da solução deverão ser acompanhados pela equipe técnica indicada pelo CONTRATANTE.

7.2.13. A execução dos serviços de entrega, instalação e configuração dos *softwares* da solução deverão contemplar, no mínimo, os seguintes itens:

a) instalação física e ativação dos componentes da solução;
b) realizar a integração à rede do CJF, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração da solução, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CJF;
c) instalação e configuração dos *softwares* e funcionalidades exigidas na especificação técnica dos elementos que compõe a solução fornecida, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CJF;
d) realizar testes de operação específicos para a solução de virtualização corporativa que comprovem o atendimento dos requisitos de criação, configuração, alteração da capacidade dos recursos (CPU, RAM e Disco), movimentação entre hosts físicos e entre repositórios de servidores virtuais, sem a necessidade de parada. Os testes deverão ser realizados em servidores virtuais rodando sistemas operacionais Windows e Linux;
e) realizar testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos diversos componentes da solução;
f) atualizar o Plano de Implantação com todas as informações que represente a topologia física e lógica e a configuração final aplicadas;

7.2.14. Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos *softwares*, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO III. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 3

(três) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

7.2.15. Concluir no prazo de 15 (quinze) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação, entrega das licenças de uso e configuração da solução, realizando todas as atividades programadas para esta etapa.

7.2.16. Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, licenciamento, instalação e configuração dos *softwares* da solução. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

7.3. Quanto ao serviço de transferência de conhecimento

7.3.1. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de, no mínimo, 40 (quarenta) horas.

7.3.2. A transferência de conhecimento deverá ser realizada em Brasília/DF e a CONTRATADA deverá providenciar as instalações para este fim.

7.3.3. A transferência de conhecimento deverá conter conteúdo teórico e prático e deverá abordar, no mínimo, os seguintes itens:

a) detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento;

b) orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando todas as funcionalidades exigidas na especificação técnica;

c) orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos e virtuais da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE nos aspectos de rede LAN e backup;

d) orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica.

7.3.4. O programa para a transferência de conhecimento deverá ser previamente aprovado pelo CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

7.3.5. Deverá ser disponibilizado material didático impresso e em mídia, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

7.3.6. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

7.3.7. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço.

7.3.8. Caso a transferência de conhecimento não seja satisfatória em termos de didática ou conhecimento técnico do instrutor, deverá ser realizada transferência de conhecimento complementar, parcial ou total, com o objetivo de suprir os pontos falhos, sem ônus adicional ao CONTRATANTE.

7.3.9. Esta transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes da solução ofertada.

7.4. Quanto ao serviço de garantia da solução

7.4.1. O prazo de garantia e direito a atualização dos *softwares* que compõe a solução é de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo da solução.

7.4.2. Os custos relativos ao serviço de garantia da solução já devem estar incluídos no preço dos próprios itens.

7.4.3. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento e na integração entre os componentes da solução, mediante a substituição de versões dos *softwares* ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nos páginas e manuais de suporte e normas técnicas específicas.

7.4.4. O direito a atualização dos *softwares* obriga a CONTRATADA a disponibilizar a atualização dos *softwares* fornecidos e que compõe a solução tão logo ocorra o lançamento de novos *softwares* em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos *softwares* fornecidos.

7.4.5. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios:

a) Quanto aos *softwares* da solução:

i. A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas nos *softwares* da solução consideradas "*bug de software*".

ii. Será considerado pelo CONTRATANTE como "*bug de software*" o comportamento ou característica dos *softwares* que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados como prejudiciais ao seu correto uso.

iii. Será de exclusiva responsabilidade da CONTRATADA o encaminhamento da falha de *software* ao laboratório do fabricante, o acompanhamento da solução e a aplicação dos respectivo *fix*, *patch* ou pacote de correção em dia e horário a ser definido pelo CONTRATANTE.

iv. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.

v. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os *softwares* objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção.

b) Quanto a integração dos componentes da solução:

i. A CONTRATADA deverá manter, durante a vigência da garantia, a correta integração entre os elementos de *hardware* e *software* que compõem a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do termo de recebimento definitivo.

ii. Quando forem identificadas falhas de funcionamento na solução que não sejam atribuídas diretamente aos elementos de *hardware* ou de *software*, caberá à CONTRADADA a análise e o encaminhamento da solução, buscando restaurar o correto funcionamento do conjunto de elementos da solução.

iii. Serão consideradas como falhas de funcionamento da integração dos componentes a redução significativa do desempenho ou a perda de funcionalidades técnicas disponibilizadas pelo conjunto da solução.

7.4.6. A atualização dos *softwares* fornecidos que compõe a solução deverá ocorrer de acordo com os seguintes princípios:

a) o CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as versões de todos os *softwares* que compõe a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos *softwares*;

b) o direito a atualização de versões dos *softwares* que compõe a solução não poderá gerar qualquer custo adicional para o CONTRATANTE;

c) deverão ser criadas contas de acesso, em nome do CONTRATANTE, no sítio internet do fabricante dos *softwares* que compõe a solução;

d) o perfil das contas criadas em nome do CONTRATANTE deverá permitir de forma irrestrita o download de drivers, firmwares, patches, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos;

e) sempre que solicitado mediante chamado de Suporte Técnico, a CONTRATADA deverá orientar o CONTRATANTE quanto aos procedimentos técnicos para a instalação ou atualização de versões dos *softwares* que compõe a solução.

7.4.7. Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para a emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

a) cessões de direito de uso perpétuo dos *softwares* fornecidos. Os termos de licenciamento de todos os *softwares* fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito pertencentes ao CONTRATANTE;

b) conjunto de direitos de atualização de versão, pelo período de 60 (sessenta) meses de garantia, de todos os *softwares* fornecidos. Abrangerá todos os *softwares* e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão patrimônio do CONTRATANTE.

7.5. Quanto ao serviço de suporte técnico

7.5.1. O serviço de suporte técnico *on-site* deverá ser executado pela CONTRATADA durante o prazo de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos *softwares* da solução.

7.5.2. O serviço de suporte técnico da solução consiste em:

a) atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando à solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação;

b) atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução;

c) realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 4 (quatro) horas a cada visita, visando assegurar o melhor desempenho da solução.

7.5.3. Quando da abertura de chamado técnico de suporte, os chamados deverão ser categorizados em 4 (quatro) níveis, da seguinte forma:

| Criticidade | Descrição | Prazo máximo para início de atendimento (contados a partir da abertura do chamado) | Prazo máximo para restauração de serviço (contados a partir da abertura do chamado) |
|---|---|---|---|
| Severidade 1 (Alta) | Atuação ON-SITE visando sanar problemas que tornem a solução inoperante, causando alto impacto nas operações do CJF. | Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE. | Em até 6 (seis) horas |
| Severidade 2 (Média/Alta) | Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não tornem a solução inoperante, causando impacto no ambiente de produção ou restrição de funcionalidade. | Em até 4 (quatro) horas deve ter um técnico da COTRATADA ON-SITE. | Em até 12 (doze) horas |
| Severidade 3 (Média/Baixa) | Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução integrada de segurança não gerando impacto ao negócio. | Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato. | Em até 24 (vinte e quatro) horas |
| Severidade 4 (Baixa) | Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração. | Em até 12 (doze) horas um técnico da CONTRATADA entra em contato. | Em até 72 (setenta e duas) horas |

7.5.4. O CONTRATANTE realizará a abertura de chamados técnicos de suporte por meio de ligação telefônica e por e-mail ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

7.5.5. A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento Plano de Implantação.

7.5.6. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

7.5.7. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

7.5.8. A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

7.5.9. A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

7.5.10. A CONTRATADA deverá realizar a cada visita, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos *softwares* que compõe a solução de segurança, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

7.5.11. As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), devendo possuir certificação emitida pelos fabricantes dos *softwares* da solução ofertada, devendo ser prestada com acompanhamento da equipe técnica do CJF.

7.5.12. A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo (ANEXO IIII), devendo ocorrer automaticamente em dia e hora previamente agendada com o CJF e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CJF. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança.

7.5.13. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

8. OBRIGAÇÕES DO CONTRATANTE

8.1. Acompanhar e fiscalizar a execução do objeto contratual.

8.2. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.

8.3. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.

8.4. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA.

8.5. Avaliar todos os serviços prestados pela CONTRATADA.

8.6. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal.

8.7. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato.

8.8. Para os serviços inclusos no período de garantia do objeto, a CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

9. GESTÃO E FISCALIZAÇÃO DO CONTRATO

9.1. A autoridade competente designará a equipe de gestão e fiscalização do contrato com as seguintes atribuições:

9.1.1. Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual.

9.1.2. Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação para fiscalizar tecnicamente o contrato.

9.1.3. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa para fiscalizar o contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

9.1.4. Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da solução.

10. FORMA DE PAGAMENTO

10.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos *softwares* da solução e garantia por 60 (sessenta) meses, serviços de instalação e configuração e serviço de

transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no Cronograma (ANEXO III).

10.2. O pagamento do serviço de Suporte Técnico será efetuado mensalmente, sendo iniciado somente após o Recebimento Definitivo da Solução, mediante envio da Nota Fiscal/Fatura pela CONTRATADA.

10.3. O pagamento será realizado no prazo de até 10 (dez) dias úteis contados a partir do recebimento da nota fiscal.

10.4. O servidor indicado para a fiscalização da presente aquisição terá o prazo de 5 (cinco) dias para "ATESTAR" a Nota Fiscal ora mencionada, após a data de apresentação do referido documento a este Órgão.

10.5. As notas fiscais deverão ser emitidas eletronicamente e encaminhadas à Seção de Protocolo e Expedição do CJF, pelo e-mail: protocolo@cjf.jus.br, procedimento adotado pelo CJF.

11. VIGÊNCIA

11.1. A vigência do Contrato será de:

11.1.1. 4 (quatro) meses, contados da assinatura do contrato, para a execução, mediante a emissão da Ordem de Serviços, da entrega, instalação, configuração, transferência de conhecimento e recebimento definitivo.

11.1.2. 60 (sessenta) meses, contados da data de emissão do Termo de Recebimento Definitivo, referente aos serviços de garantia e suporte técnico da solução de segurança para proteção de endpoint e datacenter, relativo aos serviços de natureza contínua desta contratação.

12. LOCAL DE ENTREGA E EXECUÇÃO DOS SERVIÇOS

12.1. A entrega dos *softwares* e acessórios da solução e a realização dos serviços previstos neste termo deverão ser realizados na sede do CONTRATANTE, situada no Setor de Clubes Esportivos Sul - SCES - Trecho III - Pólo 8 - Lote 9 - CEP 70200-003 - Brasília/DF.

12.2. O parque tecnológico do CONTRATANTE está distribuído entre a Sede e sua Gráfica, situada no Setor de Armazenagem e Abastecimento Norte - SAAN Quadra 01 Lote 10/70 - CEP 70.632-100 - Brasília/DF.

13. MODELO DE REMUNERAÇÃO (Glosas)

13.1. O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico por ocorrência, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor na fatura mensal do serviço de suporte técnico (glosa), nos seguintes casos:

13.1.1. Glosa de 6% (seis por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com **severidade alta**, limitada até 06 (seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.2. Glosa de 3% (três por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade **média/alta**, limitada até 12 (doze) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.3. Glosa de 2% (dois por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade **média/baixa**, limitada até 18 (dezoito) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.4. Glosa de 1% (um por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade **baixa**, limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.5. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, a cada ocorrência a CONTRATADA receberá uma Sanção de Advertência, a ser aplicada pela área Administrativa do CONTRATANTE.

13.2. A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços.

13.3. O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os *softwares* da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês.

13.4. No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, durante os últimos 12 (doze) meses, serão aplicadas as Sanções Administrativas previstas no Contrato.

13.5. No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

13.6. Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

13.7. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

14. DAS PENALIDADES

14.1. Pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções:

14.1.1. Advertência.

14.1.2. Multa no percentual correspondente a 0,05% (cinco centésimos por cento), calculada sobre o valor total da contratação, por dia de atraso na entrega do plano de implantação, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos.

14.1.3. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, por dia de atraso na entrega de todos os *softwares* e acessórios da solução, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos, caracterizando inexecução total do contrato.

14.1.4. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, por dia de atraso na conclusão da etapa de instalação e configuração da solução, além dos prazos máximos definidos no CRONOGRAMA (ANEXO III) até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.5. Multa no percentual correspondente a 0,5% (meio por cento), calculada sobre o valor total do serviço de transferência de conhecimento, por dia de atraso na conclusão do serviço de transferência de conhecimento, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.6. Multa no percentual correspondente a 20% (vinte por cento), calculada sobre o valor do suporte técnico mensal, no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, caracterizando inexecução parcial do contrato.

14.1.7. Multa no percentual correspondente a 0,20% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual disposta no item 19.1 deste Termo, no caso de atraso injustificado na sua entrega.

14.1.8. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 10% (dez por cento) sobre o valor da parte não entregue ou não executada.

14.1.9. Multa no valor de 10% (dez por cento), sobre o valor total da contratação, no caso de inexecução total do contrato.

14.1.10. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

14.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE, descontado da garantia contratual ou cobrado judicialmente.

14.3. A reincidência da aplicação de multa ou advertência dará direito ao CJF à rescisão contratual unilateral.

14.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

14.5. SUSPENSÃO TEMPORÁRIA- suspender temporariamente de participação em licitação e impedimento de contratar com a União, nos termos do art. 7° da Lei n. 10.520/2002 c/c o art. 28 do Decreto n. 5.450/2005.

14.6. SUSPENSÃO TEMPORÁRIA - pela inexecução total ou parcial do objeto será suspensa temporariamente de participar de licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos, nos termos inciso 3 do artigo 87 na lei de Licitação 8666/93, bem como conforme Acórdão 2242/2013.

14.7. DECLARAÇÃO DE INIDONEIDADE para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

15. CONFIDENCIALIDADE

15.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:

15.1.1. Política de segurança adotada pelo CJF e configurações de *hardware* e *software* decorrentes.

15.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s).

15.2. A CONTRATADA deverá concordar e assinar Termo de Confidencialidade e Sigilo da Contratada (ANEXO VII), entregando o Termo assinado pelo representante legal da empresa, com firma reconhecida.

16. VISTORIA

16.1. A LICITANTE, caso julgue conveniente para o correto dimensionamento e cumprimento das obrigações, poderá realizar uma vistoria nas instalações do CONTRATANTE para tomar conhecimento

dos serviços a serem realizados. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento dos serviços e de dificuldades técnicas não previstas:

16.1.1. A vistoria técnica deverá ocorrer por horário marcado, e será agendada por meio do telefone (61) 3022-7400/7403.

16.1.2. O agendamento de vistoria poderá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório.

16.1.3. A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.

16.1.4. Detalhes da topologia lógica da rede de dados do CONTRATANTE serão apresentados durante a vistoria somente mediante assinatura de Termo de Confidencialidade e Sigilo do Licitante (ANEXO VI), a ser preenchido e assinado pelo representante legal da empresa.

## 17. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

17.1. A LICITANTE vencedora deverá fornecer declaração comprometendo-se a prestar garantia de, no mínimo, 60 (sessenta) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

17.2. A LICITANTE deverá ofertar Suporte Técnico pelo período de 60 (sessenta) meses, a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

17.3. A proposta deverá indicar, em qual página e item da documentação apresentada, está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I deste Termo de Referência. Não será aceita proposta sem a indicação na documentação técnica apresentada.

17.4. A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.

17.5. Todos os *softwares* especificados deverão ser adquiridos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato.

17.6. A LICITANTE vencedora deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa LICITANTE tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução englobando a instalação e configuração de solução de segurança para proteção de endpoint e a instalação e configuração de solução de segurança para proteção de datacenter.

17.7. Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato.

## 18. PROVA DE CONCEITO

18.1. Poderá ser solicitada, a critério exclusivo do CJF, prova de conceito da solução à empresa classificada, antes da adjudicação, com o objetivo de realizar testes de comprovação de atendimento às especificações e requisitos exigidos nas Especificações Técnicas deste Termo de Referência.

18.2. Para a realização da prova de conceito da solução, a LICITANTE deverá disponibilizar conjunto de elementos da mesma marca, modelo e especificações detalhadas na proposta.

18.3. A realização da prova de conceito deverá ser presencial e realizada, preferencialmente, na Secretaria de Tecnologia da Informação do CJF, localizada na sede do CONTRATANTE, ou, a critério exclusivo do CJF e mediante exposição de motivos, em outro local em Brasília, devendo iniciar no prazo de até 05 (cinco) dias úteis, contados a partir da data de convocação do CONTRATANTE para a realização da prova de conceito.

18.4. A prova de conceito utilizará como base as especificações técnicas constantes neste Termo de Referência e será rejeitada a prova de conceito que:

18.4.1. Apresentar divergências entre as especificações dos *softwares* entregues para a prova de conceito em relação às especificações técnicas da proposta entregue pela LICITANTE; ou

18.4.2. Apresentar versão de *software* diferente da publicada em site oficial do fabricante e disponível para *download* por qualquer cliente; ou

18.4.3. Não comprovar o atendimento de, pelo menos, 1 (um) requisito técnico descrito no ANEXO I - Especificações Técnicas deste Termo de Referência, executada nos *softwares* entregues para a prova de conceito.

18.5. Não será aceita a proposta da LICITANTE que tiver a prova de conceito rejeitada ou não entregue no prazo estabelecido.

18.6. Nesse caso, a proposta subsequente será examinada e, assim, sucessivamente, na ordem de classificação, até a aprovação de uma prova de conceito.

19. GARANTIA DO CONTRATO

19.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, a CONTRATADA se obriga a oferecer, como prestação de garantia, o valor correspondente a 5% (cinco por cento) do valor total contratado, no prazo máximo de 20 (vinte) dias, contados a partir da emissão da Ordem de Serviço.

19.2. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

19.3. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

19.4. O termo da garantia será restituído à CONTRATADA depois de encerrada a vigência contratual, e após o cumprimento integral de todas as obrigações contratuais.

20. DO DESENVOLVIMENTO NACIONAL SUSTENTÁVEL

20.1. Não se aplica, pois, trata-se de solução de *software*.

**CONTRATO N. 031/2018-CJF**

**MÓDULO I-TERMO DE REFERÊNCIA**

**ANEXO I-ESPECIFICAÇÕES TÉCNICAS**

## Item 01 - Solução para proteção de *Endpoint*

### 1. Proteções *anti-malware* específicas para estações de trabalho Windows

1.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

1.1.1. Windows 7 (x86/x64);

1.1.2. Windows 8 e 8.1 (x86/x64);

1.1.3. Windows 10 (x86/x64).

1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais.

1.3. Deve ser integrada ao Centro de Alertas e Segurança (Windows Security Center ou Action Center) quando utilizado plataforma Microsoft.

1.4. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros.

1.5. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

1.5.1. Processos em execução em memória principal (RAM);

1.5.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

1.5.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

1.5.4. Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

1.6. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

1.7. Deve possuir detecção heurística de vírus desconhecidos.

1.8. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada.

1.9. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

1.9.1. Em tempo real de arquivos acessados pelo usuário;

1.9.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

1.9.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

1.9.4. Por linha-de-comando parametrizável;

1.9.5. Automáticos do sistema com as seguintes opções:

a) Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

b) Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

c) Frequência: horária, diária, semanal e mensal;

d) Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

1.10. Deve possuir mecanismo de cache de informações dos arquivos já escaneados.

1.11. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada.

1.12. Deve permitir a utilização de Centro de Inteligência de reputação para análise de arquivos, de modo a prover, rápida detecção de novas ameaças.

1.13. Em caso de problemas com a conectividade com o Centro de Inteligência, o mesmo deve manter uma base local para consulta de no mínimo hash de arquivos.

1.14. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça.

1.15. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante.

1.16. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança.

1.17. Deve permitir a adição automática às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de *endpoint*.

1.18. A solução de antivírus deverá suportar o envio de arquivos suspeitos a solução de análise de ameaças avançadas, apresentado como resultado na alise informações:

1.18.1. Processos de AutoStart;

1.18.2. Modificações de Arquivos de Sistema;

1.18.3. Serviços criados e modificados;

1.18.4. Atividade de Rede Suspeita;

1.18.5. Modificações de Registros.

**2. Proteções anti-malware específicas para estações de trabalho Linux**

2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

2.1.1. Suse Linux Enterprise 11 e 12;

2.1.2. Red Hat Enterprise Linux 6 e 7;

2.1.3. CentOS 6 e 7.

2.2. A solução de proteção deverá ser integrada ao sistema operacional através de módulos existentes do sistema operacional (Kernel Hook ou Fanotify).

2.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados.

2.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais.

2.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, grayware, cavalos de tróia, rootkits, e outros.

2.6. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real.

2.7. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada.

2.8. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador.

2.9. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados.

2.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 10 (dez) níveis recursivos de compactação.

2.11. As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil.

**3. Proteções anti-malware específicas para armazenamento centralizado de dados (*Storage*):**

3.1. A solução deverá ser compatível o Ambiente Computacional do CJF (Anexo II – Resumo do ambiente tecnológico do CJF).

3.2. Deverá possuir compatibilidade com NetApp Data Ontap 8.1.2 ou superior.

3.3. A solução anti-malware deverá possuir a capacidade de negar acesso aos arquivos contaminados.

3.4. A solução anti-malware em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS).

3.5. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o solução anti-malware tomará para arquivos infectados.

3.6. Possibilidade de notificação de eventos e envio de alertas de forma automática para o administrador.

3.7. Armazenamento da ocorrência de vírus em log.

3.8. Possibilidade de funcionamento independente da ferramenta de gerenciamento.

3.9. Possibilidade de retorno de versão anterior das vacinas (rollback).

3.10. Deverá detectar e remover vírus, worms, trojans, spywares e outros tipos de códigos maliciosos.

3.11. O solução anti-malware deverá permitir conexão de atualização em redes que possuam servidor proxy.

3.12. Permitir atualização automática e de forma incremental da base de dados de vacina.

3.13. Deverá fornecer em tempo real o status atualizado da solução anti-malware com no mínimo as seguintes informações: versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema.

3.14. A solução anti-malware deverá permitir gerenciamento gráfico intuitivo portável a console (gerenciamento remoto) e escaneamento centralizado.

3.15. A solução anti-malware poderá ser executada em um servidor dedicado ou ser executada no próprio Sistema de Gerenciamento e Armazenamento de Dados (NAS).

3.16. Caso a solução anti-malware necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos:

3.16.1. Deverá permitir a qualquer momento a incorporação de um novo servidor anti-malware da solução para melhoramento do desempenho;

3.16.2. Deverá permitir o banceamento de carga entre os servidores da solução e operar em alta disponibilidade;

3.16.3. Uma vez um servidor configurado em um Sistema de Gerenciamento e Armazenamento de Dados, a conexão e re-conexão entre eles deverão ocorrer automaticamente.

3.17. A solução anti-malware deverá suportar, no mínimo, 4 (quatro) conexões de, no mínimo, 10 Gbps (dez gigabit por segundo) e o acesso simultâneo de, no mínimo, 50 usuários.

3.18. A solução anti-malware deverá permitir a configuração de escaneamento nas seguintes modalidades:

3.18.1. Escaneamento manual;

3.18.2. Escaneamento em tempo real;

3.18.3. Escaneamento escalonado.

3.19. A solução anti-malware deverá permitir a configuração de uma lista de tipos de extensões predeterminadas pelo administrador do Sistema para os processos de escaneamento.

3.20. A solução deverá mover para área específica e/ou negar acesso aos arquivos contaminados que não forem possíveis de serem limpos.

3.21. A solução deverá acompanhar as requisições de escaneamento de arquivo e retornar o seu resultado.

3.22. A solução em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS).

3.23. Para melhorar o desempenho, diminuir o tráfego e aumentar a velocidade, o Sistema antivírus deverá permitir ao administrador do Sistema a configuração dos seguintes passos:

3.23.1. Configurar o Sistema de Armazenamento de Dados (STORAGE) para enviar ao Sistema antivírus somente arquivos com as extensões especificadas;

3.23.2. Os arquivos do Sistema de Armazenamento de Dados serão marcados como "limpos" se os mesmos forem escaneados antes e solicitados sem nenhuma alteração;

3.23.3. Os arquivos marcados como "limpos" não deverão ser escaneados novamente pelo sistema antivírus.

3.24. A solução deverá possuir rotinas bem definidas de escaneamento, atualizações e de logs.

3.25. Deverá garantir a integridade dos dados e ser capaz de detectar e remover malware conhecidos e desconhecidos.

3.26. A solução deverá utilizar escaneamento recursivo para arquivos compactados.

3.27. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o Sistema tomará para arquivos infectados:

3.27.1. Deixar em quarentena arquivos infectados;

3.27.2. Limpar com backup;

3.27.3. Limpar sem backup;

3.27.4. Excluir arquivo infectado.

3.28. Notificação de eventos e envio de alertas de forma automática para o administrador como resguardo de situação séria, tal como epidemia de vírus ao Sistema de Armazenamento de Dados.

3.29. Armazenamento da ocorrência de malware em log centralizado.

3.30. Possibilidade de colocar arquivos e diretórios em listas de exclusões onde estes não serão verificados pela solução.

3.31. Possibilidade de funcionamento e administração independentes de ferramenta de gerenciamento centralizado.

3.32. Gerenciamento remoto e centralizado da solução.

3.33. Realizar ações específicas para cada tipo de código malicioso.

3.34. Fornecimento de vacina para novos vírus num prazo máximo de 24 (vinte e quatro) horas, a partir do acionamento ao fornecedor.

3.35. Possibilidade de retorno de versão anterior das vacinas.

3.36. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo.

3.37. Permitir o reinício automático dos serviços do malware.

3.38. Proteção no mínimo contra códigos maliciosos classificados como vírus, trojan horses, worms entre outros.

3.39. Suporte compreensível com Help inteligente.

3.40. Da remoção:

3.40.1. Detecção e remoção de malware em tempo real;

3.40.2. Detecção e remoção de malwares, do tipo: Vírus, worms, trojan horses entre outros;

3.40.3. Proteção contra desinstalação e desativação não autorizada do produto.

3.41. Das Atualizações:

3.41.1. Permitir atualização automática e de forma incremental do cartório de vírus e da base de dados de vacina;

3.41.2. Permitir configuração de forma manual para atualizações referentes às mudanças no programa, erros resolvidos e melhorias;

3.41.3. Que a periodicidade e o horário das atualizações também possam ser configuráveis.

3.42. A solução deverá permitir conexão de atualização em redes que possuam servidor Proxy.

3.43. Fornecer em tempo real o status atualizado da solução antimalware com no mínimo as seguintes informações: Versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema (upgrade).

3.44. Se uma nova atualização for disponibilizada à solução de antivírus, o administrador do sistema poderá apagar as informações no cache do sistema para forçar a aplicação de um novo escaneamento, inclusive aqueles arquivos que foram escaneados com a versão antiga.

**4. Módulo de Host IPS e Host Firewall**

4.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.1.1. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);

4.1.2. Windows Server 2012 (32/64-bit);

4.1.3. Windows Server 2016 (32/64-bit);

4.1.4. Windows 7 (x86/x64);

4.1.5. Windows 8 e 8.1 (x86/x64);

4.1.6. Windows 10 (x86/x61).

4.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall.

4.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio).

4.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção.

4.5. Deve possuir regras para controle do tráfego de pacotes de determinadas aplicações.

4.6. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows 7 ou superior, por meio de regras de host ips.

4.7. Deve ser capaz de prevenir intrusões e proteger os *endpoints* garantindo cobertura contra ataques dia zero.

4.8. Deve ser capaz de identificar e bloquear ataques conhecidos através de assinaturas.

4.9. A atualização de assinaturas não deve exigir reinício do sistema operacional.

4.10. Deve efetuar proteção automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade.

4.11. Deve prover proteção contra as vulnerabilidades de aplicações terceiras tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras.

4.12. Deve fornecer proteção contra vulnerabilidades existentes nas estações de trabalho.

4.13. Deve proteger contra ataques locais iniciados por CD's ou dispositivos USB.

4.14. Deve proteger contra ataques que trafegam por fluxos criptografados.

4.15. Deve proteger contra ataque de negação de serviço.

4.16. Deve proteger contra tentativas de invasão.

4.17. Deve possuir proteção contra BOTs .

4.18. Deve permitir a criação de políticas de firewall diferenciadas em múltiplas placas de rede no mesmo sistema operacional.

4.19. Deve permitir a criação de políticas de segurança personalizadas.

4.20. Deve permitir limitar o número de conexões simultâneas no sistema operacional.

4.21. Deve permitir a emissão de alertas via smtp ou snmp.

4.22. Deve permitir criar regras com base nos seguintes parâmetros:

4.22.1. Descrição;

4.22.2. Ação;

4.22.3. Direção;

4.22.4. Protocolo de Rede;

4.22.5. Aplicação e Executáveis;

4.22.6. Tempo de aplicação da regra.

4.23. Deve possuir integração com o Centro de Inteligência do fabricante para verificar a reputação do endereço IP.

4.24. A reputação deve informar quatro níveis:

4.24.1. Mínimo;

4.24.2. Não verificado;

4.24.3. Médio;

4.24.4. Alto.

4.25. Para evitar consumo de banda, a solução deve manter cache para a consulta mencionada no item anterior.

4.26. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas.

4.27. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall.

4.28. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez.

4.29. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas.

4.30. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos.

4.31. 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.

**5. Módulo para controle de aplicações**

5.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

5.1.1. Windows 7 (x86/x64);

5.1.2. Windows 8 e 8.1 (x86/x64);

5.1.3. Windows 10 (x86/x61).

5.2. Deve permitir a criação de políticas de segurança personalizadas.

5.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

5.3.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

5.3.2. Range de endereços IPS;

5.3.3. Sistema operacional;

5.3.4. Grupos de máquinas espelhados do Active Directory;

5.3.5. Usuários ou grupos do Active Directory.

5.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.

5.5. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

5.5.1. Nenhum;

5.5.2. Somente bloqueios;

5.5.3. Somente regras específicas;

5.5.4. Todas as aplicações executadas.

5.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs.

5.7. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política.

5.8. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se.

5.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário.

5.10. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados.

5.11. As políticas de segurança devem permitir o controle através de regras de aplicação.

5.12. As regras de controle de aplicação devem permitir as seguintes ações:

5.12.1. Permissão de execução;

5.12.2. Bloqueio de execução;

5.12.3. Bloqueio de novas instalações.

5.13. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra.

5.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

5.14.1. Hash do executável;

5.14.2. Atributos do certificado utilizado para assinatura digital do executável;

5.14.3. Caminho lógico do executável;

5.14.4. Base de assinaturas de certificados digitais válidos e seguros.

5.15. As regras de controle de aplicação devem possuir categorias de aplicações.

5.16. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

5.17. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas.

5.18. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos.

5.19. 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.

**6. Módulo contra vazamento de informações – DLP**

6.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

6.1.1. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
6.1.2. Windows Server 2012 (32/64-bit);
6.1.3. Windows Server 2016 (32/64-bit);
6.1.4. Windows 7 (x86/x64);
6.1.5. Windows 8 e 8.1 (x86/x64);
6.1.6. Windows 10 (x86/x64).

6.2. Deve possuir nativamente templates para atender as seguintes regulamentações:

6.2.1. PCI/DSS;
6.2.2. HIPA;
6.2.3. Glba;
6.2.4. SB-1386;
6.2.5. US PII.

6.3. Deve ser capaz de detectar informações, em documentos nos formatos:

6.3.1. Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;

6.3.2. Gráficos: visio, postscript, pdf, tiff,
6.3.3. Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;
6.3.4. Códigos: c/c++, java, verilog, autocad.

6.4. Deve ser capaz de detectar informações, com base em:

6.4.1. Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;

6.4.2. Palavras ou frases configuráveis;

6.4.3. Expressões regulares;

6.4.4. Extensão dos arquivos.

6.5. Deve ser capaz de detectar em arquivos compactados.

6.6. Deve permitir a configuração de quantas camadas de compressão serão verificadas.

6.7. Deve permitir a criação de modelos personalizados para identificação de informações.

6.8. Deve permitir a criação de modelos com base em regras e operadores lógicos.

6.9. Deve possuir modelos padrões.

6.10. Deve permitir a importação e exportação de modelos.

6.11. Deve permitir a criação de políticas personalizadas.

6.12. Deve permitir a criação de políticas baseadas em múltiplos modelos.

6.13. Deve permitir mais de uma ação para cada política, como:

6.13.1. Apenas registrar o evento da violação;

6.13.2. Bloquear a transmissão;

6.13.3. Gerar alertar para o usuário;

6.13.4. Gerar alertar na central de gerenciamento;

6.13.5. Capturar informação para uma possível investigação da violação.

6.14. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede.

6.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

6.15.1. Cliente de e-mail;

6.15.2. Protocolos http, https, ftp;

6.15.3. Mídias removíveis;

6.15.4. Discos óticos cd/dvd;

6.15.5. Gravação cd/dvd;

6.15.6. Aplicações de mensagens instantâneas;

6.15.7. Tecla de print screen;

6.15.8. Aplicações p2p;

6.15.9. Área de transferência do Windows;

6.15.10. Webmail;

6.15.11. Armazenamento na nuvem (cloud);

6.15.12. Impressoras;

6.15.13. Scanners;

6.15.14. Compartilhamentos de arquivos;

6.15.15. Activesync;

6.15.16. Criptografia PGP;

6.15.17. Portas com, lpt, firewire (ieee 1394);

6.15.18. Modems;

6.15.19. Infravermelho;

6.15.20. Bluetooth.

6.16. Deve permitir a criação de exceções nas restrições dos meios de transmissão.

## 7. Módulo de proteção para Office 365

7.1. Aplicar proteções anti-malware para a proteção dos serviços Exchange Online, SharePoint Online e OneDrive for Business da Microsoft.

7.2. Detectar ameaças, exploração de documentos em nuvem, reputação web e inteligência em nuvem.

7.3. Realizar análise dinâmica com sandbox para investigar o comportamento de arquivos suspeitos não apenas correspondência padrão estática e coloca em quarentena arquivos e e-mails prejudiciais.

7.4. Empregar detecção de malware por meio de sandbox sem assinaturas, para diminuir seu risco de violação.

7.5. Monitorar o comportamento real de arquivos suspeitos em ambientes sandbox virtuais usando múltiplas versões de sistemas operacionais e aplicações.

7.6. Detectar exploração de documentos para encontrar malware escondido dentro de formatos de arquivos comuns do Office, como Word, PowerPoint e Excel.

7.7. Realizar integração nuvem-a-nuvem, através de API da Microsoft, realizando a análise de malware em sandbox.

7.8. Integrar diretamente com a Microsoft dispensando o redirecionamento de tráfego de e-mail.

7.9. Tornar visível o uso de dados sensíveis no Exchange, SharePoint e OneDrive for Business.

7.10. Monitorar em tempo real para bloquear, colocar em quarentena, ou fazer relatórios de políticas de conformidade.

## 8. Funcionalidades gerais de atualização

8.1. 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.

8.2. Deve permitir atualização incremental da lista de definições de vírus.

8.3. 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.

8.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines.

8.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas.

8.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento.

8.7. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

8.8. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

## 9. Funcionalidades gerais de administração

9.1. 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.

9.2. Deve possibilitar instalação "silenciosa".

9.3. Deve permitir o bloqueio por nome de arquivo.

9.4. Deve permitir o travamento de pastas e diretórios.

9.5. Deve permitir o travamento de compartilhamentos.

9.6. Deve permitir o rastreamento e bloqueio de infecções.

9.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks.

9.8. 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.

9.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro *software* ou agente.

9.10. Deve permitir a desinstalação através do servidor ou console de gerenciamento da solução.

9.11. Deve ter a possibilidade de exportar e importar configurações da solução.

9.12. A solução deve permitir a geração de backup ou snapshots da base de dados e dos demais componentes (Chaves Criptográficas) através da console de gerenciamento.

9.13. Deve ter a possibilidade de determinar a capacidade ou prazo de armazenamento da área de quarentena.

9.14. Deve permitir a deleção dos arquivos quarentenados.

9.15. Deve permitir remoção automática de clientes inativos por determinado período de tempo.

9.16. Deve permitir integração com Active Directory para acesso a console de administração.

9.17. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada.

9.18. Deve permitir criação de diversos perfis e usuários para acesso a console de administração.

9.19. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante.

9.20. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP.

9.21. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento.

9.22. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional.

9.23. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus.

9.24. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias.

9.25. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web ou console MMC.

9.26. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção.

9.27. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory.

9.28. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio.

9.29. Deve permitir a criação de usuários locais de administração da console de anti-malware.

9.30. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware.

9.31. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento.

9.32. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador.

9.33. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks.

9.34. Deve permitir a gerência de domínios separados para usuários previamente definidos.

9.35. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração.

9.36. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

**10. Funcionalidades gerais de controle de dispositivos**

10.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.

10.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total.

10.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão.

10.4. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total.

10.5. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

**11. Funcionalidades gerais anti-ransonware**

11.1. Deve utilizar mecanismos de proteção específicos contra ataques ransonware.

**12. Funcionalidades gerais de *Machine Learning***

12.1. Deve ter a capacidade de implementar a funcionalidade de "Machine Learning" utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos, como também as características de boa pontuação.

12.1.1. Exploração de navegadores com reputação de URL;

12.1.2. Websites infectados com reputação de URL;

12.1.3. Office Exploits com reputação de URL;

12.1.4. Arquivos anexos com reputação de arquivos;

12.1.5. Download de arquivos com reputação de arquivos;

12.1.6. Execução do instalador de *software* com classificação comportamental do instalador (boa e ruim);

12.1.7. Execução do malware de *software* com classificação comportamental do instalador (boa e ruim);

12.1.8. A funcionalidade de "Machine Learning" deve trabalhar baseado no mínimo nas seguintes premissas:

12.1.9. Atualização da base de reputação das URL's com a periodicidade mínima de 1 hora;

12.1.10. Bloqueio de URL's de má reputação;

12.1.11. Bloqueio das instruções de "Command & Control";

12.1.12. Atualização da base de reputação de Arquivos com a periodicidade mínima de 1 hora;

12.1.13. Bloqueio da ameaças polimorfas mesmo que arquivos desconhecidos;

12.1.14. Prevenção de Falso Positivos;

12.1.15. Bloqueio de malwares desconhecidos e suas variantes;

12.1.16. Implementar a classificação comportamental dos arquivos;

12.1.17. "Aprendizado" a partir dos indicadores de compromisso (IoC).

12.2. A funcionalidade de "Machine Learning" deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:

12.2.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;

12.2.2. Arquivos de *softwares* mundialmente espalhados na rede mundial de computadores;

12.2.3. Sites Web mundialmente espalhados pela rede mundial de computadores.

**Item 02 - Solução de Segurança para *Datacenter***

1. Deve aplicar ao ambiente de servidores de rede (*datacenter*) as mesmas proteções especificadas no Item 1 – Solução para proteção de *endpoints*

2. Deve oferecer proteção proativa contra ataques tipo Dia-Zero para no mínimo:

2.1. Deve impedir a exploração maliciosa de sistemas e aplicações;

2.2. Deve prevenir a entrada e distribuição de códigos maliciosos.

3. Deve ser uma solução específica e otimizada para funcionar e interoperar com ambiente virtual VMware bem como com a plataforma de virtualização de redes e segurança VMware NSX.

4. Deve implementar Controle de Aplicação, Controle de Integridade e Inspeção de Log.

5. Deve implementar, sem necessidade de agente: Antimalware, Firewall e IPS de host no ambiente virtual de servidores.

6. Deve suportar vMotion.

7. Deve ter a capacidade de integração nativa com a tecnologia VMWare NSX atuando de forma automática para isolar um determinado servidor virtual infectado.

8. Deve ter a capacidade de liberar apenas alguns serviços quando identificado como infectado.

9. Deve manter em conformidade com as políticas de seguranças através de verificações continua em clientes e servidores.

10. Deve efetuar "hardening" de sistemas operacionais, aplicações e bancos de dados.

11. Deve conter políticas de segurança nativas para aplicativos Microsoft.

12. Deve conter políticas de "hardening" padrões e nativas, possibilitando o fechamento do *hardware*, protegendo aplicativos de alto risco e base de dados, contra arquivos executáveis não autorizados a "rodar".

13. Deve impedir a execução de aplicações não autorizadas.

14. Deve permitir ao Administrador bloquear trafego por porta, por protocolo, por IP ou por faixa de endereços IP.

15. Proteger arquivos e registros do sistema baseado em políticas.

16. Monitorar arquivos e registros do sistema baseado em políticas.

17. Deve possuir Sistema de Prevenção de Intrusos.

18. Deve possuir Sistema de Detecção de Intrusos.

19. Deve permitir ao administrador configurar filtros de eventos para encaminhamento ao servidor de gerenciamento.

20. Deve possuir sistema de atualização automática de políticas e pacotes de relatórios a partir do site do fabricante.

21. Deve ter a capacidade de importar e exportar políticas customizadas ou de terceiros.

22. Deve ter e capacidade de controlar o comportamento detectando e prevenindo ações especificas que uma aplicação ou usuários executem de forma a prejudicar o funcionamento do sistema ou aplicativo.

23. Deve possuir sistema de criação de usuários com perfis diferenciados de acesso aos recursos da console de gerenciamento.

24. Deve permitir o envio de alertas através de e-mail e SNMP baseados em filtros de eventos recebidos pela console de gerenciamento.

25. Deve possuir políticas predefinidas de monitoramento, de no mínimo os seguintes recursos:

25.1. Falha de acesso;

25.2. Logon com sucesso;

25.3. Detecção de logoff remoto;

25.4. Alteração de configuração pelo Usuário;

25.5. Alteração no grupo de gerenciamento.

26. Deve monitorar arquivos e eventos em servidores mesmo sem o agente instalado.

27. Deve possuir recurso de prevenção contra acesso indevido de usuários e de aplicações a outros recursos do sistema, como arquivos, processos, bibliotecas e registros.

28. Deve ter a capacidade de através do recurso de controle de aplicação, monitorar com opção de bloqueio, as atividades da aplicação, assim como o recurso de rede e de dispositivos.

29. Deve ter a capacidade de prevenção contra ataques de exploração, com regras pré-definidas baseadas no comportamento padrão das aplicações do servidor.

30. Deve ter a capacidade de prevenção de intrusão baseado no comportamento das aplicações.

31. Possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção.

32. Implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas.

33. Permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema.

34. Deve possuir recurso nativo de firewall, restringindo atividades de rede por IP e Porta nos sentidos de entrada e saída.

35. Deve ter a capacidade de prevenção contra alteração maliciosa de privilégios do servidor.

36. Deve conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo as aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache, Adicionar principais soluções que vocês possuam.

37. Deve ter a capacidade de prevenir contra alterações maliciosa em arquivos e registros do servidor.

38. Deve ter a capacidade de proteção contra execução de instalações e operações maliciosas no servidor.

39. Deve ter a capacidade de monitorar mídias removíveis proteger contra malwares.

40. Possuir capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos.

41. Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura.

42. Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs.

43. Implementar inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor.

44. Deve ter a opção de monitoramento granular de arquivos e diretórios dos servidores e estações.

45. Deve ter a capacidade de prevenir a adição de códigos em processos em memória para servidores Windows (memory injection protection).

46. Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros, possibilitando a coleta de logs de gerenciamento e correlação em "real-time".

47. Deve ter a capacidade de monitor alterações em arquivos críticos do sistema operacional e diretórios das aplicações críticas.

48. A solução deve ter a capacidade de no mínimo:

48.1. Bloquear o uso de aplicações indevidas;

48.2. Proteger o "core" do sistema operacional.

49. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos.

50. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

50.1. Origem confiável;

50.2. Origem não confiável;

50.3. Comportamento do arquivo.

51. Capacidade de implementar regras distintas por grupo.

52. Capacidade de identificar e proteger ataques direcionados, impossibilitando o início do ataque e não somente impedindo as ações após invasão do equipamento.

53. A solução deve implementar em um único agente as funcionalidades de HIPS, HIDS e Host Firewall.

54. A solução deve ser suportada, no mínimo, na versão VMware ESX v6 ou superior.

55. A solução deve suportar, no mínimo, a instalação dos binários do agente nos seguintes sistemas operacionais:

55.1. Suse Linux Enterprise 11 e 12;
55.2. Red Hat Enterprise Linux 6 e 7;
55.3. Centos 6 e 7;
55.4. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
55.5. Windows Server 2012 (32/64-bit);
55.6. Windows Server 2016 (32/64-bit).

# CONTRATO N. 031/2018-CJF

## MÓDULO I-TERMO DE REFERÊNCIA

## ANEXO II-RESUMO DO AMBIENTE TECNOLÓGICO DO CJF

### 1. Plataforma de Videoconferência

| Equipamento/*Software* | Descrição | Quantidade |
|---|---|---|
| Sistema de Unidade de Controle Multiponto (MCU) | Marca Avaya; Modelo Scopia Elite 6110 | 1 |
| Terminal de Comunicação FULLHD (1080p) CODEC | Marca Avaya; Modelo Scopia XT5000 + Scopia XT3WAY Microphone POD | 4 |
| Monitor LED | Marca Samsung; Modelo ED46D | 8 |
| Sistema de Acesso via PC e dispositivos móveis | Marca Avaya; Modelo Scopia Elite 6110 SFTW Licensing/PKG Scopia Management | 10 |

### 2. Plataforma de *Hardware*

| Tipo do Ativo | Marca/Modelo do Ativo | Descrição | Quantidade |
|---|---|---|---|
| **Servidores Rack** | IBM RISC pSeries p630 - 7028-6C4 | 4x 36GB HD, 12 GB de memória, 4 Processadores RISC Power4+, 1 Unidade fita DAT. | 2 |
| | DELL / PE R720 | 32 GB de memória, 2 x Quad Core Intel Xeon E5-2660 | 2 |
| **Servidores Blade** | Chassis HP c7000 | Cada chassi com 6 fontes | 2 |
| | HP / BL460C | Servidor de dois processadores de núcleo óctuplo com 256GB de RAM | 23 |
| **Storages** | NetApp FAS2040 | 2 Controladoras e uma capacidade de 40T bruto sendo 3 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP. Data-on-Tap 7.3.7 | 1 |
| | NetApp FAS6290 | 2 Controladoras e uma capacidade de 200TB sendo 5 shelves com discos SATA e 5 shelves com discos SAS. Suporte para FCP, NFS, HTTP. Data-on-Tap 8.2 | 1 |
| **Tape Library (Biblioteca Robotizada)** | QUANTUM / Scalar i500 | Biblioteca composta por 4 drives LTO 5, com capacidade para 179 fitas LTO5, conexão via Fibre Channel | 1 |
| **Escâner** | Kodak i3400 | Kodak i3400 com mesa digitalizadora padrão A3 | 5 |
| **Estações de trabalho** | Dell Optiplex 7010 | Desktop Core i7 8GB RAM 1TB HDD | 400 |
| | HP Elitebook 810 | Notebook | 17 |

| Tipo do Ativo | Marca/Modelo do Ativo | Descrição | Quantidade |
|---|---|---|---|
| **Switches de Convergência** | Cisco Nexus 5548UP | 2 switches topo de rack com 48 portas sendo 16 FC de 8Gb/s e 32 Ethernet de 10Gb/s para rede local Storage/Blade | 2 |
| **Switches de Core** | H3C / S7506E | Concentradores da Rede Local 48 Portas Ethernet 10/100/1000 Mbps, 2 módulos de comunicação 10GB com 8 portas cada, 2 módulos Compat Flash com 2 portas 10GB | 2 |
| **Switches de Acesso** | H3C / S5500 | Switchs ethernet 24 portas 10/100/1000 Mbps com Uplink 10Gbps e alimentação redundante | 34 |
| **Controlador Rede Wireless** | H3C / WX2200 | Switch para Gerência Wireless com 3 portas | 1 |
| **Access Points (APs)** | H3C / AP3950 | Acesso Rede Wireless 802.11a/b/g/n | 40 |

**3. Plataforma de Segurança**

| Tipo do Proteção | Marca/Modelo do Ativo | Descrição | Quantidade |
|---|---|---|---|
| **Borda** | Fortinet FortiGate 1500D | Firewall UTM com 4 portas 10 Gbps e 8 portas 1 Gbps | 2 |
| | Fortinet FortiWeb 3000D | Firewall de aplicação Web - WAF | 2 |
| | Fortinet FortiSandbox 2000E | Sandbox para emulação e análise de malwares | 1 |
| **E-mail** | Trend Micro InterScan Messaging Security Virtual Appliance | Ferramenta de segurança de borda (MTA) para proteção anti-malware de e-mail | 2 |
| | Trend Micro ScanMail for Microsoft Exchange | Ferramenta de segurança para proteção anti-malware para Microsoft Exchange | 2 |
| | Fortinet FortiMail VM | Ferramenta de segurança de borda (MTA) para proteção anti-malware de e-mail | 1 |
| **Datacenter** | Trend Micro Deep Security | Anti-malware para servidores de rede | 400 |
| **Endpoint** | Trend Micro OfficeScan | Anti-malware para estações de trabalho | 500 |

| Tipo do Proteção | Marca/Modelo do Ativo | Descrição | Quantidade |
|---|---|---|---|
| | Trend Micro Vulnerability Protection | Bloqueio contra exploração de vulnerabilidades conhecidas (virtual patch) | 500 |
| | Trend Micro Endpoint Application Control | Controle de aplicações instaladas nas estações de trabalho | 500 |
| **Mobile** | Trend Micro Mobile Security for Enterprise | Proteção para smartphones | 10 |
| **Ferramentas de Gerência** | Trend Micro Control Manager | Gerenciador dos produtos Trend Micro | 1 |
| | Trend Micro Smart Protection Server | Servidor de atualização e de verificação de reputação de arquivos que se comunica com a nuvem da Trend Micro | 1 |
| | Symantec Control Compliance Suite Vulnerabily Manager | Solução para gestão de vulnerabilidades de segurança dos ativos de TI | 1 |
| | Fortinet FortiAnalyzer VM | Gerenciamento centralizado de segurança | 1 |
| | Fortinet FortiAnalyzer VM | Centralizador de logs dos produtos Fortinet | 1 |

**4. Plataforma de *Software***

O quadro a seguir apresenta os sistemas operacionais, aplicativos, *softwares* de gerência, SGBDs, servidores de aplicação, servidores web e ferramentas em uso no CJF:

| Software | Nome/Versão | Descrição |
|---|---|---|
| **Sistema Operacional** | MS / Windows 2003, 2008, 2008 R2 e 2012 Server | Sistema Operacional de 32 bits e 64 bits |
| | MS / Windows 7 Pro (Port) e Windows 10 | Sistema Operacional de 64 bits |
| | Suse Linux 9,10, 11 e 12 | Sistema Operacional de 32 bits e 64 bits |
| | IBM AIX 6.1 | Sistema Operacional de 32 bits |
| | Oracle Linux 4/5/6/7 | Sistema Operacional de 64 bits |
| | CentOS 4/5/6 | Sistema Operacional de 32 bits e 64 bits |
| | Red Hat Linux 5, 6 e 7 | Sistema Operacional de 32 bits e 64 bits |
| **Servidores Aplicações** | IIS 6.0 (Internet Information Services) | Servidor de Aplicações Microsoft ASP / HTML |

| Software | Nome/Versão | Descrição |
|---|---|---|
| | Oracle 11g v11.2.03 | Sistema gerenciador de banco de dados Oracle |
| | ODI 10 / Sunopsis | Ferramentas ETL Oracle Data Integrator e Sunopsis |
| **Solução de Gerenciamento de Identidades e Controle de Acesso** | Novell Identity Manager 2.7<br>Novell Access Manager 2.6.0<br>Novell iManager 2.7.0<br>Provisioning Module for Novell Identity Manager 2.7<br>Microsoft Active Directory 2008 | Solução de Gerenciamento de Identidades e Controle de Acesso |
| **Servidores Web** | Mailman 2.1.15 | Servidor de Listas de Discussão |
| | IMAP 4.1.3 | Servidor de POP IMAP Courier |
| | PostFix 2.4.3 | Servidor de SMTP |
| | Open LDAP | Servidor de Diretórios |

## 5. CERTIFICAÇÃO DIGITAL

5.1. Certificado Digital Padrão ACJUS da cadeia ICP-Brasil.

**CONTRATO N. 031/2018-CJF**

**MÓDULO I-TERMO DE REFERÊNCIA**

**ANEXO III-CRONOGRAMA DE IMPLANTAÇÃO**

| **Prazo Máximo (em dias corridos)** | **Cronograma de Atividades da Prestação dos Serviços** | **Responsável** |
|---|---|---|
| D | Emissão da Ordem de Serviço. | CJF e CONTRATADA |
| D + 3 | Reunião de Planejamento. | CJF e CONTRATADA |
| D + 10 | Entregar o Plano de Implantação contendo o planejamento para a implantação da solução. Comprovar que os técnicos envolvidos nos procedimentos e atividades de implantação são certificados pelo fabricante da solução. Entrega dos *softwares* e documentações. | CONTRATADA |
| 3 dias após a etapa anterior | Emitir o **Termo de Recebimento Provisório** após a entrega do *software* e das documentações (**P**). | CJF |
| P + 15 | Finalizar o serviço de instalação, licenciamento, configuração e funcionamento perfeito de todos os *softwares* da solução em sua última versão. Entregar toda documentação técnica dos procedimentos executados durante a implantação. | CONTRATADA |
| 10 dias após a etapa anterior | Emitir o **Termo de Recebimento Definitivo** após a verificação do atendimento de todas obrigações contratuais previstas para a etapa de instalação e configuração da solução. | CJF |

**CONTRATO N. 031/2018-CJF**

**MÓDULO I-TERMO DE REFERÊNCIA**

**ANEXO IV-TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA**

1. A empresa **ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA**, pessoa jurídica com sede em SCN Quadra 1, Bloco F, Salas 501 a 503, Edifício América Office Tower, Asa Norte, Brasília – DF. CEP: 70.711-905, inscrita no CNPJ/MF n. 21.547.011/0001-66, neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do Contrato n. 031/2018-CJF.

3. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado

entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília- DF, 19 de dezembro de 2018.

**MÁRCIA DE CARVALHO**
Diretora-Executiva de Administração e
de Gestão de Pessoas do Conselho da Justiça Federal

**MURILO ROSSETTO**
Diretor da Alltech Soluções em Tecnologia Ltda.

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

# CONTRATO N. 031/2018-CJF

## MÓDULO II-PLANILHA DE PREÇOS

| Item | Descrição | Quantidade | Unitário | Total |
|---|---|---|---|---|
| **1** | **Solução para proteção de *endpoint*** | | | |
| 1.1 | Licenciamento da solução para estações de trabalho Windows | 550 | R$ 378,28 | R$ 208.054,00 |
| 1.2 | Licenciamento da solução para estações de trabalho Linux | 30 | R$ 378,28 | R$ 11.348,40 |
| 1.3 | Licenciamento da solução para armazenamento centralizado de dados/Storage | 2 | R$ 14.752,80 | R$ 29.505,60 |
| 1.4 | Serviço de instalação e configuração da solução | 1 | R$ 9.500,00 | R$ 9.500,00 |
| 1.5 | Serviço de suporte técnico (mensal) para até 582 licenças | 60 | R$ 1.110,20 | R$ 66.612,00 |
| | | | **Total Item 01** | **R$ 325.020,00** |
| **2** | **Solução de segurança para *datacenter*** | | | |
| 2.1 | Licenciamento da solução de segurança para *datacenter* **(32 hosts (64 sockets) ou 750 VMs)** | 18 | R$ 30.000,00 | R$ 540.000,00 |
| 2.2 | Serviço de instalação e configuração da solução. | 1 | R$ 9.502,40 | R$ 9.502,40 |
| 2.3 | Serviço de suporte técnico (mensal) para até 32 hosts. | 60 | R$ 2.174,96 | R$ 130.497,60 |
| | | | **Total Item 02** | **R$ 680.000,00** |
| **3** | **Transferência de conhecimento (por pessoa).** | 3 | R$ 7.703,50 | R$ 23.110,50 |
| | | | **Total Item 03** | R$ 23.110,50 |

| | |
|---|---|
| **Total da Contratação** | **R$ 1.028.130,50** |