PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 005/2016 – CJF

PROCESSO N. CJF-ADM-2015/0058

PREGÃO ELETRÔNICO N.02/2016 - CJF

DADOS DA EMPRESA
CONTRATADA: GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA
CNPJ/MF: 08.366.661/0001-47
ENDEREÇO: SCN Quadra 4, Bloco "B", Sala 1302-M, Centro Empresarial Varig, Brasília - DF
TELEFONE: (61) 3327-2777 (61) 3321-0901
E-MAIL: ronaldo@globalip.com.br
SIGNATÁRIO EMPRESA: RONALDO DE ALBUQUERQUE RIBEIRO - Diretor Comercial
SIGNATÁRIO CJF: EVA MARIA FERREIRA BARROS - Diretora-Geral

DADOS DO CONTRATO
OBJETO: contratação, sob demanda, de solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, com garantia de 24 meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico
FUNDAMENTAÇÃO LEGAL: Lei n. 10.520/2002, Decreto n. 5.450/2005, Decreto n. 7.892/2013, Lei Complementar n. 123/2006, Decreto n. 8.538/2015, Lei n. 8.666/1993, Decreto 7.174/2010, Lei n. 12.846/2013, e, em conformidade com as informações constantes no Processo n.CJF-ADM-2015/0058.
VIGÊNCIA: _____/_____/_____ a _____/_____/_____
VALOR DO CONTRATO: R$ 1.479.734,00
UNIDADE FISCALIZADORA: STI
OBSERVAÇÕES: a) Clausula 11ª – garantia contratual: 5%, no prazo máximo de 20 (vinte) dias, contado da assinatura do Contrato; b) Cláusula 6ª – vigência: **28 meses** sendo: 6.1.1. **04 (quatro) meses**, contados da emissão da Ordem de Serviço, destinados a execução da entrega, instalação e configuração e transferência de conhecimento. 6.1.2. **24 (vinte e quatro) meses**, contados da data de emissão do Termo de Recebimento Definitivo, referente à garantia e suporte técnico da solução unificada de segurança para proteção de e-mail e endpoint contra ataques avançados.

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 005/2016 - CJF

Contrato firmado entre o **CONSELHO DA JUSTIÇA FEDERAL** e a empresa **GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA**, para contratação, sob demanda, de solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados.

CONTRATANTE: **A UNIÃO** por intermédio do **CONSELHO DA JUSTIÇA FEDERAL - CJF**, Órgão integrante do Poder Judiciário, inscrito no 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-Geral, a Senhora **EVA MARIA FERREIRA BARROS**, brasileira, inscrita no CPF/MF n. 188.490.083-68, portadora da Carteira de Identidade n. 666.351- SSP/DF, residente e domiciliada em Brasília - DF.

CONTRATADA: **GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA**, inscrita no CNPJ/MF n. 08.366.661/0001-47, com sede no SCN Quadra 4, Bloco "B", Sala 1302-M, Centro Empresarial Varig, Brasília - DF, neste ato representada pelo Diretor Comercial, o Senhor **RONALDO DE ALBUQUERQUE RIBEIRO**, brasileiro, inscrito no CPF/MF n. 498.123.511-91 e portador da Carteira de Identidade n. 1.232.450 – SSP/DF, residente e domiciliado em Brasília - 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, regulamentada pelo Decreto n. 8.538, de 06 de outubro de 2015, na Lei n. 8.666, de 21 de junho de 1993 e alterações, Decreto 7.174 de 12 de maio de 2010 e ainda na Lei n. 12.846, de 1º de agosto de 2013, em conformidade com as informações constantes no Processo n.CJF-ADM-2015/0058, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1.O objeto deste Contrato consiste na contratação, SOB DEMANDA, de solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de 24 meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, conforme especificado no Termo de Referência (Módulo I) do edital, na proposta comercial e tudo que consta do Pregão Eletrônico n. 02/2016, que ficam fazendo parte integrante do presente contrato, independentemente de sua transcrição.

1.1.O detalhamento do objeto é apresentado no Anexo I - Termo de Referência e seus anexos, os quais aderem a este Contrato e dele fazem parte, independentemente de transcrição.

CLÁUSULA SEGUNDA – DO FORNECIMENTO

2.1. Os fornecimentos/serviços serão prestados em estrita observância as determinações, forma e condições constantes no Edital do Pregão Eletrônico n. 02/2016 seus Módulos e na proposta da CONTRATADA.

2.2. A entrega do objeto deste Contrato deverá ser realizada na sede do CONTRATANTE, localizado no Setor de Clubes Esportivos Sul SCES, Trecho III, Lote 9, Polo 8, Brasília - DF. Em dia de expediente normal do CONTRATANTE, das 9h às 19h.

2.3. O fornecimento dos bens e serviços, descritos neste Contrato, poderá ser composto conforme os seguintes subitens:

2.3.1. Renovação e complementação das licenças, *MCAfee - Intel Security*, atualmente instaladas no CONTRATANTE (subitem 3.1) do Anexo I - Termo de Referência, ou

2.3.2. Substituição da solução de segurança atualmente implantada no CONTRATANTE.

2.4. Independentemente das opções descritas acima, as soluções devem possuir licenciamento para a completa proteção do ambiente tecnológico descrito no subitem 3.1 do Anexo I - Termo de Referência deste Contrato.

CLÁUSULA TERCEIRA – EXECUÇÃO DO OBJETO

3.1. A solução unificada de segurança para proteção de *e-mail* e *endpoint* contra-ataques avançados deverá operar de forma unificada, ou seja, todos os equipamentos, *softwares* fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir a perfeita integração entre todos os pontos da solução, seja em *gateway* ou *endpoint*, para a proteção do ambiente tecnológico do CJF.

3.2. Todos componentes da solução de unificada de segurança para proteção de *e-mail* e *endpoint* contra-ataques avançados deverão ser do mesmo fabricante, visando a plena compatibilidade, o gerenciamento centralizado e completa integração de todos os itens da solução.

3.3 Todas as soluções, independentemente do fabricante, deverão atender as

condições, características e especificações técnicas previstas no Anexo I - Termo de Referência e demais itens não previstos que possam influir direta ou indiretamente no ambiente computacional do CONTRATANTE, bem como nos aspectos de disponibilidade e segurança requeridos.

3.4 Toda a solução deverá ser compatível com o ambiente tecnológico do CJF - Anexo II do Termo de Referência.

3.5 Os modelos e versões dos equipamentos (*hardware*) que compõe a solução deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato.

3.6 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 Anexo I - Termo de Referência, que não impacte na perda de funcionalidade da solução.

3.7 As licenças de uso de *software* necessárias para o funcionamento dos diversos elementos da solução serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante ou seu representante.

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

3.9 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.

CLÁUSULA QUARTA - OBRIGAÇÕES DA CONTRATADA

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

4.1.1 Fornecer os equipamentos e *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.

4.1.2 Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Contrato.

4.1.3 Submeter à prévia aprovação do CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

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

4.1.5 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.

4.1.6 Prestar as atividades objeto do Contrato, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e *softwares* que compõem a solução.

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

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

4.1.9 Indicar profissional com certificação PMP (*Project Management Professional*) que atuará desde o início da execução do Contrato até a conclusão da implantação da solução como Gerente de Projeto.

4.1.10 Responsabilizar-se por todos os ônus referentes aos serviços 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.

4.1.11 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.

4.1.12 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.

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

4.1.14 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.

4.1.15 Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1°, da Lei n. 8.666/1993, as solicitações do CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto contratado.

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

4.1.17 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.

4.1.18 Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito,

qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

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

4.1.20 Executar as atividades previstas no Contrato em estrito cumprimento aos prazos previstos no Anexo III do Termo de Referência - Cronograma de Implantação, após a emissão de Ordem de Serviço pelo CONTRATANTE.

4.2 Quanto à entrega, instalação e configuração dos equipamentos e *softwares* da solução

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

4.2.2 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 unificada de segurança para proteção de *e-mail* e *endpoint* contra-ataques avançados.

4.2.3 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 equipamentos e *softwares* que compõe a solução.

4.2.4 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, retirada das embalagens e conferência dos equipamentos, *softwares* e acessórios entregues;

b) detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos *racks*, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência 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 equipamentos e *softwares* da solução;

f) transferência de conhecimento.

4.2.5 Entregar todos os equipamentos e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.

4.2.6 Entregar os equipamentos devidamente protegidos e embalados;

originais e lacrados, os quais devem evitar danos de transporte e manuseio.

4.2.7 Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE.

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

4.2.9 Entregar todos os documentos comprobatórios de garantia e suporte técnico indicados nos itens 6.4 e 6.5, do Anexo I - Termo de Referência, deste Contrato.

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

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

4.2.12 A equipe da CONTRATADA deverá possuir certificação emitida pelos fabricantes dos equipamentos e *softwares* da solução ofertada e deverá estar qualificada a configurar os componentes da atual infraestrutura do CJF, conforme equipamentos, modelos e versões informados no Anexo II do Termo de Referência - Ambiente Tecnológico do CJF.

4.2.13 Aceitar que as atividades de entrega, instalação e configuração dos equipamentos e *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.

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

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

4.2.16 Instalação física e ativação dos equipamentos da solução.

4.2.17 Realizar a integração dos novos equipamentos às redes 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 dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CJF.

4.2.18 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.

4.2.19 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*.

4.2.20 Realizar testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos diversos componentes da solução.

4.2.21 Atualizar o Plano de Implantação com todas as informações que represente a topologia física e lógica e a configuração final aplicadas.

4.2.22 Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no Anexo III do Termo de Referência - Cronograma de Implantação. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório 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.

4.2.23 Concluir no prazo de 30 (trinta) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação, entrega das licenças de uso e configuração dos equipamentos e *softwares* da solução, realizando todas as atividades programadas para esta etapa.

4.2.24 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 equipamentos e *softwares* da solução. O recebimento definitivo realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

4.3 Quanto ao serviço de serviço de transferência de conhecimento

4.3.1 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 80 (oitenta) horas.

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

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

4.3.4 Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento.

4.3.5 Orientar sobre os componentes, procedimentos de instalação e administração da solução unificada de segurança contra ataques avançados direcionados para e-mail e endpoint, explorando todas as funcionalidades exigidas na especificação técnica.

4.3.6 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.

4.3.7 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.

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

4.3.9 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).

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

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

4.3.12 Para todos os efeitos, inclusive de emissão do Termo de Recebimento Definitivo, a transferência de conhecimento faz parte do processo de implantação da solução.

4.3.13 Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos carga horária, programa apresentado e estrutura de, deverá ser realizado novamente, sem ônus adicional ao CONTRATANTE.

4.3.14 Esta transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e *softwares* da solução ofertada.

4.4 Quanto ao serviço de garantia da solução

4.4.1 O prazo de garantia dos equipamentos e direito a atualização dos *softwares* que compõe a solução é de 24 (vinte e quatro) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo da solução.

4.4.2 Os custos relativos ao serviço de garantia dos equipamentos e *softwares* que compõe a solução já devem estar incluídos no preço dos próprios itens.

4.4.3 O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos *softwares* e na integração entre os componentes da solução, mediante a substituição de equipamentos e 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.

4.4.4 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.

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

a) Quanto aos equipamentos da solução:

i. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia.

ii. Substituir, no prazo de 8 (oito) horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas.

iii. Nos casos em que não seja possível o reparo dentro do prazo estipulado acima, substituir no prazo máximo de 72 (setenta e duas) horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso.

iv. Substituir, no prazo de 120 (cento e vinte) horas, qualquer equipamento, componente ou periférico por outro original e novo, na ocorrência dos seguintes casos:

- Se for constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada.
- Se no período de 15 (quinze) dias corridos, contados após a abertura de chamado de Suporte Técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes.

v. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.

vi. Devolver, em perfeito estado de funcionamento, no prazo máximo de 15 (quinze) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

vii. 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 Contrato ou no uso dos acessos, privilégios ou informações obtidos em função das atividades por estes executadas.

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

b) 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. Serão 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.

c) 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.

4.4.6 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 compõem a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos *softwares*.

b) o direito a atualização de versões dos *softwares* que compõem 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 deverão 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.

4.4.7 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) Certificado de garantia de que todos os equipamentos que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, com prazo de solução de até 8 (oito) horas, pelo período de 24 (vinte e quatro) meses totais exigidos no item 6.4.1.

i. Caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados.

b) 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.

c) Conjunto de direitos de atualização de versão, pelo período de 24 (vinte e quatro) 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.

4.5 Quanto ao serviço de suporte técnico

4.5.1 O serviço de suporte técnico *on-site* para os equipamentos e *softwares* que compõe a solução deverá ser executado pela CONTRATADA durante o prazo de 24 (vinte e quatro) 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 equipamentos e *softwares* da solução.

4.5.2 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 a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução (equipamentos e *softwares*), 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 a cada mês, e com duração de pelo menos 4 (quatro) horas a cada visita, visando assegurar o melhor desempenho da solução.

d) substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

4.5.3 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 CONTRATADA 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 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

4.5.4 O CONTRATANTE realizará a abertura de chamados técnicos de suporte por meio de ligação telefônica, por *e-mail* ou via *Internet*, em período integral, 24 (vinte

e quatro) horas por dia, 07 (sete) dias por semana.

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

4.5.6 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.

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

4.5.8 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.

4.5.9 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.

4.5.10 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 equipamentos e *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.

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

4.5.12 A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo (Anexo III do Termo de Referência - Cronograma de Implantação), 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.

4.5.13 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.

a) receber cópia do Termo de Recebimento Provisório (TRP) após entrega da subscrição e demais documentações, conforme descrito no Anexo III do Termo de Referência - Cronograma de Implantação. A finalização da entrega deverá ser formalizada mediante

comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 5 (cinco) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

b) receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à entrega da subscrição e demais documentações. O recebimento definitivo realizar-se-á no prazo máximo de 5 (cinco) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

c) executar as atividades previstas neste Contrato em estrito cumprimento aos prazos previstos no Anexo III do Termo de Referência - Cronograma de Implantação;

d) não transferir no todo ou em parte, a execução do serviço objeto deste Contrato;

e) manter, durante a execução deste contrato as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA QUINTA– OBRIGAÇÕES DO CONTRATANTE

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

5.2 Acompanhar e fiscalizar a execução do objeto contratual.

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

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

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

5.6 Avaliar todos os serviços prestados pela CONTRATADA.

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

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

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

CLÁUSULA SEXTA – DA VIGÊNCIA DO CONTRATO

6.1. Este Contrato terá vigência de **28 (vinte e oito) meses** sendo:

6.1.1. **04 (quatro) meses**, contados da emissão da Ordem de Serviço, destinados a execução da entrega, instalação e configuração e transferência de conhecimento.

6.1.2. **24 (vinte e quatro) meses**, contados da data de emissão do Termo de Recebimento Definitivo, referente à garantia e suporte técnico da solução unificada de segurança para proteção de e-mail e endpoint contra ataques avançados.

CLÁUSULA SÉTIMA – DO PREÇO E DO VALOR DO CONTRATO

7.1. O preço que o CONTRATANTE se obriga a pagar à CONTRATADA, nos termos deste Contrato, é de **R$ 1.479.734,00 (um milhão quatrocentos e setenta e nove mil setecentos e trinta e quatro reais),** conforme especificado no Anexo II - Planilha de Preços deste Contrato, e do qual serão feitas as glosas e retenções legais.

7.2. 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 deste Contrato.

CLÁUSULA OITAVA – RECURSOS FINANCEIROS

8.1. As despesas com a execução do presente contrato correrão à conta de recursos orçamentários da União destinados ao CONTRATANTE consignados no PTRES: 085321, no Elemento de Despesa 3390.39 e 4490.39, com a respectiva emissão das notas de empenhos n.ºs 2016NE000234 e 2016NE000236.

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

CLÁUSULA NONA – ACOMPANHAMENTO 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.

CLÁUSULA DÉCIMA – DO PAGAMENTO

10.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos equipamentos, *softwares*, serviços de instalação e configuração e garantia por 24 (vinte e quatro) meses, após receber cópia do Termo de Recebimento Definitivo; os documentos de cobrança deverão ser emitidos eletronicamente e encaminhados à Seção de Protocolo e

Expedição do Conselho da Justiça Federal, pelo e-mail: protocolo@cjf.jus.br, e será pago com os recursos consignados ao Conselho da Justiça Federal, no Orçamento Geral da União.

10.2. A CONTRATADA deverá emitir nota fiscal/fatura do serviço contratado somente após a emissão pelo CONTRATANTE do Termo de Recebimento Definitivo.

10.3. O pagamento do serviço de Suporte Técnico Será efetuado mensalmente, após envio da fatura pela CONTRATADA, podendo ser iniciado somente após e a emissão do Termo de Recebimento Definitivo.

10.4. O pagamento será efetuado após o recebimento definitivo. Esse caracterizar-se-á pelo recebimento circunstanciado do Atesto da Nota Fiscal, que ficará a cargo do fiscal deste Contrato. Após o recebimento definitivo, o crédito será realizado em conta corrente bancária através de ordem bancária, a qual será emitida até o décimo dia útil. Na Nota Fiscal deverá constar o número da conta corrente, o nome do banco e o código da agência da CONTRATADA.

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

10.6. 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.

10.7. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor deste Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas, nos termos do item 12 do Anexo I - Termo de Referência.

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA CONTRATUAL

11.1. Para o integral cumprimento de todas as obrigações contratuais assumidas, nos termos do art. 56, §1º da Lei n. 8.666/1993, a CONTRATADA deverá entregar ao CONTRATANTE, no prazo máximo de 20 (vinte) dias, contado da assinatura deste Contrato, garantia correspondente a 5% (cinco por cento) do valor total contratado.

11.2. 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.

11.3. 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.

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

11.5. 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.

11.6. 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.

11.7. 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.

11.8. 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.

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

CLÁUSULA DÉCIMA SEGUNDA – DAS PENALIDADES

12.1. 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:

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

12.1.2 **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 Anexo III do Termo de Referência – Cronograma de Implantação, até o limite de 30 (trinta) dias corridos.

12.1.3 **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 equipamentos e acessórios da solução, além do prazo máximo definido no Anexo III do Termo de Referência - Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

12.1.4 **Multa** no percentual correspondente a 0,15% (quinze décimos 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 Anexo III do Termo de Referência – Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do Contrato.

12.1.5 **Multa** no percentual correspondente a 1% (um 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 Anexo III do Termo de Referência – Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do Contrato.

12.1.6 **Multa** no percentual correspondente a 1% (um por cento), calculada sobre o valor total da contratação, 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.

12.1.7 **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 18 deste Contrato, no caso de atraso injustificado na sua entrega.

12.1.8 A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 20% (vinte por cento) sobre o valor da parte não entregue ou não executada.

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

12.2 O período de atraso será contado em dias corridos.

12.3 No caso de aplicação de multa, a CONTRATADA deverá efetuar o recolhimento aos cofres da União do valor devido no prazo máximo de 15 (quinze) dias, contados do recebimento do ofício de notificação.

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

12.5 Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA ao CONTRATANTE, este será encaminhado para inscrição em dívida ativa.

12.6 A aplicação das sanções acima não prejudicará a imposição de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

12.7. 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 n. 10.520/2002, aplicando-lhes, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

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

12.9. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores - SICAF.

12.10. Nos termos do §3º do art. 86 e do §1º 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.

12.11. 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.

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

CLÁUSULA DÉCIMA TERCEIRA – RESCISÃO

13.1. O presente contrato poderá ser rescindido a juízo do CONTRATANTE, com base nos artigos 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 QUARTA – DA PUBLICAÇÃO

14.1. 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 QUINTA – DAS DISPOSIÇÕES GERAIS

15.1. 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 artigo 393 do Código Civil, enquanto tais motivos perdurarem.

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

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

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

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

15.6. 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, na Seção de Protocolo e Expedição - SEPEXP.

CLÁUSULA DÉCIMA SEXTA – FORO

16.1. O Foro 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 02 (duas) vias de igual teor, um dos quais destinada à CONTRATADA, o que, depois de lido e achado conforme, vai assinado pelos representantes das partes contratantes.

Brasília-DF, 19 de abril de 2016.

EVA MARIA FERREIRA BARROS
Diretora – Geral do
Conselho da Justiça Federal

RONALDO DE ALBUQUERQUE RIBEIRO
Diretor Comercial da
Global Ip Tecnologia da Informação Ltda

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO I AO CONTRATO N. 005/2016 - CJF

TERMO DE REFERÊNCIA

1. OBJETO

Contratação, SOB DEMANDA, de solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de 24 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. (...)

3. DESCRIÇÃO DOS PRODUTOS

3.1 Quadro demonstrativo da situação atual de licenças – Solução McAfee – Intel Security:

SKU	Descrição	Quantidade de licenças
EMG4500BARMA	McAfee Email Gateway	01
ESGYCM-AA	McAfee Email Gateway	570
EPAYFM-AA	McAfee Endpoint Protection - Advanced Suite	570
NAPYCM-AB	McAfee VirusScan for Storage	02

3.1. Ambiente tecnológico do CJF para dimensionamento da complementação de licenças da atual solução ou fornecimento de licenças de outros fabricantes:

Descrição	Quantidade
Estações de trabalho - Windows	550
Estações de trabalho - Linux	50
Estações de trabalho - Mac	10
Servidores Windows	150
Servidores Linux	300
Armazenamento Centralizado de Dados - Storage	02
E-mail Gateway	02
Hosts VMware/ CPUs (*sockets*)	18/ 36
Proteção contra ataques avançados	02
Gerência da solução	01

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

4. DO FORNECIMENTO

4.1. 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:

4.1.1. Renovação e complementação das licenças McAfee – Intel Security atualmente instaladas no CONTRATANTE (subitem 3.1); ou

4.1.2. Substituição da solução de segurança atualmente implantada no CONTRATANTE.

4.2. Independentemente das opções descritas acima, as soluções devem possuir licenciamento para a completa proteção do ambiente tecnológico descrito no subitem 3.1.

5. DA EXECUÇÃO DO OBJETO

5.1. A solução de unificada de segurança para proteção de *e-mail* e *endpoint* contra ataques avançados deverá operar de forma unificada, ou seja, todos os equipamentos, *softwares* fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir a perfeita integração entre todos os pontos da solução, seja em *gateway* ou *endpoint*, para a proteção do ambiente tecnológico do CJF.

5.2. Todos componentes da solução de unificada de segurança para proteção de *e-mail* e *endpoint* contra ataques avançados deverão ser do mesmo fabricante, visando a plena compatibilidade, o gerenciamento centralizado e completa integração de todos os itens da solução.

5.3. 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, bem como nos aspectos de disponibilidade e segurança requeridos.
5.4. Toda a solução deverá ser compatível com o ambiente tecnológico do CJF (ANEXO II)
5.5. Os modelos e versões dos equipamentos (*hardware*) que compõe a solução deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato.
5.6. 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.
5.7. As licenças de uso de *software* necessárias para o funcionamento dos diversos elementos da solução serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante ou seu representante.
5.8. Os *softwares* deverão ser fornecidos em sua versão mais atualizada.
5.9. 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.

6. OBRIGAÇÕES DA CONTRATADA

6.1. Obrigações Gerais

6.1.1. Fornecer os equipamentos e *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.
6.1.2. Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.
6.1.3. Submeter à prévia aprovação da CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.
6.1.4. Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.
6.1.5. Sujeitar-se à fiscalização da 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.
6.1.6. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e *softwares* que compõem a solução.
6.1.7. 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.
6.1.8. Credenciar devidamente um Representante Técnico para, em todas as questões relativas ao cumprimento do objeto, representar a CONTRATADA.
6.1.9. Indicar profissional com certificação PMP (Project Management Professional) que atuará desde o início da execução do contrato até a conclusão da implantação da solução como Gerente de Projeto.
6.1.10. 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.
6.1.11. 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.
6.1.12. 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.
6.1.13. Guardar inteiro sigilo dos dados que vier a ter acesso, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.
6.1.14. 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.

6.1.15. Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações da CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado.
6.1.16. 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.
6.1.17. 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.
6.1.18. Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.
6.1.19. Corrigir as falhas detectadas pela Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE.
6.1.20. 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

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

6.2.1. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e *softwares* da solução de acordo com os prazos definidos no cronograma, contados a partir da emissão de Ordem de Serviço pelo CONTRATANTE.
6.2.2. 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 unificada de segurança para proteção de e-mail e *endpoint* contra ataques avançados.
6.2.3. 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 equipamentos e *softwares* que compõe a solução.
6.2.4. 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:
g) Detalhar os procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, *softwares* e acessórios entregues.
h) Detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP.
i) Elaborar e documentar topologia lógica de rede, interligando os elementos de conectividade fornecidos aos existentes no CJF.
j) Elaborar atividades de teste de operação da solução.
k) Elaborar planos de testes para os diversos componentes da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos equipamentos e *softwares* da solução.
l) Transferência de conhecimento.
6.2.5. Entregar todos os equipamentos e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.
6.2.6. Entregar os equipamentos devidamente protegidos e embalados, originais e lacrados, os quais devem evitar danos de transporte e manuseio.
6.2.7. Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE.
6.2.8. Entregar os equipamentos e *softwares*, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.
6.2.9. Entregar todos os documentos comprobatórios de garantia e suporte técnico indicados nos itens 6.4 e 6.5.
6.2.10. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.
6.2.11. Instalar os equipamentos e *softwares* nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica do CONTRATANTE.
6.2.12. A equipe da CONTRATADA deverá possuir certificação emitida pelos fabricantes dos equipamentos e *softwares* da solução ofertada e deverá estar qualificada a configurar os componentes da atual infraestrutura do CJF, conforme equipamentos, modelos e versões informados no ANEXO II - Ambiente Tecnológico do CJF.
6.2.13. Aceitar que as atividades de entrega, instalação e configuração dos equipamentos e *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.

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

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

a) Instalação física e ativação dos equipamentos da solução.

b) Realizar a integração dos novos equipamentos às redes 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 dos equipamentos, 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.

6.2.16. Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, 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 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

6.2.17. Concluir no prazo de 30 (trinta) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação, entrega das licenças de uso e configuração dos equipamentos e *softwares* da solução, realizando todas as atividades programadas para esta etapa.

6.2.18. 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 equipamentos e *softwares* da solução. O recebimento definitivo realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

6.3. Quanto ao serviço de serviço de transferência de conhecimento

6.3.1. 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 80 (oitenta) horas.

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

6.3.3. 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 unificada de segurança contra ataques avançados direcionados para e-mail e *endpoint*, 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.

6.3.4. O programa para a transferência de conhecimento deverá ser previamente aprovado pelo

CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.
6.3.5. 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).
6.3.6. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.
6.3.7. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço na reunião de planejamento.
6.3.8. Para todos os efeitos, inclusive de emissão do Termo de Recebimento Definitivo, a transferência de conhecimento faz parte do processo de implantação da solução.
6.3.9. Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos carga horária, programa apresentado e estrutura de, deverá ser realizado novamente, sem ônus adicional ao CONTRATANTE.
6.3.10. Esta transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e *softwares* da solução ofertada.

6.4. Quanto ao serviço de garantia da solução

6.4.1. O prazo de garantia dos equipamentos e direito a atualização dos *softwares* que compõe a solução é de 24 (vinte e quatro) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo da solução.
6.4.2. Os custos relativos ao serviço de garantia dos equipamentos e *softwares* que compõe a solução já devem estar incluídos no preço dos próprios itens.
6.4.3. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos *softwares* e na integração entre os componentes da solução, mediante a substituição de equipamentos e 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.
6.4.4. 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.
6.4.5. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios:
d) Quanto aos equipamentos da solução:
ix. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia.
x. Substituir, no prazo de 8 (oito) horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas.
xi. Nos casos em que não seja possível o reparo dentro do prazo estipulado acima, substituir no prazo máximo de 72 (setenta e duas) horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso.
xii. Substituir, no prazo de 120 (cento e vinte) horas, qualquer equipamento, componente ou periférico por outro original e novo, na ocorrência dos seguintes casos:
- Se for constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada.
- Se no período de 15 (quinze) dias corridos, contados após a abertura de chamado de Suporte Técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes.

xiii. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.
xiv. Devolver, em perfeito estado de funcionamento, no prazo máximo de 15 (quinze) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.
xv. 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 obtidos em função das atividades por estes executadas.

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

e) Quanto aos *softwares* da solução:

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

v. 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.

vi. Serão 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.

f) Quanto a integração dos componentes da solução:

iv. 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.

v. 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.

vi. 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.

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

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

g) O direito a atualização de versões dos *softwares* que compõem a solução não poderá gerar qualquer custo adicional para o CONTRATANTE.

h) Deverão ser criadas contas de acesso, em nome do CONTRATANTE, no sítio internet do fabricante dos *softwares* que compõe a solução.

i) O perfil das contas criadas em nome do CONTRATANTE deverão permitir de forma irrestrita o *download* de *drivers*, *firmwares*, *patches*, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos.

j) 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.

6.4.7. 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:

d) Certificado de garantia de que todos os equipamentos que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, com prazo de solução de até 8 (oito) horas, pelo período de 24 (vinte e quatro) meses totais exigidos no item 6.4.1.

ii. Caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados.

e) 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.

f) Conjunto de direitos de atualização de versão, pelo período de 24 (vinte e quatro) 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.

6.5. Quanto ao serviço de suporte técnico

6.5.1. O serviço de suporte técnico *on-site* para os equipamentos e *softwares* que compõe a solução deverá ser executado pela CONTRATADA durante o prazo de 24 (vinte e quatro) 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 equipamentos e *softwares* da solução.

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

e) Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução (equipamentos e *softwares*), permitindo o retorno à condição normal de operação.

f) 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.

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

h) Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

6.5.3. 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 CONTRATADAON-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 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 CONTRATADAentra em contato.	Em até 72 (setenta e duas) horas

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

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

6.5.6. 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.

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

6.5.8. 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.

6.5.9. 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.

6.5.10. 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 equipamentos e *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.

6.5.11. As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), devendo possuir certificação emitida pelos fabricantes dos equipamentos e *softwares* da solução ofertada, devendo ser

prestada com acompanhamento da equipe técnica do CJF.
6.5.12. 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.
6.5.13. 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.

7. OBRIGAÇÕES DO CONTRATANTE

7.1. Acompanhar e fiscalizar a execução do objeto contratual.
7.2. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.
7.3. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.
7.4. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA.
7.5. Avaliar todos os serviços prestados pela CONTRATADA.
7.6. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal.
7.7. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato.
7.8. Para os serviços inclusos no período de garantia do objeto, a Contratante permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

8. GESTÃO E FISCALIZAÇÃO DO CONTRATO

8.1. A autoridade competente designará a equipe de gestão e fiscalização do contrato com as seguintes atribuições:
8.1.1. Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual.
8.1.2. Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação para fiscalizar tecnicamente o contrato.
8.1.3. 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.
8.1.4. 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.

9. FORMA DE PAGAMENTO

9.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos equipamentos, *softwares*, serviços de instalação e configuração e garantia por 24 (vinte e quatro) meses, após receber cópia do Termo de Recebimento Definitivo.
9.2. O pagamento do serviço de Suporte Técnico será efetuado mensalmente, após envio da fatura pela CONTRATADA, podendo ser iniciado somente após a emissão do Termo de Recebimento Definitivo.

10. (...)

11. LOCAL DE ENTREGA E EXECUÇÃO DOS SERVIÇOS

11.1. A entrega dos equipamentos, *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.
11.2. 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.

12. MODELO DE REMUNERAÇÃO (Glosas)

12.1. O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor na fatura mensal do serviço de suporte

técnico (glosa), nos seguintes casos:

12.1.1. Glosa de 5% (cinco 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).

12.1.2. 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).

12.1.3. 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).

12.1.4. Glosa de 1% (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 baixa**, limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

12.1.5. 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.

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

12.3. O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os equipamentos e *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.

12.4. 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 meses, serão aplicadas as Sanções Administrativas previstas no Contrato.

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

12.6. 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.

12.7. 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.

13. DAS PENALIDADES

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

13.1.1. Advertência.

13.1.2. 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.

13.1.3. 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 equipamentos e acessórios da solução**, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

13.1.4. Multa no percentual correspondente a 0,15% (quinze décimos 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.

13.1.5. Multa no percentual correspondente a 1% (um 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.

13.1.6. Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total da contratação, **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.

13.1.7. 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 18 deste Termo, **no caso de atraso injustificado na sua entrega.**
13.1.8. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 20% (vinte por cento) sobre o valor da parte não entregue ou não executada.
13.1.9. Multa no valor de 10% (dez por cento), sobre o valor total da contratação, **no caso de inexecução total do contrato.**
13.1.10. 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.
13.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE, descontado da garantia contratual ou cobrado judicialmente.
13.3. A reincidência da aplicação de multa ou advertência dará direito ao CJF à rescisão contratual unilateral.
13.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

14. CONFIDENCIALIDADE

14.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:
14.1.1. Política de segurança adotada pelo CJF e configurações de *hardware* e *software* decorrentes.
14.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s).
14.1.3. Qualquer informação do CONTRATANTE que venha tomar conhecimento em razão da execução dos serviços.
14.2. 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.

15. VISTORIA

15.1. 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:
15.1.1. A vistoria técnica deverá ocorrer por horário marcado, e será agendada por meio do telefone (61) 3022-7400/7403.
15.1.2. O agendamento de vistoria poderá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório.
15.1.3. A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.
15.1.4. 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.

16. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1. A LICITANTE vencedora deverá fornecer declaração comprometendo-se a prestar garantia de, no mínimo, 24 (vinte e quatro) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).
16.2. A LICITANTE deverá ofertar Suporte Técnico pelo período de 24 (vinte e quatro) meses, a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).
16.3. 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.
16.4. 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.
16.5. Todos os equipamentos e *softwares* especificados deverão ser adquiridos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato.
16.6. 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 e-mail, solução de segurança para proteção de *endpoint* e solução de segurança contra Ataques Avançados Persistentes – APT.

16.7. 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.

17. PROVA DE CONCEITO

17.1. 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 caso a documentação entregue pela LICITANTE seja considerada insuficiente para comprovar o atendimento a todos os itens exigidos.

17.2. Para a realização da prova de conceito da solução, a LICITANTE deverá disponibilizar conjunto de elementos que atendas as funcionalidades: solução de segurança para proteção de e-mail, solução de segurança para proteção de *endpoint* e solução de segurança contra Ataques Avançados Persistentes – APT, devendo ser da mesma marca, modelo e especificações detalhadas na proposta.

17.3. 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, em dias úteis, ou, a critério exclusivo do CJF e mediante exposição de motivos, em qualquer cidade brasileira, 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.

17.4. O CONTRATANTE, a seu critério, poderá prorrogar a duração da prova de conceito por mais 02 (dois) dias úteis.

17.5. A prova de conceito utilizará como base as especificações técnicas constantes neste Termo de Referência.

17.6. Será rejeitada a prova de conceito que:

17.6.1. Não comprovar o atendimento de, pelo menos, 01 (um) requisito técnico descrito no ANEXO I - Especificações Técnicas deste Termo de Referência, executada nos equipamentos e *softwares* entregues para a prova de conceito.

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

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

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

18. GARANTIA DO CONTRATO

18.1. 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.

18.2. 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.

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

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

19. DOCUMENTOS ANEXOS

19.1. Seguem anexos a este Termo de Referência os seguintes documentos:

19.1.1. Anexo I – Especificação Técnica da Solução.

19.1.2. Anexo II – Ambiente Tecnológico do CJF.

19.1.3. Anexo III – Cronograma de Implantação.

19.1.4. Anexo IV – Planilha de Preços.

19.1.5. (...).

19.1.6. (...)

19.1.7. (...)

ANEXO I DO TERMO DE REFERÊNCIA DO CONTRATO N. 005/2016 -CJF

ESPECIFICAÇÕES TÉCNICAS

SOLUÇÃO UNIFICADA DE SEGURANÇA PARA PROTEÇÃO DE E-MAIL E *ENDPOINT* CONTRA ATAQUES AVANÇADOS

1. SOLUÇÃO PARA PROTEÇÃO DE *ENDPOINT*

1.1. **Funcionalidade de proteção *anti-malware* para Windows**

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

a) Windows Server 2003 sp2 (32/64-bit);
b) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
c) Windows Server 2012 (32/64-bit);
d) Windows XP sp2 / sp3 (x86/x64);
e) Windows 7 (x86/x64);
f) Windows 8 e 8.1 (x86/x64);
g) Windows 10 (x86/x64).

1.1.2. 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;

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

1.1.4. A Solução deverá possuir integração nativa com a solução listada no Item 3**Erro! Fonte de referência não encontrada.** – Solução Proteção Contra Ameaças Avançadas;

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

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

a) Processos em execução em memória principal (RAM);
b) Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
c) Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;
d) Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

1.1.7. 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;

1.1.8. Deve possuir detecção heurística de vírus desconhecidos;

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

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

a) Em tempo real de arquivos acessados pelo usuário;
b) Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
c) Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
d) Por linha-de-comando, parametrizável, com opção de limpeza;
e) Automáticos do sistema com as seguintes opções:

- Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- Frequência: horária, diária, semanal e mensal;
- Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

1.1.11. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

1.1.12. 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;

1.1.13. Deve permitir a utilização de Centro de Inteligência de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

1.1.14. 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 e URL's maliciosas;
1.1.15. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;
1.1.16. 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;
1.1.17. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
1.1.18. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
1.1.19. 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;
1.1.20. A solução de antivírus devera submeter arquivos suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na alise informações;
a) Processos de AutoStart;
b) Modificações de Arquivos de Sistema;
c) Serviços criados e modificados;
d) Atividade de Rede Suspeita;
e) Modificações de Registros.
1.1.21. A solução de análise de ameaças avançadas deverá realizar automaticamente o bloqueio em ações suspeitas nos Desktops infectados com aquela ameaça analisada em sandbox.

1.2. **Funcionalidade de proteção anti-malware para estações Linux**

1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
a) Suse Linux Enterprise 9, 10 e 11;
b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0;
c) Centos 4.0, 5.0 e 6.0.
1.2.2. A solução de proteção deverá ser integrada ao sistema operacional através de módulos existentes do sistema operacional (Kernel Hook ou Fanotify);
1.2.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;
1.2.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;
1.2.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, grayware, cavalos de tróia, rootkits, e outros;
1.2.6. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;
1.2.7. 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;
1.2.8. 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;
1.2.9. 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;
1.2.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;
1.2.11. As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil.

1.3. **Funcionalidade anti-malware para armazenamento centralizado de dados (*Storage*):**

1.3.1. A solução deverá ser compatível o Ambiente Computacional do CJF (ANEXO II);
1.3.2. Deverá possuir compatibilidade com NetApp Data Ontap 8.1.2 ou superior;
1.3.3. A solução anti-malware deverá possuir a capacidade de negar acesso aos arquivos contaminados;
1.3.4. A solução anti-malware em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS);
1.3.5. 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;

1.3.6. Possibilidade de notificação de eventos e envio de alertas de forma automática para o administrador;
1.3.7. Armazenamento da ocorrência de vírus em log;
1.3.8. Possibilidade de funcionamento independente da ferramenta de gerenciamento;
1.3.9. Possibilidade de retorno de versão anterior das vacinas (rollback);
1.3.10. Deverá detectar e remover vírus, worms, trojans, spywares e outros tipos de códigos maliciosos;
1.3.11. O solução anti-malware deverá permitir conexão de atualização em redes que possuam servidor proxy;
1.3.12. Permitir atualização automática e de forma incremental da base de dados de vacina;
1.3.13. 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;
1.3.14. A solução anti-malware deverá permitir gerenciamento gráfico intuitivo portável a console (gerenciamento remoto) e escaneamento centralizado;
1.3.15. A solução anti-malware poderá ser executada em um servidor dedicado ou ser executada no próprio Sistema de Gerenciamento e Armazenamento de Dados (NAS);
1.3.16. Caso a solução anti-malware necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos:
a) Deverá permitir a qualquer momento a incorporação de um novo servidor anti-malware da solução para melhoramento do desempenho;
b) Deverá permitir o escalonamento Round Robin, isto é, se o primeiro servidor estiver ocupado, a solicitação é enviada ao próximo servidor disponivel;
c) Uma vez um servidor configurado em um Sistema de Gerenciamento e Armazenamento de Dados, a conexão e re-conexão entre eles deverão ocorrer automaticamente.
1.3.17. 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;
1.3.18. A solução anti-malware deverá permitir a configuração de escaneamento nas seguintes modalidades:
a) Escaneamento manual;
b) Escaneamento em tempo real;
c) Escaneamento escalonado.
1.3.19. 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;
1.3.20. A solução deverá mover para área específica e/ou negar acesso aos arquivos contaminados que não forem possíveis de serem limpos;
1.3.21. A solução deverá acompanhar as requisições de escaneamento de arquivo e retornar o seu resultado;
1.3.22. A solução em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS);
1.3.23. 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:
a) Configurar o Sistema de Armazenamento de Dados (STORAGE) para enviar ao Sistema antivírus somente arquivos com as extensões especificadas;
b) Os arquivos do Sistema de Armazenamento de Dados serão marcados como "limpos" se os mesmos forem escaneados antes e solicitados sem nenhuma alteração;
c) Os arquivos marcados como "limpos" não deverão ser escaneados novamente pelo Sistema antivírus.
1.3.24. A solução deverá possuir rotinas bem definidas de escaneamento, atualizações e de logs;
1.3.25. Deverá garantir a integridade dos dados e ser capaz de detectar e remover *malware* conhecidos e desconhecidos.
1.3.26. A solução deverá utilizar escaneamento recursivo para arquivos compactados;
1.3.27. 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:
a) Deixar em quarentena arquivos infectados;
b) Limpar com backup;
c) Limpar sem backup;
d) Excluir arquivo infectado.
1.3.28. 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;
1.3.29. Armazenamento da ocorrência de malware em log centralizado;

1.3.30. Possibilidade de colocar arquivos e diretórios em listas de exclusões onde estes não serão verificados pela solução;
1.3.31. Possibilidade de funcionamento e administração independentes de ferramenta de gerenciamento centralizado;
1.3.32. Gerenciamento remoto e centralizado da solução;
1.3.33. Realizar ações específicas para cada tipo de código malicioso;
1.3.34. Fornecimento de vacina para novos vírus num prazo máximo de 24 (vinte e quatro) horas, a partir do acionamento ao fornecedor;
1.3.35. Possibilidade de retorno de versão anterior das vacinas;
1.3.36. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
1.3.37. Permitir o reinício automático dos serviços do *malware*;
1.3.38. Proteção no mínimo contra códigos maliciosos classificados como vírus, trojan *horses*, *worms* entre outros;
1.3.39. Suporte compreensível com Help inteligente;
1.3.40. Da remoção:
a) Detecção e remoção de malware em tempo real;
b) Detecção e remoção de malwares, do tipo: Vírus, *worms*, *trojan horses* entre outros;
c) Proteção contra desinstalação e desativação não autorizada do produto.
1.3.41. Das Atualizações:
a) Permitir atualização automática e de forma incremental do cartório de vírus e da base de dados de vacina;
b) Permitir configuração de forma manual para atualizações referentes às mudanças no programa, erros resolvidos e melhorias;
c) Que a periodicidade e o horário das atualizações também possam ser configuráveis.
1.3.42. A solução deverá permitir conexão de atualização em redes que possuam servidor Proxy;
1.3.43. 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*);
1.3.44. 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.

1.4. **Funcionalidade de proteção anti-malware para estações Mac OS**

1.4.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:
a) Mac os x 10.6.8 (snow leopard) e 10.7 (lion) em processadores 32 e 64 bits;
b) Mac os x Server 10.6.8 e 10.7 em processadores 32 e 64 bits;
c) Mac os x 10.8 (mountain lion) em processadores 64 bits;
1.4.2. Suporte ao apple remote desktop para instalação remota da solução;
1.4.3. Gerenciamento integrado à console de gerência central da solução
1.4.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware e outros tipos de códigos maliciosos;
1.4.5. Permitir a verificação das ameaças da maneira manual e agendada;
1.4.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
1.4.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;
1.4.8. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
1.4.9. Deve possuir no mecanismo de autoproteção as seguintes proteções:
1.4.10. Autenticação de comandos ipc;
1.4.11. Proteção e verificação dos arquivos de assinatura;
1.4.12. Proteção dos processos do agente de segurança;
1.4.13. Proteção das chaves de registro do agente de segurança;
1.4.14. Proteção do diretório de instalação do agente de segurança.

1.5. **Funcionalidade de atualização**

1.5.1. 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;
1.5.2. Deve permitir atualização incremental da lista de definições de vírus;
1.5.3. 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;
1.5.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;
1.5.5. 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;
1.5.6. 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;
1.5.7. 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;
1.5.8. 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.

1.6. **Funcionalidade de administração**

1.6.1. 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;
1.6.2. Deve possibilitar instalação "silenciosa";
1.6.3. Deve permitir o bloqueio por nome de arquivo;
1.6.4. Deve permitir o travamento de pastas e diretórios;
1.6.5. Deve permitir o travamento de compartilhamentos;
1.6.6. Deve permitir o rastreamento e bloqueio de infecções;
1.6.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
1.6.8. 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;
1.6.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro *software* ou agente;
1.6.10. Deve permitir a desinstalação através da console de gerenciamento da solução;
1.6.11. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
1.6.12. 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;
1.6.13. Deve ter a possibilidade de determinar a capacidade ou prazo de armazenamento da área de quarentena;
1.6.14. Deve permitir a deleção dos arquivos quarentenados;
1.6.15. Deve permitir remoção automática de clientes inativos por determinado período de tempo;
1.6.16. Deve permitir integração com Active Directory para acesso a console de administração;
1.6.17. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;
1.6.18. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
1.6.19. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
1.6.20. 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;
1.6.21. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;
1.6.22. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

1.6.23. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
1.6.24. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;
1.6.25. 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;
1.6.26. 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;
1.6.27. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web ou console MMC;
1.6.28. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;
1.6.29. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
1.6.30. 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;
1.6.31. Deve permitir a criação de usuários locais de administração da console de anti-malware;
1.6.32. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
1.6.33. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
1.6.34. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;
1.6.35. 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;
1.6.36. Deve permitir a gerência de domínios separados para usuários previamente definidos;
1.6.37. Deve ser capaz de enviar notificações especificas aos respectivos administradores de cada domínio definido na console de administração;
1.6.38. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

1.7. **Funcionalidade de controle de dispositivos**

1.7.1. 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;
1.7.2. 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;
1.7.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;
1.7.4. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
1.7.5. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

1.8. **Funcionalidade de Host IPS e Host Firewall**

1.8.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
a) Windows Server 2003 sp2 (32/64-bit);
b) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
c) Windows Server 2012 (32/64-bit);
d) Windows XP sp2 / sp3 (x86/x64);
e) Windows vista (x86/x64);
f) Windows 7 (x86/x64);
g) Windows 8 e 8.1 (x86/x64);
h) Windows 10 (x86/x61).
1.8.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

1.8.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
1.8.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;
1.8.5. Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída
1.8.6. A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;
1.8.7. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou superior, por meio de regras de host ips;
1.8.8. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;
1.8.9. Deve ser capaz de identificar e bloquear ataques conhecidos através de assinaturas;
1.8.10. A atualização de assinaturas não deve exigir reinício do sistema operacional;
1.8.11. Deve efetuar varredura de segurança 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;
1.8.12. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;
1.8.13. Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, 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;
1.8.14. Deve fornecer proteção contra vulnerabilidades existentes nas estações de trabalho;
1.8.15. Deve proteger contra ataques locais iniciados por CD's ou dispositivos USB;
1.8.16. Deve proteger contra ataques que trafegam por fluxos criptografados;
1.8.17. Deve proteger contra ataque de negação de serviço;
1.8.18. Deve proteger contra tentativas de invasão;
1.8.19. Deve possuir proteção contra BOTs ;
1.8.20. Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;
1.8.21. Deve permitir a criação de políticas de segurança personalizadas;
1.8.22. Deve permitir limitar o número de conexões simultâneas no sistema operacional;
1.8.23. Deve permitir a emissão de alertas via smtp e snmp;
1.8.24. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;
1.8.25. Deve permitir criar regras com base nos seguintes parâmetros:
a) Descrição;
b) Ação;
c) Direção;
d) Protocolo de Rede;
e) Aplicação e Executáveis;
f) Tempo de aplicação da regra.
1.8.26. Deve possuir integração com o Centro de Inteligência do fabricante para verificar a reputação do endereço IP;
1.8.27. A reputação deve informar quatro níveis:
a) Mínimo;
b) Não verificado;
c) Médio;
d) Alto.
1.8.28. Para evitar consumo de banda, a solução deve manter um cache para este tipo de consulta;
1.8.29. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;
1.8.30. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;
1.8.31. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;
1.8.32. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
1.8.33. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados, para facilitar a visualização e gerenciamentos;

1.8.34. 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.

1.9. **Módulo para controle de aplicações**

1.9.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
a) Windows Server 2003 sp2 (32/64-bit);
b) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
c) Windows Server 2012 (32/64-bit);
d) Windows XP sp2 / sp3 (x86/x64);
e) Windows 7 (x86/x64);
f) Windows 8 e 8.1 (x86/x64);
g) Windows 10 (x86/x61).
1.9.2. Deve permitir a criação de políticas de segurança personalizadas;
1.9.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:
a) Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
b) Range de endereços IPS;
c) Sistema operacional;
d) Grupos de máquinas espelhados do Active Directory;
e) Usuários ou grupos do Active Directory.
1.9.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;
1.9.5. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:
a) Nenhum;
b) Somente bloqueios;
c) Somente regras específicas;
d) Todas as aplicações executadas.
1.9.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs;
1.9.7. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;
1.9.8. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;
1.9.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;
1.9.10. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;
1.9.11. As políticas de segurança devem permitir o controle através de regras de aplicação;
1.9.12. As regras de controle de aplicação devem permitir as seguintes ações:
a) Permissão de execução;
b) Bloqueio de execução;
c) Bloqueio de novas instalações.
1.9.13. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
1.9.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:
a) Hash do executável;
b) Atributos do certificado utilizado para assinatura digital do executável;
c) Caminho lógico do executável;
d) Base de assinaturas de certificados digitais válidos e seguros.
1.9.15. As regras de controle de aplicação devem possuir categorias de aplicações;
1.9.16. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.
1.9.17. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
1.9.18. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados, para facilitar na visualização e gerenciamentos;

1.9.19. 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.

1.10. **Funcionalidade contra vazamento de informações – DLP**

1.10.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
a) Windows Server 2003 sp2 (32/64-bit);
b) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
c) Windows Server 2012 (32/64-bit);
d) Windows XP sp2 / sp3 (x86/x64);
e) Windows 7 (x86/x64);
f) Windows 8 e 8.1 (x86/x64);
g) Windows 10 (x86/x64).
1.10.2. Deve possuir nativamente templates para atender as seguintes regulamentações:
a) PCI/DSS;
b) HIPA;
c) Glba;
d) SB-1386;
e) US PII.
1.10.3. Deve ser capaz de detectar informações, em documentos nos formatos:
a) Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;
b) Gráficos: visio, postscript, pdf, tiff,
c) Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;
d) Códigos: c/c++, java, verilog, autocad.
1.10.4. Deve ser capaz de detectar informações, com base em:
a) Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;
b) Palavras ou frases configuráveis;
c) Expressões regulares;
d) Extensão dos arquivos.
1.10.5. Deve ser capaz de detectar em arquivos compactados;
1.10.6. Deve permitir a configuração de quantas camadas de compressão serão verificadas;
1.10.7. Deve permitir a criação de modelos personalizados para identificação de informações;
1.10.8. Deve permitir a criação de modelos com base em regras e operadores lógicos;
1.10.9. Deve possuir modelos padrões;
1.10.10. Deve permitir a importação e exportação de modelos;
1.10.11. Deve permitir a criação de políticas personalizadas
1.10.12. Deve permitir a criação de políticas baseadas em múltiplos modelos;
1.10.13. Deve permitir mais de uma ação para cada política, como:
a) Apenas registrar o evento da violação;
b) Bloquear a transmissão;
c) Gerar alertar para o usuário;
d) Gerar alertar na central de gerenciamento;
e) Capturar informação para uma possível investigação da violação.
1.10.14. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;
1.10.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:
a) Cliente de e-mail;
b) Protocolos http, https, ftp;
c) Mídias removíveis;
d) Discos óticos cd/dvd;
e) Gravação cd/dvd;
f) Aplicações de mensagens instantâneas;
g) Tecla de print screen;
h) Aplicações p2p;
i) Área de transferência do Windows;
j) Webmail;
k) Armazenamento na nuvem (cloud);
l) Impressoras;

m) Scanners;
n) Compartilhamentos de arquivos;
o) Activesync;
p) Criptografia PGP;
q) Portas com, lpt, firewire (ieee 1394);
r) Modems;
s) Infravermelho;
t) Bluetooth;

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

1.11. **Funcionalidade de proteção para smartphones e tablets**

1.11.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:
a) IOS;
b) Android;
c) Windows Phone.

1.11.2. As funcionalidades estarão disponíveis de acordo com cada plataforma

1.11.3. Deve permitir o provisionamento de configurações de:
a) Wi-fi;
b) Exchange Activesync;
c) VPN;
d) Proxy HTTP;
e) Certificados digitais;

1.11.4. Deve possuir proteção de anti-malware;

1.11.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

1.11.6. Deve possuir capacidade de detecção de spam proveniente de SMS;

1.11.7. Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

1.11.8. Deve permitir o bloqueio de aplicativos de acordo com sua categoria;

1.11.9. Controle da política de segurança de senhas, com critérios mínimos de:
a) Padrão de senha;
b) Uso obrigatório de senha;
c) Tamanho mínimo;
d) Tempo de expiração;
e) Bloqueio automático da tela;
f) Bloqueio por tentativas inválidas.

1.11.10. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:
a) Câmera;
b) Wlan/wifi;
c) Aceitar TLS não confiável;
d) Instalação de aplicativos;
e) Sincronia automática enquanto em modo roaming;
f) Dados de diagnostico;
g) Forçar backups criptografados;
h) Itunes;
i) Compra dentro de aplicativos;
j) Captura de tela;
k) Siri;
l) Siri com tela bloqueada;
m) Filtro de profanidade;
n) Jogos multijogador;
o) Discagem por voz;
p) Youtube;
q) Abertura de documentos de aplicativos gerenciados em aplicativos terceiros;
r) Abertura de documentos de aplicativos terceiros em aplicativos gerenciados;

s) Microsoft Activesync.

1.12. **Funcionalidade para Proteção Avançada de Servidores**

1.12.1. Deve oferecer proteção proativa contra ataques tipo Dia-Zero diretamente no equipamento, para no mínimo:
a) Deve impedir a exploração maliciosa de sistemas e aplicações;
b) Deve prevenir a entrada e distribuição de códigos maliciosos.
1.12.2. Deve ser uma solução específica e otimizada para funcionar e interoperar com ambiente virtual;
1.12.3. Deve permitir a implementação, sem necessidade de agente, no ambiente virtual de servidores, no mínimo, as seguintes tecnologias:
a) Antivirus;
b) Firewall;
c) IPS.
1.12.4. Deve suportar vMotion;
1.12.5. Deve ter a capacidade de integração nativa com a tecnologia VMWare NSX ou Vshield Endpoint, atuando de forma automática para isolar um determinado servidor virtual infectado;
1.12.6. Deve ter a capacidade de liberar apenas alguns serviços quando identificado como infectado;
1.12.7. Deve manter em conformidade com as políticas de seguranças através de verificações continua em clientes e servidores;
1.12.8. Deve efetuar "hardening" de sistemas operacionais, aplicações e bancos de dados;
1.12.9. Deve conter políticas de segurança nativas para aplicativos Microsoft;
1.12.10. 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";
1.12.11. Deve impedir a execução de aplicações não autorizadas;
1.12.12. Deve permitir ao Administrador bloquear trafego por porta, por protocolo, por IP ou por faixa de endereços IP;
1.12.13. Proteger arquivos e registros do sistema baseado em políticas;
1.12.14. Monitorar arquivos e registros do sistema baseado em políticas;
1.12.15. Deve possuir Sistema de Prevenção de Intrusos;
1.12.16. Deve possuir Sistema de Detecção de Intrusos;
1.12.17. Deve permitir ao administrador configurar filtros de eventos para encaminhamento ao servidor de gerenciamento;
1.12.18. Deve possuir sistema de atualização automática de políticas e pacotes de relatórios a partir do site do fabricante;
1.12.19. Deve ter a capacidade de importar e exportar políticas customizadas ou de terceiros;
1.12.20. 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;
1.12.21. Deve possuir sistema de criação de usuários com perfis diferenciados de acesso aos recursos da console de gerenciamento;
1.12.22. Deve permitir o envio de alertas através de E-mail e SNMP baseados em filtros de eventos recebidos pela console de gerenciamento;
1.12.23. Deve possuir políticas predefinidas de monitoramento, de no mínimo os seguintes recursos:
a) Falha de acesso;
b) Logon com sucesso;
c) Detecção de logoff remoto;
d) Alteração de configuração pelo Usuário;
e) Alteração no grupo de gerenciamento.
1.12.24. Deve monitorar arquivos e eventos em servidores mesmo sem o agente instalado;
1.12.25. Deve possuir recurso de prevenção contra acesso indevido de usuários e de aplicações a outros recursos do sistema, como arquivos, processos, bibliotecas e registros;
1.12.26. 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;
1.12.27. Deve ter a capacidade de prevenção contra ataques de exploração, com regras pré-definidas baseadas no comportamento padrão das aplicações do servidor;
1.12.28. Deve ter a capacidade de prevenção de intrusão baseado no comportamento das aplicações;

1.12.29. Deve possuir recurso nativo de firewall, restringindo atividades de rede por IP e Porta nos sentidos de entrada e saída;
1.12.30. Deve ter a capacidade de prevenção contra alteração maliciosa de privilégios do servidor;
1.12.31. Deve ter a capacidade de prevenir contra alterações maliciosa em arquivos e registros do servidor;
1.12.32. Deve ter a capacidade de proteção contra execução de instalações e operações maliciosas no servidor;
1.12.33. Deve ter a capacidade de monitorar mídias removíveis proteger contra *malwares*;
1.12.34. Deve ter a opção de monitoramento granular de arquivos e diretórios dos servidores e estações;
1.12.35. Deve ter a capacidade de prevenir a adição de códigos em processos em memória para servidores Windows (memory injection protection);
1.12.36. 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";
1.12.37. Deve ter a capacidade de monitor alterações em arquivos críticos do sistema operacional e diretórios das aplicações críticas.
1.12.38. A solução deve ter a capacidade de no mínimo:
a) Bloquear o uso de aplicações indevidas;
b) Proteger o "core" do sistema operacional.
1.12.39. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
1.12.40. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:
a) Origem confiável;
b) Origem não confiável;
c) Comportamento do arquivo.
1.12.41. Capacidade de implementar regras distintas por grupo;
1.12.42. Capacidade de identificar e proteger ataques direcionados, impossibilitando o início do ataque e não somente impedindo as ações após invasão do equipamento;
1.12.43. A solução deve implementar em um único agente as funcionalidades de HIPS, HIDS e Host Firewall;
1.12.44. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários da console de gerenciamento em ambientes físicos e virtuais:
a) Windows XP Professional;
b) Windows 7;
c) Windows Server 2003 Standard/ Enterprise 32-bit;
d) Windows Server 2003 Standard/ Enterprise 64-bit;
e) Windows Server 2008 e 2008 R2;
f) Windows Server 2012;
1.12.45. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do servidor de gerenciamento em ambientes físicos e virtuais:
a) Windows Server 2003 Standard/ Enterprise 32-bit;
b) Windows Server 2003 Standard/ Enterprise 64-bit;
c) Windows Server 2008 e 2008 R2;
d) Windows Server 2012;
1.12.46. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do agente:
a) Suse Linux Enterprise 9, 10 e 11;
b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0;
c) Centos 4.0, 5.0 e 6.0.
d) Windows Server 2003 sp2 (32/64-bit);
e) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
f) Windows Server 2012 (32/64-bit).
1.12.47. A solução deve ser suportada, no mínimo, na versão VMware ESX v5.5;
1.12.48. Os agentes devem ser suportados quando instalados nos seguintes sistemas operacionais tipo Guest em sistemas Virtualizados VMWare:
a) Suse Linux Enterprise 9, 10 e 11;
b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0;
c) Centos 4.0, 5.0 e 6.0.
d) Windows Server 2003 sp2 (32/64-bit);
e) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);

f) Windows Server 2012 (32/64-bit).

1.12.49. O *software* deve suportar os componentes IDS e IPS, para no mínimo os seguintes sistemas operacionais:

a) Suse Linux Enterprise 9, 10 e 11;
b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0;
c) Centos 4.0, 5.0 e 6.0.
d) Windows Server 2003 sp2 (32/64-bit);
e) Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
f) Windows Server 2012 (32/64-bit).

2. SOLUÇÃO PARA PROTEÇÃO DE E-MAIL

2.1. A solução deve ser oferecida em alta disponibilidade, sendo que pelo menos dos nós do cluster deve ser *appliance* físico, suficientemente dimensionada para suportar a, no mínimo, 650 (seiscentos e cinquenta) caixas postais, não considerando grupos ou listas de distribuição como caixas postais e ao processamento de 200.000 (duzentos mil) mensagens por hora;

2.2. **Funcionalidade para proteção para servidor de e-mail**

2.2.1. Compatíveis com as plataformas Windows 2003, Windows 2008 e Windows 2012;
2.2.2. Deve suportar cluster ativo/passivo da solução Exchange;
2.2.3. Deve ser compatível com VSAPI versões 2.0, 2.5 ou 2.6;
2.2.4. Suporte a Exchange 2013 ou superior;
2.2.5. Rastreamento em tempo real, para arquivos anexados a mensagens do Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:
2.2.6. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);
2.2.7. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);
2.2.8. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s);
2.2.9. Rastreamento manual às pastas do Exchange, com opção de limpeza;
2.2.10. Programação de rastreamentos automáticos do Exchange com as seguintes opções:
a) Escopo: Todas as pastas locais, ou pastas específicas;
b) Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
c) Freqüência: Horária, diária, semanal, mensal.
2.2.11. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;
2.2.12. Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional);
2.2.13. Identificação de remetente e destinatário das mensagens;
2.2.14. Permitir bloqueios baseados nos seguintes critérios:
a) Tipo de arquivo;
b) Nome do arquivo;
c) Tamanho do arquivo.
2.2.15. Permitir a instalação em ambientes em Cluster Microsoft;
2.2.16. Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, entre outros;
2.2.17. Permitir a instalação remota a múltiplos servidores Exchange, monitorando o status de cada instalação;
2.2.18. Permitir a verificação em tempo real, manual ou agendada de grupos e bases de dados no Exchange;
2.2.19. A verificação no Information Store deve ser realizada nas Public e Private Stores;
2.2.20. Bloqueio dos arquivos em anexos deve ser com base em política por usuário e integrado com o active directory para a criação dessas políticas;
2.2.21. Prover proteção para mensagens enviadas via Outlook Web Access (OWA);
2.2.22. Permitir o gerenciamento de vários servidores Exchange simultaneamente;
2.2.23. Gerenciamento via console web ou console MMC;
2.2.24. Produto deve ter capacidade de fazer reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;
2.2.25. Produto deve executar rastreamento agendado ou manual nas caixas de e-mail dos usuários;
2.2.26. Deve ser compatível com IPV6;
2.2.27. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;
2.2.28. Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;

2.2.29. Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;
2.2.30. Os usuários devem ter a capacidade de se permitido criarem suas exceções de recebimento através de *white list* gerenciada no próprio Outlook.

2.3. **Funcionalidade para proteção para proteção de gateway**

2.3.1. Deve ser compatível com ambientes virtuais VMware;
2.3.2. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para especifica mensagem, sem necessidade de integração com produtos de terceiros ou "open source";
2.3.3. Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior, em todos os appliances /equipamentos da solução ofertada;
2.3.4. Deve permitir realizar o rastreamento da mensagem, conforme citado anteriormente, utilizando caracteres double-byte para líguas estrangeiras;
2.3.5. Deve possuir funcionalidade de criação de Alias e Mascaramento de endereço;
2.3.6. Deve ser possível realizar notificação do administrador por e-mail caso os filtros antispam não recebam atualizações por um determinado período de tempo;
2.3.7. Deve ser capaz de integração com LDAP Microsoft Active Directory 2003, Microsoft Active Directory 2008 e Lotus Domino 6.5 ou superior para sincronização e autenticação;
2.3.8. Deve permitir a criação de políticas diferenciadas para tratamento de SPAM, Vírus, Filtragem de Conteúdo e Controle de reputação (traffic shaping), de acordo com o destinatário da mensagem e reputação de origem;
2.3.9. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento do usuários válidos e ações de Vírus, Spam e Filtragem de Conteúdo diferenciadas por grupo do LDAP;
2.3.10. Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico, sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;
2.3.11. Deve possuir mecanismos de backup/restore da configuração existente na solução;
2.3.12. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;
2.3.13. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:
a) Apagar mensagem;
b) Enviar para Quarentena;
c) Encaminhar mensagem;
d) Encaminhar em BCC;
e) Gravar mensagem em disco;
f) Gravar em pasta de conformidade;
g) Modificar o assunto;
h) Adicionar informações ao cabeçalho;
i) Deferir a mensagem;
j) Rejeitar a mensagem.
2.3.14. Deve ter a capacidade de verificação em tempo real de SMTP;
2.3.15. Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;
2.3.16. Deve ter a capacidade de verificação manual dos message stores;
2.3.17. Deve ter a capacidade de verificação agendada dos message stores;
2.3.18. Deve permitir verificar mailbox stores e public foldes;
2.3.19. Deve permitir definir a "idade mínima" das mensagens a serem verificadas;
2.3.20. Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:
a) Tempo máximo de verificação;
b) Número máximo de decomposição de arquivos compactados recursivamente;
c) Tamanho máximo do arquivo descompactado.
2.3.21. Número máximo de arquivos descompactados;
2.3.22. Deve ser capaz de permitir definir ações distintas para as mensagens categorizadas como phishing, spam ou bloqueadas por regra de conformidade;

2.3.23. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;
2.3.24. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);
2.3.25. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);
2.3.26. Deve possuir centro especializado, 24x7, com monitoramento de mais de 2 milhões de mailboxes, para processamento de SPAMs recebidos e criação automática de novos filtros/assinaturas;
2.3.27. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;
2.3.28. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;
2.3.29. Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);
2.3.30. Deve ter a capacidade de reconhecimento de ameaças Dia-Zero, com assinatura de suspeitos de vírus;
2.3.31. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:
a) Assinaturas para corpo da mensagem e anexos;
b) Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;
c) Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramente do fornecedor da solução);
d) Identificação de idiomas;
e) Filtros de URLs;
f) Filtros anti-phishing.
2.3.32. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;
2.3.33. Deve permitir a criação de regras de conformidade para o bloqueio de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo Administrador;
2.3.34. Deve possuir tecnologia para detecção de spam, de malwares, de phishing, de spear phising e de coleta de diretório (usuários inválidos);
2.3.35. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;
2.3.36. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o controle do percentual de mensagens que serão recusadas;
2.3.37. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;
2.3.38. Deve possuir tecnologia para prevenção de ataques de "Bounce Messages";
2.3.39. Deve possuir a capacidade de implementar Sender Policy Framework (SPF);
2.3.40. Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;
2.3.41. Deve possuir a capacidade para criação de regras baseada na detecção por "Wildcard";
2.3.42. Deve possuir a capacidade para criação de regras baseada na detecção por expressões regulares;
2.3.43. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);
2.3.44. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;
2.3.45. Deve ter capacidade de detecção e bloqueio de mensagens indesejadas em multiplos idiomas, incluindo português;
2.3.46. Deve ter capacidade de detecção e bloqueio de mensagens indesejadas por país de origem;
2.3.47. Deve possuir capacidade de criar uma lista de IP's confiáveis baseado no comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;
2.3.48. Deve possuir a capacidade de atualização automática periódica da lista de IP's confiáveis, citada no item anterior;
2.3.49. Deve ter a capacidade de deleção total de mensagens enviadas por "Mass-Mailing Worms", com opção de ações diferenciadas por tráfego de entrada e saída;
2.3.50. Deve ter a capacidade de reconhecimento de Spywares;
2.3.51. Deve possuir recurso para detecção dos ataques de duas escalas para Vírus e Diretório (LDAP), capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;
2.3.52. Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;

2.3.53. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo;
2.3.54. Deve ter a capacidade de implementar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;
2.3.55. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena (digest);
2.3.56. Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;
2.3.57. Deve permitir que o usuário cadastre endereços de e-mail em listas negras/listas brancas pessoais;
2.3.58. Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);
2.3.59. Deverá fazer listas de exceções para domínios utilizando-se de DKIM;
2.3.60. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;
2.3.61. Permitir a criação de white e black lists para detecção de SPAMs;
2.3.62. Possuir proteção contra phishings e spear phishing;
2.3.63. Possuir proteção inteligente contra ataques de engenharia social;
2.3.64. Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;
2.3.65. Possuir inteligência contra ataques de exploração de códigos avançados (exploits) e de dia-zero (zero-day);
2.3.66. Possui reputação de links que estejam dentro do corpo das mensagens;
2.3.67. Possui níveis de sensibilidade no bloqueio de mensagens com links de má reputação;
2.3.68. Possui white list para a checagem de reputação em URL's dentro de mensagens;
2.3.69. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;
2.3.70. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;
2.3.71. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;
2.3.72. Implementar proteção contra spywares, contra dialers, contra ferramentas hackers e contra ferramentas para descoberta de senhas de aplicativos;
2.3.73. Bloqueio de malware empacotado (packed malware) de forma heurística;
2.3.74. A solução de anti-spam deverá submeter e-mails suspeitos a solução de analise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise das informações:
a) Processos de autostart;
b) Modificações de arquivos de sistema;
c) Serviços criados e modificados;
d) Atividade de rede suspeita;
e) Modificações de registros.
2.3.75. O fabricante ofertado deve possuir conhecimento em mais de 190 milhões de ameaças conhecidas;
2.3.76. Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;
2.3.77. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;
2.3.78. Permitir criar filtros definidos pelo tamanho de mensagem;
2.3.79. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;
2.3.80. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;
2.3.81. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;
2.3.82. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;
2.3.83. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;
2.3.84. Permitir criar regras distintas para mensagens que entram e saem do ambiente;
2.3.85. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;
2.3.86. Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;
2.3.87. Permitir limitar o número de destinatários por mensagem;
2.3.88. Possui regra específica para anexos protegidos por senha

2.3.89. Possuir módulo de Data Loss Prevention (DLP), prevenido ações de vazamento de informações, com regras baseadas em:
a) Palavras chaves;
b) Expressões regulares;
c) Extensões de arquivos.
2.3.90. Permitir a checagem em Centro de Inteligência (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;
2.3.91. Permitir a configuração de reputação personalizada local;
2.3.92. Possibilidade de exceções ao bloqueio por reputação com base em *range* de IP ou IP;
2.3.93. Configurar nível de sensibilidade da reputação de IPs em, no mínimo, 3 (três) níveis;
2.3.94. Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:
2.3.95. O Centro de Inteligência deve ser do mesmo fabricante do *software* ofertado para a funcionalidade de proteção de gateway;
2.3.96. Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails);
2.3.97. Permitir personalizar os filtros baseado em:
a) Tempo;
b) Total de mensagens;
c) Porcentagem de mensagens;
d) Ação a ser tomada.
2.3.98. Prevenir contra-ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;
2.3.99. Prevenir contra-ataques de vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;
2.3.100. Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas;
2.3.101. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;
2.3.102. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;
2.3.103. Permitir inserção de carimbo no assunto da mensagem;
2.3.104. Permitir a inserção de um header customizado (X-header);
2.3.105. Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;
2.3.106. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;
2.3.107. Permitir a inserção de texto no corpo da mensagem;
2.3.108. Permitir customizar a mensagem que será inserida no corpo das mensagens;
2.3.109. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;
2.3.110. Permitir inserir variáveis nas notificações, onde informem:
a) Remetente;
b) Destinatário;
c) Assunto;
d) Data;
e) Nome do arquivo detectado;
f) Nome do vírus detectado;
g) Protocolo de escaneamento;
h) Tamanho total da mensagem e seus anexos;
i) Tamanho total do anexo;
j) Número de anexos detectados pela regra;
k) Ação tomada pela ferramenta;
l) Nome da quarentena para onde a mensagem foi enviada.
2.3.111. Permitir configurar ações para mensagens fora do padrão (mensagens malformadas);
2.3.112. Permitir ação personalizada para mensagens com anexos protegidos por senha;
2.3.113. Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;
2.3.114. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

2.3.115. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;
2.3.116. Permitir exclusão automática das mensagens em quarentena;
2.3.117. Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo:
a) Microsoft Active Directory;
b) OpenLDAP.
2.3.118. Gerenciamento via console web HTTPS ou console MMC;
2.3.119. A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento;
2.3.120. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;
2.3.121. Realizar atualização de vacinas de forma incremental;
2.3.122. Possibilidade de configurar o "greeting" SMTP;
2.3.123. Permitir o controle de relay baseado no domínio e/ou endereço IP;
2.3.124. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;
2.3.125. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio;
2.3.126. Definição de timeout de conexão SMTP;
2.3.127. Suporte a ilimitadas conexões SMTP;
2.3.128. Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único;
2.3.129. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;
2.3.130. A solução deve ofertar possibilidade de ter domínio mascarado;
2.3.131. Possuir autenticação via TLS (Transport Layer Security);
2.3.132. A solução deve apresentar relatórios criados através de console web;
2.3.133. A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;
2.3.134. A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;
2.3.135. A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;
2.3.136. A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;
2.3.137. A solução deve permitir reindexação da base de dados de forma agendada;
2.3.138. É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;
2.3.139. A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;
2.3.140. A solução deve integrar o login da console de gerenciamento com o serviço de LDAP pré-configurado;
2.3.141. A solução deve ser gerenciada totalmente por sua console Web, além de possui interface CLI intuitiva com gerenciamento dedica a solução;
2.3.142. Deve operar em alta disponibilidade;
2.3.143. Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;
2.3.144. Permitir configurar as portas de comunicação para o gerenciamento;
2.3.145. Realizar a verificação em background, para não impactar na performance;
2.3.146. Possuir verificação em memória e *multi-threaded*;
2.3.147. Possuir ação de limpeza para os arquivos anexados;
2.3.148. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;
2.3.149. Permitir a filtragem baseado no tamanho da mensagem;
2.3.150. Realizar a verificação contra códigos maliciosos no corpo da mensagem;
2.3.151. Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;
2.3.152. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;
2.3.153. Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;
2.3.154. Deve ter lista de aprovados para o recebimento de mensagens de determinados remetentes;
2.3.155. Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;

2.3.156. Os usuários devem ter a capacidade de se permitido criarem suas exceções de recebimento através de white list gerenciada no próprio Outlook;
2.3.157. Avaliar reputação e emular links HTTP que estejam dentro do e-mail quanto a sua reputação e caso reputação negativa deve ser tomada uma ação na mensagem;
2.3.158. Permitir criar regras de controle de conteúdo definidos por rotas, usuários e grupos;
2.3.159. Regra de controle de conteúdo deve procurar por conteúdo no subject, corpo e cabeçalho da mensagem;
2.3.160. Deve ter a possibilidade de em caso de um conteúdo malicioso, executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem ou passar parte da mensagem;
2.3.161. Possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os e-mails detectados como SPAM, para que o usuário possa refinar a ferramenta;
2.3.162. Deve possuir área de quarentena no servidor com gerencia pelo administrador através da liberação de mensagens ou deleção;
2.3.163. Deve possuir exceções nas políticas de bloqueio de anexo e de bloqueio de conteúdo;
2.3.164. No caso de violação de anexo não desejado deve possuir capacidade de executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira ou fazer o backup/cópia da mensagem;
2.3.165. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;
2.3.166. Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;
2.3.167. Gerenciamento via console web ou console MMC;
2.3.168. Possuir controle de time-out para a console de gerenciamento;
2.3.169. Permitir configurar as notificações a serem enviadas para o administrador, via e-mail e SNMP;
2.3.170. Realizar ações específicas para cada tipo de código malicioso;
2.3.171. Capacidade para, em caso de epidemia, bloquear a entrada de determinados e-mails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;
2.3.172. Proteção contra spywares, sem a necessidade de um *software* ou agente adicional;
2.3.173. Deve detectar e bloquear malwares empacotados (packed malwares);
2.3.174. Para mensagens infectadas, deve poder tomar as seguintes ações: limpar, substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar ou quarentenar parte da mensagem;
2.3.175. Deve possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;
2.3.176. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;
2.3.177. Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;
2.3.178. Deve gerar relatórios de:

a) Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;
b) Principais vírus/malwares, spywares e graywares;
c) Principais remetentes de vírus/malwares, spywares e graywares;
d) Resumo das ações tomadas contra vírus/malwares, spywares e graywares;
e) Resumo do bloqueio de anexos;
f) Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;
g) Principais tipos de anexos bloqueados;
h) Principais nomes de anexos bloqueados;
i) Principais extenções de anexos bloqueados;
j) Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;
k) Principais remetentes e destinatários filtrados.
l) Resumo de spam
m) Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;
n) Principais fontes e destinatários de spam;
o) Tráfego por hora, dia e mês.

3. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

3.1. A solução para proteção contra ameaças avançadas deverá funcionar completamente integrada com o Item 1 – Solução para proteção de *endpoint* e com o Item 2 – Solução para proteção de e-mail, sendo capaz de receber arquivos, e-mails, URL's, dentro outros, para análise avançada;
3.2. A solução deverá ser capaz de gerar índices de comprometimento bem como bloquear ameaças persistentes direcionadas aos endpoints e ao serviço de e-mail do CONTRATANTE;
3.3. A solução para proteção contra ameaças avançadas deverá ser capaz de:
3.3.1. Detectar ataques direcionados persistentes – APT;
3.3.2. Realizar a análise virtual de ameaças;
3.3.3. Correlacionar regras para detecção de conteúdo malicioso;
3.3.4. Analisar todos os estágios de uma sequência de ataques;
3.3.5. Proteger contra ataques em rede;
3.3.6. Monitoração e gerir riscos que permitam a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente.
3.4. Detecção, visibilidade, bloqueio e informação sobre incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;
3.5. Deverá ser capaz de identificar *softwares* ou comportamentos maliciosos, tais como:
3.5.1. Malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede;
3.5.2. Vermes de rede e de e-mail no tráfego de rede;
3.5.3. Programas de exploração de vulnerabilidades (Exploits) na rede;
3.5.4. Ataques de engenharia social que procurem fazer com que o usuário forneça suas credenciais de acesso (phishing, spear phishing);
3.5.5. Empacotamentos maliciosos no tráfego da rede;
3.5.6. Tráfego web malicioso através de consultas a sistemas de reputação na Internet;
3.5.7. Tentativas de roubo de informação;
3.5.8. Outras incidentes de segurança que representem risco a integridade, disponibilidade ou autenticidade de informação do CONTRATANTE.
3.6. Características de Desempenho e Escalabilidade:
3.6.1. Suportar uma análise de tráfego agregado de, no mínimo, 1 Gbps (um gigabit por segundo);
3.6.2. Suportar, no mínimo, 100.000 (cem mil) conexões simultâneas e ser capaz de processar, no mínimo, 200.000 (duzentos mil) mensagens por hora;
3.6.3. A solução deverá prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de call-backs;
3.6.4. A solução deverá ser executada em *Hardware* e *Software* específicos (appliance) com sistema operacional especializado. Todas as funcionalidades deverão ser executadas no mesmo equipamento, com exceção das funcionalidades de relatórios, as quais poderão ser executadas em appliance ou servidor dedicado para este fim;
3.6.5. Possuir no mínimo 02 (dois) discos rígidos 160 GB (cento e sessenta gigabytes);
3.6.6. Possuir configuração mínima de RAID entre os discos;
3.6.7. Possuir no mínimo 04 (quatro) interfaces 10/100/1000BaseTX, não sendo computadas interfaces de gerencia e sincronismo;
3.6.8. Possuir fontes redundantes e hot swappable;
3.6.9. Possuir no máximo 2U padrão 19" Rack
3.6.10. Possuir interface de console do tipo RS-232, ou similar;
3.6.11. Operar em alta disponibilidade.
3.7. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas;
3.8. Permitir a rápida identificação da criticidade dos eventos de segurança;
3.9. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;
3.10. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;
3.11. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;
3.12. Permitir a integração com sistemas de serviço de diretório;

3.13. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;
3.14. A análise de SMTP será realizada em uma solução separada do sensor de HTTP e demais protocolos;
3.15. A análise em SMTP será realizando de modo MTA (Inline);
3.16. A análise de e-mail em sandbox deverá ocorrer em arquivos Microsoft Office, PDF, arquivos compactados e executáveis do tipo PE;
3.17. A análise em sandbox será realizada na própria solução, não sendo necessário integrações com demais soluções ofertadas;
3.18. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;
3.19. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;
3.20. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;
3.21. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;
3.22. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;
3.23. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;
3.24. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;
3.25. Capacidade de oferecer informações para analise forense de artefatos suspeitos de serem maliciosos;
3.26. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;
3.27. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;
3.28. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF's, executáveis, PPT, DOC, XLS, ZIP e RAR;
3.29. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;
3.30. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;
3.31. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;
3.32. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;
3.33. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos(compactados);
3.34. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.
3.35. Deve possuir foco em proteção contra APT's (Advanced Persistent Threats);
3.36. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;
3.37. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;
3.38. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

3.39. Deverá permitir a análise especifica de eventos de segurança de computadores suspeitos de atividade maliciosa;
3.40. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;
3.41. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;
3.42. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;
3.43. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;
3.44. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;
3.45. Deve possuir interface web para busca e investigação local de incidentes;
3.46. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows XP e Windows 7;
3.47. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;
3.48. Deve possuir capacidade de analise virtual de artefatos internamente;
3.49. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;
3.50. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;
3.51. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;
3.52. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:
3.52.1. Resumidos;
3.52.2. Visão Geral dos Incidentes de Segurança
3.52.3. Discriminação dos Tipos de Incidentes
3.52.4. Top Ameaças Analisadas
3.52.5. Top Hosts Infectados
3.52.6. Recomendações de Segurança
3.52.7. Executivos;
3.52.8. Deve possuir detalhes técnicos dos incidentes detectados.
3.53. Deve possuir estatística do tráfego analisado;
3.54. Deve possuir indicadores de risco do ambiente;
3.55. Recomendações de Segurança
3.56. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;
3.57. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;
3.58. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;
3.59. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;
3.60. Deve possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de analise virtual;
3.61. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;
3.62. Deve ser capaz de detectar e bloquear tentativas de scan de rede;
3.63. Deve ser capaz de detectar e bloquear propagação de malwares na rede;
3.64. Deve ser capaz de detectar e bloquear tentativas de brute-force;
3.65. Deve ser capaz de detectar e bloquear tentativas de fuga e roubo de informação;
3.66. Deve ser capaz de detectar e bloquear ameaças que se replicam na rede;
3.67. Deve ser capaz de detectar e bloquear exploits na rede;

3.68. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;
3.69. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;
3.70. Capacidade de salvar uma investigação antes de ser finalizada;
3.71. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;
3.72. Capacidade de emitir relatórios baseados nas investigações;
3.73. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;
3.74. Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;
3.75. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;
3.76. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);
3.77. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;
3.78. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;
3.79. Deve permitir encaminhamento de logs via syslog;
3.80. Deve permitir receber logs de diferentes dispositivos;
3.81. Deve correlacionar os eventos de todos os componentes da solução;
3.82. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;
3.83. Deve permitir a configuração de alarmes personalizados, com base em investigações;
3.84. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;
3.85. A solução deverá prover as funcionalidades de gerenciamento centralizado para os módulos de analise dos ambientes de endpoint, rede e e-mail;
3.86. A solução deve ter como característica básica correlacionar as informações detectadas pelo módulo de APT de endpoint, módulo de APT de rede e módulo de APT de e-mail. Não serão aceitas correlações advindas somente das tecnologias de IPS/IDS;
3.87. O módulo de análise de e-mail deve ter a capacidade de identificar uma ameaça, mesmo que esta seja originada a partir de uma URL curta, fazendo uma inspeção no conteúdo original, mesmo antes do usuário ter acesso ao conteúdo indicado pela URL, possibilitando categorizar a origem da informação;
3.88. A tecnologia de Sand-box deve permitir a execução em ambiente tanto virtual quanto em bare-metal, utilizando como fonte de informação a rede mundial de inteligência do fabricante;
3.89. Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX);
3.90. Deve suportar análise de documentos em PDF;
3.91. Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR);
3.92. Deve analisar dinamicamente binários PE de 32-bits;
3.93. Deve analisar dinamicamente binários PE de 64-bits;
3.94. Deve analisar dinamicamente bibliotecas dinâmicas (DLL);
3.95. Deve analisar dinamicamente binários BHO;
3.96. Deve poder funcionar em ambiente totalmente virtualizado;
3.97. Deve possuir tecnologia própria de análise de artefatos em sandboxing;
3.98. Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência;
3.99. Deve prover possibilidade de uso da rede dedicada para a internet na análise de sandbox;
3.100. Deve analisar dinamicamente arquivos do Adobe Flash (SWF);
3.101. Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra;
3.102. Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo, ao nível de API, exibindo as funções com argumentos e retornos de execução;
3.103. Deve analisar dinamicamente rootkits;
3.104. Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado;
3.105. Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;
3.106. Capacidade de integração via API com soluções terceiras;
3.107. O Fabricante deverá disponibilizar acesso a base de dados externa que possibilite a correlação entre informações geradas no ambiente com informações de outros clientes que foram afetados pelo mesmo padrão ou tipo de ameaça. Este acesso deverá ser web, e deverá possuir referências e atalhos nos próprios relatórios e logs locais da solução;
3.108. Características do Gerenciamento da Solução:

3.108.1. A console de gerenciamento deve informar origens georeferenciadas de ataques e eventos de segurança monitorados pela solução;
3.108.2. Implementar gerenciamento centralizado com no mínimo as seguintes funções: criação de regras de tratamento de malware, administração de usuários, configurações de host e network;
3.108.3. Implementar a funcionalidade de event server, com mecanismo de rotação automático dos arquivos de evento;
3.108.4. Implementar mecanismo de triangulação e correlação dos vetores de ataque;
3.108.5. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;
3.108.6. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;
3.108.7. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;
3.108.8. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;
3.108.9. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;
3.108.10. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
3.108.11. A console de gerenciamento deverá ser gerenciada por Internet Explorer e Firefox;
3.108.12. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;
3.108.13. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
3.108.14. Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a analise de artefatos por meio de analisador virtual com a capacidade de gerar no mínimo 24 máquinas virtuais de análise;
3.108.15. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.
3.108.16. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:
a) Uso de CPU
b) Uso de Disco;
c) Uso de Memória;
d) Tráfego malicioso analisado;
e) Todo o tráfego analisado.
3.109. Características da Administração da Solução:
3.109.1. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS:
3.109.2. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 ou similar;
3.109.3. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP;
3.109.4. Implementar sincronização de hora através de protocolo NTP;
3.109.5. Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);
3.109.6. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao *hardware*, log do mecanismo de health-check e log da base de dados;
3.109.7. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução;
3.109.8. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização de no mínimo as seguintes informações: Sumário de detecção e proteção, gráfico de top infecções, e gráfico da quantidade de e-mails monitorados;
3.109.9. Implementar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar o modo de operação;
3.109.10. Implementar a atualização (updates) dos appliances via mecanismo de push dos seguintes módulos: segurança de conteúdo e atualização de patch;
3.109.11. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

a) Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;
b) Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.
3.109.12. A solução deverá ter integração com ferramentas de SIEM;
3.109.13. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;
3.109.14. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;
3.109.15. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

a) Computadores infectados;
b) Origem de infecções;
c) Estatísticas de ameaças;
d) Riscos potenciais de segurança;
e) Riscos de perda de informações;
f) Risco de sistema comprometido;
g) Risco de disseminação de ameaças;
h) Eventos suspeitos;
i) Infecções de malware.

3.109.16. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

a) Critérios de pesquisa por dia, mês e ano;
b) Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;
c) Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;
d) Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

3.110. Console de Gerenciamento
3.110.1. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;
3.110.2. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP;
3.110.3. Implementar sincronização de hora através de protocolo NTP;
3.110.4. Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);
3.110.5. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao *hardware*, log do mecanismo de health-check e log da base de dados;
3.110.6. Implementar através da interface gráfica mecanismo para configuração de notificações dos alertas;
3.110.7. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução;
3.110.8. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização das seguintes informações ou similares: Sumário de detecção e proteção, gráfico de top infecções, e gráfico do troughput de tráfego monitorado.

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO II DO TERMO DE REFERÊNCIA DO CONTRATO N. 005/2016

AMBIENTE TECNOLÓGICO DO CJF

1. PRINCÍPIOS

1.1. A plataforma de *hardware* e *software* do ambiente implantado no CJF e a metodologia para administração adotada visam atender, prioritariamente, os seguintes princípios:

1.1.1. **Escalabilidade,** possibilitando o crescimento modular,

1.1.2. **Capacidade,** viabilizando o gerenciamento de grandes volumes de dados e tabelas;

1.1.3. **Conectividade,** permitindo o acesso aos dados por usuários internos e externos ao CJF, a partir de protocolos de rede múltiplos;

1.1.4. **Desempenho,** garantindo o acesso simultâneo de número expressivo de usuários do CJF e de instalações externas, governamentais ou não;

1.1.5. **Disponibilidade,** dotando o ambiente corporativo de um nível aceitável de tolerância a falhas;

1.1.6. **Continuidade,** normatizando e divulgando às áreas responsáveis os procedimentos e processos de execução dos serviços, mediante documentação organizada e padronizada;

1.1.7. **Controle,** efetuando registros de todos os problemas, alterações e implementações realizadas no ambiente computacional;

1.1.8. **Segurança,** prevendo mecanismos de controle de acesso às informações e ferramentas que garantam a integridade e confiabilidade dos dados;

1.1.9. **Governança,** adequando todos os procedimentos, processos, documentações e execução de serviços em plena compatibilidade com as melhores práticas utilizadas pelo mercado ou com modelos adotados pelo CJF.

1.2. A(s) empresa(s) contratada(s) deverá(ão) prestar os serviços considerando o ambiente atual e previsto para o CJF, composto das seguintes tecnologias, entre outras:

2. PLATAFORMA DE SEGURANÇA

Tipo do Ativo	Marca/Modelo do Ativo	Descrição	Quantidade
Unidade de Gerenciamento Múltiplo de Ameaças	*Fortigate* 3040B	Solução em *Appliance* de controle multiameaça de tecnologia UTM em cluster, com capacidade de 40Gbps de *throughput*	2
Unidade centralizadora de logs e relatórios	*FortiAnalyzer*-2000B	Solução em Appliance de Análise e Auditoria de dados trafegados para equipamentos *Fortinet.*	1
Firewall de Aplicação Web	Fortiweb-3000D	Solução de firewall de aplicação, aceleração e balanceamento de tráfego em cluster.	2
Software de Gerenciamento e Análise de Vulnerabilidades	*Symantec Control Compliance Suite Vulnerability Manager*	*Software* integrado de gerenciamento e análise de vulnerabilidades	1

3. PLATAFORMA DE *HARDWARE*

Encontra-se descrito no quadro abaixo, a infraestrutura de *hardware* em uso no CJF:

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
Videoconferência	Radvision / Scopia 24	Unidade de Controle Multiponto (MCU)	2
	HP / DL160	Servidor 4GB HD, 4 GB de memória, 2 Processadores Xeon Quad Core	4
	Sony / PCS-G50	Equipamento de videoconferência (Codec)	25

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
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
Scanner	Fujitsu e HP		14
Estações de trabalho	Dell Optiplex 7010	Desktop	400
	HP Elitebook 810	Notebook	17
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	29
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	30

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 e 2008 R2 Server	Sistema Operacional de 32 bits e 64 bits
	MS / Windows 7 Pro (Port)	Sistema Operacional de 64 bits
	Suse Linux 9, 10 e 11	Sistema Operacional de 32 bits
	IBM AIX 6.1	Sistema Operacional de 32 bits
Servidores Aplicações	IIS 6.0 (Internet Information Services)	Servidor de Aplicações Microsoft ASP / HTML
	Apache 2.2.12	Servidor de Aplicações Apache / PHP
	Tomcat 5, 6 e 7	Servidor de Aplicações Java
	OAS 10g v10.1.35	Servidor de Aplicações Oracle
	Plone / Zope	Servidor de Aplicações Zope
	JBoss 5.1.0	Servidor de Aplicações Jboss Java
Aplicativos	MS / Office 2007 e 2013	Suite de Aplicativos para Escritório
	IE 9 e 10, Chrome e Firefox	*Software* de Navegação Internet (Browser)
***Softwares* / Ferramentas de Gerência / Administração / Monitoração**	Webmin 1.350	Ferramenta de Administração de Servidores
	Awstats 6.6	Ferramenta de Estatística de Sites
	Zabbix 2.0	*Software* de Monitoramento do Ambiente
	McAfee Email Gateway	Ferramenta de Antispam
	Fortigate 3040B / Fortiweb 3000D	Solução de Segurança para Rede Corporativa (Firewall, IPS, Filtro de Conteúdo Web, VPN)

Software	Nome/Versão	Descrição
	Symantec Control Compliance Control Suite	Solução para gestão de vulnerabilidades dos ativos de TI
	VMware vSphere ESXi 5.5	Ferramenta de Virtualização de Servidores
	McAfee Endpoint Protection	Solução de antivirus
	Jabber – OpenFire 3.7.1	Administração Chat
	Cacti 0.8.8b	Ferramenta de Estatística de Utilização de Rede
	Windows Media Services 9.0	Serviço de Streaming de Video
Gerenciador de Banco de Dados e ferramenta ETL	Postgres 9.1.3	Sistema gerenciador de banco de dados Postgres
	MySql 5.0.26	Sistema gerenciador de banco de dados MySql
	SqlServer 2008	Sistema gerenciador de banco de dados SqlServer
	Ingres II 10.1	Sistema gerenciador de banco de dados Ingres
	Brs 8 0	Sistema gerenciador de banco de dados Brs
	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 Novell Access Manager 2 6.0 Novell iManager 2 7.0 Provisioning Module for Novell Identity Manager 2.7 Microsoft Active Directory 2008	Solução de Gerenciamento de Identidades e Controle de Acesso
Servidores Web	IMAP 4.1.3	Servidor de POP IMAP Courier
	PostFix 2.4.3	Servidor de SMTP
	Squid 3.1.1	Servidor de Webcache
	Open LDAP	Servidor de Diretórios
Solução para backup e restore	Symantec NetBackup 7.5	Cópias de segurança
Solução para arquivamento	Symantec Enterprise Vault 11	Arquivamento de arquivos

ANEXO III DO TERMO DE REFERÊNCIA DO CONTRATO N. 005/2016 - CJF

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 de segurança. Deverá dispor sobre o cronograma para instalação, configuração, testes, validação, documentação e treinamento, indicando os principais riscos e forma de mitigação.	CONTRATADA
D + 10	Comprovar que os técnicos envolvidos nos procedimentos e atividades de implantação são certificados pelo fabricante da solução de segurança.	CONTRATADA
D + 20	Aprovar o Plano de Implantação da solução de segurança.	CJF
D + 45	Entregar todos os equipamentos da solução.	CONTRATADA
D + 55	Emitir o **Termo de Recebimento Provisório** após a entrega do *software* e das documentações.	CJF
D + 85	Finalizar o serviço de implantação da solução com o funcionamento perfeito de todos os *softwares*, em sua última versão. Realizar a transferência de conhecimento e entregar toda documentação técnica dos procedimentos executados no serviço de implantação/ migração.	CONTRATADA
D + 100	Emitir o **Termo de Recebimento Definitivo** após a finalização dos serviços de instalação, configuração e treinamento, acompanhado da documentação técnica detalhada de todos os procedimentos executados.	CJF

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO II DO CONTRATO N. 005/2016 - CJF

PLANILHA DE PREÇOS

Item	Descrição	Produtos que compõem a solução	Qtd.	Valor Unitário	Valor Total
1	**1. Solução de proteção para endpoint com garantia de 24 meses, composto por:**	**Trend Micro Smart Protection Complete Trend Micro Deep Security Enterprise**			
	Estações de trabalho Windows	Trend Micro OfficeScan Enterprise	550	R$ 335,00	R$ 184.250,00
	Estações de trabalho Linux	Trend Micro Server Protect for Linux	50	R$ 335,00	R$ 16.750,00
	Estações de trabalho Mac	Trend Micro Security for MAC (OfficeScan Module)	10	R$ 335,00	R$ 3.350,00
	Servidores Windows	Trend Micro Deep Security	150	R$ 335,00	R$ 50.250,00
	Servidores Linux	Trend Micro Deep Security	300	R$ 335,00	R$ 100.500,00
	Storage	Trend Micro Server Protect for Storage	2	R$ 335,00	R$ 670,00
				A = Total do Item 1	**R$ 355.770,00**

Item	Descrição	Produtos que compõem a solução	Qtd.	Valor Unitário	Valor Total
2	Solução de proteção para e-mail com garantia de 24 meses	Trend Micro Smart Protection Complete Trend Micro ScanMail for Exchange Trend Micro InterScan Messaging Security	2	R$ 23.400,00	R$ 46.800,00
3	Solução de proteção contra ameaças avançadas com garantia de 24 meses	Trend Micro Deep Discovery	2	R$ 426.107,00	R$ 852.214,00
4	Gerência da solução	Trend Micro Smart Protection Complete Trend Micro Control Manager	1	R$ 25.000,00	R$ 25.000,00
				B = Total dos Itens 2 a 4	**R$ 924.014,00**
				C = Valor Total Licenças de Software	**R$ 1.279.784,00**
5	Suporte Técnico		24 meses	R$ 5.425,00	R$ 130.200,00
6	Serviços de instalação, configuração e implantação da solução		1	R$ 46.500,00	R$ 46.500,00
7	Transferência de conhecimento de no mínimo 80 horas para até 2 Técnicos do CONTRATANTE		2	R$ 11.625,00	R$ 23.250,00
				D = Valor Total Serviços	**R$ 199.950,00**

Valor Total do Contrato (C+D)	**R$ 1.479.734,00**