UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Divisão de Suporte Santa Mônica
Av. João Naves de Ávila, 2121 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3225-8036 - www.cti.ufu.br

TERMO DE REFERÊNCIA

1. OBJETO (IN. 04/2014, Art. 14, inciso I e Art. 15)

1.1. REGISTRO DE PREÇOS para eventual contratação de fornecimento da aquisição, manutenção, atualização e upgrade de Solução de Segurança Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, conforme condições, quantidades, exigências e estimativas, estabelecidas neste instrumento:

Grupo	Item	Descrição/Especificação	Qtde
1	1	Solução de Proteção de Estação de Trabalho, Servidores Windows, Linux e MAC Solução de Proteção de Estação de Trabalho para controle de aplicações Solução de Proteção de Estação de Trabalho contra vazamento de informações – DLP	5.000
	1	Implementação das soluções e transferência de tecnologia	20h
	1	Treinamento Oficial do Fabricante	02 Servidores
	1	Licença Banco de Dados SQL Server	02
2	2	Operação Assistida (Quantidade em Horas)	1.000 Hrs

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. JUSTIFICATIVA (IN. 04/2014, Art. 14, inciso II e Art. 16)

Vivemos em um mundo no qual a velocidade de criação e renovação dos aparatos tecnológicos é tão alta, que a segurança fica comprometida. Assim sendo, as organizações enfrentam o desafio de preservar o seu maior patrimônio: a informação, vital para todos os níveis hierárquicos e fundamental para manter a perenidade e sustentabilidade das organizações. O cenário atual mostra que o fluxo de informações dentro das empresas e organizações é cada vez mais intenso e, manter essas informações seguras é fundamental. Com isso, tornou-se indispensável investir na Segurança da Informação e Comunicação (SIC).

A SIC e é composta por práticas exercidas a cada minuto, com o intuito de assegurar que os elementos responsáveis por alimentar, armazenar, processar e distribuir informações estejam protegidos ao máximo contra a quebra da confidencialidade, contra o comprometimento da integridade e contra a indisponibilidade de acesso aos recursos.

Confidencialidade, integridade e disponibilidade são três importantes pilares da Segurança da Informação. A confidencialidade é a garantia de que a informação é acessível somente para pessoas autorizadas; a integridade é a salvaguarda da informação e dos métodos de processamento e, por fim, a disponibilidade é a garantia de que os usuários autorizados obtenham, sempre que necessário acesso à informação e aos ativos correspondentes.

A falta de conhecimento, conscientização e crença por parte da liderança, dos funcionários e dos parceiros de negócios; falta de plano de ação constante e pragas virtuais, como Vírus, Worms, Trojan Horse, Spyware, Adware, RootKits, Botnet e Bombas Lógicas são os principais perigos que ameaçam a SIC de uma empresa.

Cada vez mais as organizações se tornam dependentes das informações contidas em sistemas de informação, mas se esquecem que falhas acontecem. Uma empresa que não possui sistema de segurança coloca em risco sua própria continuidade. Há danos que são irreversíveis e, muitas vezes, o que é possível recuperar custa muito caro.

Destaca-se ainda a ameaça relativa à elevada interconectividade mundial entre os maiores desafios da atualidade, confirmadas pelo World Economic Fórum em suas análises sobre os riscos globais, tanto em 2014 quanto em 2015, em que são evidenciados, entre os grandes riscos tecnológicos, os ataques a redes e infraestruturas críticas da informação; o aumento dos ataques cibernéticos; e os incidentes de fraudes e roubos de dados.

As corporações que fazem uso ou oferecem serviços por meio da Internet ou por outras redes parceiras devem ter extrema preocupação com esse canal de comunicação, pois além do incomensurável benefício de permitir conectividade em âmbito global, também representa, em contrapartida, risco potencial para infestações e recebimentos de pacotes desnecessários e maliciosos.

No cenário atual, as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações efetivas de prevenção e combate às práticas maliciosas no uso de Tecnologia da Informação, por meio de ações transversais, integradoras, interdisciplinares e multissetoriais. Nesta direção, a proteção dos ativos de informação implica na definição de investimentos para um melhor posicionamento das instituições governamentais em relação à produção e custódia, principalmente, às informações dos cidadãos brasileiros e do Estado. Assim posto, os ativos de informação guardam relação direta com riscos de SIC e de Segurança Cibernética (SegCiber), uma vez que a dependência tecnológica das instituições governamentais é cada vez maior.

Observa-se também que em período recente, diversos órgãos e entidades, conforme amplamente divulgado na mídia, foram alvos de ações maliciosas, com destaque para ações de engenharia social, desfigurações de sítios, degradação dos serviços e acessos indevidos a sistemas computacionais, com exposição de 17 vulnerabilidades e consequente vazamento de informações, causando prejuízos ao Estado, com reflexos negativos para a sociedade. Observa-se também a diversificação tanto da metodologia de ataque, gerando variados efeitos, quanto da forma de disseminação. Além disso, o índice de sucesso alcançado tem sido bastante alto e até mesmo grandes corporações têm se ressentido de tais ataques.

As organizações especializadas em segurança têm sido unânimes em suas recomendações e ações no sentido de que a melhor forma de defesa é a integração das várias ferramentas disponíveis, criando-se desta forma um conjunto de barreiras capazes de detectar em tempo hábil qualquer forma de ataque, conhecida ou não, e ao mesmo tempo impedir a sua propagação.

A gestão das contas de acessos privilegiados também é um ponto crítico na manutenção de ambientes computacionais. A auditoria dos acessos e controle das atividades é fator fundamental na gestão de TI.

O Decreto nº 3.505, de 13 de Junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, nos incisos I e V do seu artigo 3º estabelece como objetivos dessa política:

> *"...Art. 3º São objetivos da Política da Informação:*
> *I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;..."*
> *"...V - promover as ações necessárias à implementação e manutenção da segurança da informação;..."*

Baseada nesta orientação, a Coordenação de Tecnologia da Informação, ciente das consequências que podem advir de um ataque à rede da Universidade Federal de Uberlândia - UFU, seja com o objetivo meramente de paralisar a rede de comunicação de dados ou com objetivos mais perniciosos de roubo ou destruição de informações, definiu como prioridade a imediata atualização e expansão do sistema de antivírus atualmente em uso, implementando-se um sistema de defesa mais amplo que contemple também outras formas de ataque.

A solução integrada amplia o número e a intensidade das defesas em face da exponencial curva crescente de complexidade dos ataques e vulnerabilidades e, por ser integrada, racionaliza o controle e a administração resultando numa maior eficiência.

Visando propiciar à Administração Pública uma consecução mais econômica e vantajosa de seus fins, servindo como instrumento de racionalização da atividade administrativa, com redução de custos e otimização da aplicação dos recursos humanos, devemos estabelecer um viés de padronização nas soluções de infraestrutura de TI da Universidade Federal de Uberlândia - UFU.

Prezando pela melhoria da qualidade dos serviços prestados a seus usuários internos e externos, além do contínuo aperfeiçoamento de Governança de TI, especialmente no tocante ao crucial tema da segurança da informação, aponta-se como essencial ao adequado funcionamento de sua estrutura tecnológica a implementação de uma Solução de Segurança e Proteção da Informação eficiente, atualizada e que contemple o quantitativo total dos usuários e dispositivos do Órgão. Além disso, devido ao cenário existente, há a necessidade de economia e redução de custos com eventuais incidentes de segurança.

Para manter o atual parque computacional padronizado e protegido contra as mais atuais técnicas de ataques, atendendo às demandas da Universidade Federal de Uberlândia - UFU, será necessário a aquisição de um pacote integrado de solução de segurança.

Hoje com o advento de novas tecnologias, como celulares smartphone e tablets, além do surgimento de novas formas de explorar vulnerabilidades como os ataques direcionados denominados como “Ameaças Avançadas Persistentes” (APT – Advanced Persistent Threat), torna-se necessário uma expansão de camadas de proteção de segurança, aderindo também a camada de gerenciamento seguro e automatizado na solução, autenticação forte e controle de acesso aos dados.

Ainda em conformidade com os normativos dos órgãos de controle e normativos internos do Órgão e diretivas do Governo Federal em atendimento à Segurança da Informação e Comunicações, faz-se necessário o atendimento aos seguintes tópicos:

A Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 preconiza:

> *“Art. 1º Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.*
> *(...)*
>
> *Art. 2º (...)*
> *VII - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portando, à tecnologia da informação e comunicações;*
> *(...)”*

A Política de Segurança da Informação e Comunicação da Universidade Federal de Uberlândia - UFU preconiza:

> *Art. 19. A CGMI fica autorizada a promover limitações de acesso à rede mundial de computadores, com o objetivo de eliminar, antes de sua chegada aos destinatários, os e-mails que contenham arquivos incompatíveis com os serviços realizados no âmbito do Ministério, respeitando-se o sigilo das informações.*
> *Art. 35.O administrador de rede deverá manter instalados sistemas de segurança. É imprescindível um 'firewall, sendo desejável, além disto, um sistema analisador de conteúdo para proteger a rede sob sua responsabilidade.*

De acordo com o disposto na “Seção III” da Lei nº 12.527, de 18 de novembro de 2011, os órgãos públicos integrantes da administração direta devem adotar medidas para garantir a proteção das informações sigilosas de seus usuários, conforme transcrição a seguir:

> *“Seção III*
> *DA PROTEÇÃO E DO CONTROLE DE INFORMAÇÕES SIGILOSAS*
> *Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.*
> *§ 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.*
> *§ 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.*
> *§ 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.*
> *Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.*
> *Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei.”*

Ainda, conforme o disposto no § 1º do art. 30, do Decreto nº 4.553/2002:

> *“Art. 30. Os documentos sigilosos serão mantidos ou guardados em condições especiais de segurança, conforme regulamento.*
> *§ 1º Para a guarda de documentos ultrassecretos e secretos é obrigatório o uso de cofre forte ou estrutura que ofereça segurança equivalente ou superior.”*

A solução a ser implantada visa oferecer altíssimo nível de segurança ao ambiente operacional da Universidade Federal de Uberlândia - UFU, propiciando uma ação proativa às infestações constantes que ocorrem na rede de dados deste órgão, sejam ela as mais conhecidas, assim como, as ameaças mais avançadas, conhecidas hoje como “Ameaças Persistentes Avançadas” (APT – Advanced Persistent Threat), tanto como prover de controle de recebimento e envio de Spam em nosso correio eletrônico.

2.2. ALINHAMENTO AO PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PDTIC (IN. 04/2014, Art. 16, inciso I)

2.2.1. Este processo de aquisição está alinhado ao Plano Diretor de Tecnologia da Informação – PDTIC 2017/2019.

3. DESCRIÇÃO DA SOLUÇÃO (IN. 04/2014, Art. 14, inciso II; Art. 16, inciso II e Art. 12, inciso IV)

3.1. DESCRIÇÃO (DETALHAMENTO DA NECESSIDADE)

3.1.1. Contratação de empresa especializada para fornecimento da aquisição, manutenção, atualização e upgrade de Solução de Segurança Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Universidade Federal de Uberlândia - UFU, conforme detalhamentos e especificações técnicas descritas neste Termo de Referência e seus anexos.

3.2. BENS E/OU SERVIÇOS QUE COMPÕEM A SOLUÇÃO

Item	Descrição/Especificação	Unidade de Medida
1	Solução de Proteção de Estação de Trabalho, Servidores Windows, Linux e mac Solução de Proteção de Estação de Trabalho para controle de aplicações Solução de Proteção de Estação de Trabalho contra vazamento de informações – DLP	Licenças de uso de software
2	Operação Assistida - Pacote de hores de suporte	Horas
3	Treinamento Oficial do Fabricante	Pessoas
4	Licença Banco de Dados SQL Server	Licenças de uso de software

3.3. ESPECIFICAÇÃO TÉCNICA:

3.3.1. Com o fornecimento da solução suportada por fabricantes distintos, será necessário que tal integração seja realizada pela CONTRATADA sem ônus ao Órgão, onde deverá ser possível validar as informações e indicar as ações de segurança a serem seguidas traduzidas em uma linguagem única;
3.3.2. Os requisitos técnicos da solução a ser contratada estão descritos no ANEXO I – do TR.

3.4. RESULTADOS A SEREM ALCANÇADOS

A implantação da solução contribuirá de forma qualitativa nos processos internos da instituição e será capaz de favorecer demais aspectos associados à disponibilização dos serviços de TI. Isto inclui:

3.4.1. A redução dos impactos de manutenção ou relacionados com falhas e paradas de serviços (planejados ou não);
3.4.2. A redução de incidentes que provocam diminuição de desempenho tanto da TI quanto da instituição;
3.4.3. Amplificação da camada de proteção e disponibilidade da informação;
3.4.4. Obtenção de preço mais vantajoso em detrimento de repactuação da contratação da solução atual, haja vista a validade contratual a muito expirada;
3.4.5. Eficiência do trabalho, diminuindo custos administrativos;
3.4.6. Aumentar a eficiência contra as vulnerabilidades, segurança, proteção e autenticidade de dados sensíveis da organização, controlando pró-ativamente todos os pontos possíveis de acesso não autorizado as informações sensíveis (endpoint, rede e storage);
3.4.7. Integração obtidas entre os módulos de segurança, acarretando em uma visão unificada do ambiente de segurança de dados, possibilitando uma tomada de ação mais eficaz e rápida;
3.4.8. Os ciberataques, muitas vezes, são originados no ambiente interno da rede utilizando-se de dados fornecidos por pessoas da própria organização ou por acessos indevidos, conseguidos por meio de engenharia social. Trata-se de uma ameaça vinda de usuários comuns internos, muitas vezes desavisados e/ou mal-intencionados. É imperiosa a necessidade de gerencia, informação customizada e integrada relacionada aos mais recentes tipos, meios, métodos e origens de como estas novas ameaças podem ser mitigadas e prevenidas;
3.4.9. Proteção, autenticidade e acessibilidade as informações.

4. NECESSIDADE DE NEGÓCIO DA ÁREA REQUISITANTE (IN. 04/2014, Art. 17, inciso I)

4.1. REQUISITOS DE NEGÓCIO

4.1.1. Proteção de dados independente de onde estão armazenados seja em ambientes locais ou compartilhamentos, monitorando como estão sendo usados dentro e fora da rede da Órgão e protegendo-os contra roubo e mal uso;
4.1.2. Proteção, monitoração e inspeção do tráfego web, possibilitando validar como estão sendo usados os dados dentro e fora da rede da Órgão e protegendo-os contra roubo e mal uso;
4.1.3. À medida que os dados são distribuídos em diferentes áreas de armazenamento sejam públicas ou privadas, a capacidade de impor consistentemente as políticas de segurança e conformidade se torna ainda mais crítica;
4.1.4. Proteção de dados durante o tráfego de e-mail, externo ao ambiente do Órgão;
4.1.5. Componente de auxílio na proteção contra o vazamento de dados sendo enviado externo ao ambiente gerenciado pelo Órgão;
4.1.6. Simulação de ataque de Phishing possibilitando o levantamento do nível de maturidade dos usuários quanto a prevenção de tais ataques;
4.1.7. Auxílio no crescimento e homogeneização da maturidade dos usuários finais, possibilitando treinamento na identificação de tais ameaças;
4.1.8. Descoberta de dados independente de onde estão armazenados na nuvem, em dispositivos móveis e em ambientes locais, monitorando como estão sendo usados dentro e fora da rede da Órgão e protegendo-os contra roubo e/ou vazamento;
4.1.9. À medida que os dados são distribuídos em diferentes aplicativos e dispositivos, a capacidade de impor consistentemente as políticas de segurança e conformidade se torna ainda mais crítica, a partir de console de gerenciamento unificado a criação de políticas uma única vez, as impõe em todos os locais e corrige incidentes rapidamente com fluxos de trabalho automatizados;
4.1.10. Possibilidade de otimização de todas as operações de gerenciamento de sistemas e endpoints obtendo economias imediatas e eficiências organizacionais. A partir do conceito do portfólio unificado de segurança e gerenciamento de endpoints padronizado em toda a infraestrutura de TI;
4.1.11. Capacidade de fornece uma visão global da TI, combinada à capacidade de modelar as responsabilidades organizacionais;
4.1.12. Capacidade de entregar serviço avançado e redução de problemas na instalação, através da implementação de sistemas e processos de migração padronizados;
4.1.13. Capacidade de promove maior inteligência ao Órgão em relação à distribuição de software, gerenciamento de licenças de software e conformidade com as políticas de gerenciamento de software;
4.1.14. Capacidade de orquestrar o fortalecimento dos sistemas e a proteção contra ameaças sem agentes e baseada em políticas para ambientes VMware;
4.1.15. Possibilidade de monitoração e o fortalecimento contínuos da segurança para servidores locais, AWS e nuvens OpenStack;
4.1.16. Possibilita que o Órgão monitore os sistemas continuamente e permitindo o fortalecimento baseado no host dos servidores físicos e virtuais locais, AWS e nuvens OpenStack;
4.1.17. Capacidade de implementar automaticamente o antimalware sem agentes e a proteção contra ameaças na rede ambientes VMware;
4.1.18. Possibilita a utilização do VMware NSX para automatizar a orquestração baseada em políticas das configurações de segurança;
4.1.19. Detecção e proteção de ameaças com base na rede e sem agente (IPS de rede);
4.1.20. Capacidade de fornecer informações de segurança prontas para uso e automatiza da área de segurança do Órgão, através da segurança baseada em políticas, habilitando serviços de segurança centrados no aplicativo e integrados ao VMware;
4.1.21. Possibilidade de implementar ações de quarentena de arquivos nos servidores atacados com correção baseada em política;
4.1.22. Proteção da informação contra ameaças avançadas independente de onde estão armazenados seja em ambientes locais ou compartilhamentos, monitorando como estão sendo usados dentro e fora da rede da Órgão e protegendo-os contra roubo e mal uso;
4.1.23. À medida que os dados são distribuídos em diferentes áreas de armazenamento, a proteção contra ataque de APT deve ser estendida aos mesmos níveis contemplando minimamente o ambiente dos endpoints e rede;
4.1.24. Capacidade de monitorar e indicar providencias em um eventual ataque;
4.1.25. Capacidade de identificar tentativas de acessos mal-intencionados;
4.1.26. Capacidade de integração e monitoração com a grande maioria das plataformas de segurança, proporcionando controle das informações.

4.2. REQUISITOS DE CAPACITAÇÃO

4.2.1. A CONTRATADA deverá repassar ao CONTRATANTE todas as informações solicitadas e documentação exigida nesse Termo de Referência;
4.2.2. A CONTRATADA deverá prover treinamento oficial do fabricante para a solução de segurança para capacitar até 02 funcionários e auxiliar na utilização das ferramentas e recursos da solução;
4.2.3. Deverá ser fornecido repasse de conhecimento customizado para o ambiente da CONTRATANTE da(s) solução(ões) adquirida(s);
4.2.4. O treinamento deverá ser ministrado por técnico certificado com certificações técnicas (não comerciais e/ou técnica-comercial) pelo fabricante nos

componentes da solução ofertada;
4.2.5. A transferência de tecnologia deverá capacitar as equipes locais e as do CONTRATANTE principal a operar, configurar, administrar e resolver problemas usuais na solução ofertada, englobando tanto os componentes de hardware quanto de software ofertados;

4.2.5.1. A transferência da tecnologia será realizada em salas disponibilizadas pelo CONTRATANTE e deverá englobar as instruções para o uso de todas as ferramentas solicitadas em edital ou neste Termo de Referência. O instrutor deverá possuir pleno conhecimento da ferramenta;
4.2.5.2. A capacitação deverá contemplar, no mínimo, os seguintes tópicos:

a. Introdução;
b. Tipos de malware;
c. Instalação em ambientes Windows e Linux;
d. Criação de pacotes de instalação; e. Configuração dos módulos que compõem a solução;
f. Configuração de proteção para:

- Navegação;
- Arquivos compactados;
- Discos removíveis; e
- E-mails.
- g. Gerenciamento centralizado das funcionalidades via console;

h. Atualização de softwares e vacinas.

4.2.5.3. A capacitação deverá ser avaliada por meio de formulário de AVALIAÇÃO, constante no ANEXO VI – do TR;
4.2.5.4. A capacitação somente será tida por aceito no caso de uma avaliação média deste pelos alunos for igual ou superior de 80%. No caso de avaliação abaixo de 80%, deverão ser realizados os seguintes procedimentos:

Item	Avaliação Média da Capacitação (A)	Procedimento a Ser Realizados
1	80% > A ≥ 70%	Ministrar aulas de reforço de 2 (duas) horas- aulas.
2	70% > A ≥ 60%	Ministrar aulas de reforço de 4 (quatro) horas- aulas.
3	A < 60%	Realizar nova capacitação

4.2.6. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.

4.3. REQUISITOS LEGAIS

4.3.1. O processo de licitação deverá obedecer a Lei 8.666, de 21 de junho de 1993, o Decreto 5.450 de 31 de maio de 2005, o Decreto nº 7.174, de 12 de maio de 2010, o Decreto nº 7.892, de 23 de janeiro de 2013, a Instrução Normativa nº 4, de 11 de setembro de 2014, , o Plano Diretor de Tecnologia da Informação - PDTI 2017-2019, legislação correlata, e demais exigências previstas em Edital e seus anexos.

4.4. REQUISITOS DE MANUTENÇÃO

4.4.1. Licença de uso com validade de 60 meses.

4.5. REQUISITOS TEMPORAIS (DE PRAZOS)

4.5.1. O prazo de entrega e instalação deverá ser de no máximo 60 (Sessenta) dias, contados da assinatura do contrato;
4.5.2. Garantia de funcionamento pelo período de 60 (sessenta) meses;
4.5.3. O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia não poderá exceder 120 (cento e vinte) minutos, a contar da abertura do chamado telefônico ou registro em sistema web para os dias úteis de 08:00 às 17:00.

4.6. REQUISITOS DE SEGURANÇA

4.6.1. Atendimento à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

4.7. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

4.7.1. A contratação deverá obedecer ao disposto no Decreto nº 99.658, de 30 de outubro de 1990, no Decreto nº 6.087, de 20 de abril de 2007 e na Instrução Normativa SLTI/MP nº 1, de 19 de janeiro de 2010.

5. MACRO REQUISITOS TECNOLÓGICOS (IN. 04/2014, Art. 17, inciso II)

5.1. REQUISITOS DE ARQUITETURA TECNOLÓGICA

5.1.1. A CONTRATANTE deverá fornecer o espaço físico e os recursos necessários à execução dos serviços, equipamentos de informática (incluindo servidores e computadores de atendimento), software (incluindo sistema operacional), de acordo com as especificações técnicas do projeto, suprimentos de informática, materiais, instalações, meios de comunicação e mobiliário para a equipe.
5.1.2. A CONTRATADA devera fornecer software de banco de dados homologado pela solução e sua licença, sem limite de capacitada;
5.1.3. A CONTRATADA deverá fornecer a licença perpétua do software SQL Server 2016 ou superior no modelo de licenciamento por Núcleo;
5.1.4. A CONTRATADA deverá fornecer a licença perpetua do software SQL Server 2016 ou superior para no mínimo 4 núcleos.

5.2. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

5.2.1. A CONTRATANTE deverá fornecer ambiente com todas as operações de backup atualizadas;
5.2.2. A CONTRATANTE deverá fornecer diagrama de rede atualizado para estudo de viabilidade de implantação da solução a ser contratada.

5.3. REQUISITOS DE IMPLANTAÇÃO

5.3.1. A CONTRATADA deverá prover equipe técnica de implantação capacitada na solução;
5.3.2. A CONTRATADA deverá prover hardwares e softwares atualizados com as últimas versões disponibilizadas pelo fabricante;
5.3.3. A CONTRATADA deverá prover instalador da solução contratada, assim como, suas atualizações;
5.3.4. A CONTRATADA deverá acompanhar os testes e a homologação, junto com os técnicos da CONTRATANTE, dos novos produtos ou pacotes de atualização/correção disponibilizados pelo fabricante.

5.4. REQUISITOS DE GARANTIA E MANUTENÇÃO

5.4.1. A CONTRATADA assegurará garantia integral dos softwares pelo período de 60 (sessenta) meses a partir da data do aceite da instalação, prestada no local onde os software estiver instalado (on site), sem ônus para a CONTRATANTE;
5.4.2. A CONTRATADA assegurará, durante o período de garantia, o perfeito e integral funcionamento do software, sem ônus para a CONTRATANTE;

5.4.3. Durante o prazo de garantia da SOLUÇÃO, a substituição de peças e/ou componentes da SOLUÇÃO será feita sem custo para a CONTRATANTE, sob a forma de permuta on-site. As peças e/ou componentes novos deverão ser compatíveis com a SOLUÇÃO, não podendo ser de configuração ou qualidade inferior à substituída;
5.4.4. Durante todo o período de garantia deverá ser disponibilizado para a instalação em até 15 dias de seu lançamento, todas as atualizações de produto, assim como, novas versões;
5.4.5. Suporte na modalidade 8x5x365 deverá ser realizado pela CONTRATADA;
5.4.6. Atendimento local deverá ser realizado na sede da CONTRATANTE;
5.4.7. Durante o período de garantia do software, a CONTRATADA deverá prestar, sem ônus adicional para a CONTRATANTE, na localidade onde o software estiverem instalados, assistência técnica oferecendo, no mínimo, os seguintes serviços:
5.4.7.1. Atendimento telefônico, com funcionamento de segunda a sexta-feira, das 08:00 às 17:00 horas, para registro e acompanhamento dos chamados de suporte técnico visando esclarecer dúvidas relativas ao uso dos componentes da solução;
5.4.7.2. Deslocamento de técnicos e/ou mão de obra para atendimento de segunda a sexta-feira, das 08:00 às 17:00;

5.4.8. Durante o período de garantia a CONTRATADA deverá disponibilizar um Portal de Serviços, no padrão web (informar na Proposta comercial de Preço – item 15.5.2) que permita o acompanhamento de todos os chamados técnicos da CONTRATANTE, seu gerenciamento e a geração de relatórios gerenciais;
5.4.9. O Portal de Serviços deverá disponibilizar as seguintes funcionalidades básicas:

5.4.9.1. Abertura e fechamento de chamados técnicos on-line;
5.4.9.2. Situação on-line das ocorrências em andamento;
5.4.9.3. Geração de relatórios de intervenções técnicas;
5.4.9.4. Geração de relatórios gerenciais.

5.4.10. A CONTRATADA deverá permitir a abertura e fechamento de chamado técnico por meio de acionamento telefônico e por meio de Portal de Serviços. Os relatórios do portal deverão conter as informações de chamados abertos via telefone e via portal;
5.4.11. A CONTRATADA ficará responsável pelo registro e gerenciamento dos chamados técnicos;
5.4.12. A CONTRATADA apresentará documento contendo esquema de funcionamento da assistência técnica e do suporte técnico que atenderão aos chamados técnicos;
5.4.13. Caso ocorram alterações no documento mencionado no item anterior, a CONTRATADA deverá entregar novo documento com as atualizações realizadas no prazo máximo de 5 (cinco) dias úteis;
5.4.14. O serviço de suporte técnico deverá permitir o acesso da CONTRATANTE à base de conhecimento do fabricante da solução, provendo informações, assistência e orientação para: instalação, desinstalação, configuração e atualização de imagem de firmware, aplicação de correções (patches), diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento da solução;
5.4.15. A CONTRATADA deverá promover o isolamento e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento da solução;

5.4.15.1. Serão consideradas falhas de laboratório o comportamento ou característica dos programas que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados pelo CONTRATANTE como prejudiciais ao seu uso.

5.5. REQUISITOS DE CAPACITAÇÃO TECNOLÓGICA

5.5.1. A Contratada deverá prover treinamento oficial do fabricante para a solução de segurança para capacitar até 02 funcionários e auxiliar na utilização das ferramentas e recursos da solução;
5.5.2. A CONTRATADA será responsável por ministrar capacitação, no intuito de capacitar os servidores a disseminar, implantar e gerenciar a solução ofertada. Esta demanda será solicitada pela CONTRATANTE mediante Ordem de Serviço Específica;
5.5.3. A CONTRATADA será responsável por ministrar capacitação, no intuito de capacitar os servidores a disseminar, implantar e gerenciar a solução ofertada. Esta demanda será solicitada pela CONTRATANTE mediante Ordem de Serviço Específica;
5.5.4. A CONTRATADA será responsável pelo fornecimento de todo o material didático e de suporte necessários à execução da capacitação, sem qualquer ônus para a CONTRATANTE;
5.5.5. Todas as capacitações deverão ser realizadas em português e o material didático deverá estar redigido em língua portuguesa e/ou inglesa;
5.5.6. 6.8 A capacitação deverá ser aplicada em laboratório providenciado pela CONTRATADA, com a disponibilização de computadores onde as ferramentas, objeto da capacitação, deverão estar instaladas e prontas para uso;
5.5.7. A transferência de tecnologia será realizada em salas disponibilizadas pelo CONTRATANTE e deverá englobar as instruções para o uso de todas as ferramentas solicitadas em edital ou neste Termo de Referência. O instrutor deverá possuir pleno conhecimento da ferramenta;
5.5.8. A capacitação deverá contemplar, no mínimo, os seguintes tópicos:

5.5.8.1. Introdução;
5.5.8.2. Tipos de malware;
5.5.8.3. Instalação em ambientes Windows e Linux;
5.5.8.4. Criação de pacotes de instalação; e. Configuração dos módulos que compõem a solução;
5.5.8.5. Configuração de proteção para:

5.5.8.5.1. Navegação;
5.5.8.5.2. Arquivos compactados;
5.5.8.5.3. Discos removíveis; e
5.5.8.5.4. E-mails.

5.5.8.6. Gerenciamento centralizado das funcionalidades via console;
5.5.8.7. Atualização de softwares e vacinas.

5.5.9. A transferência de conhecimento deverá proporcionar ao treinando as condições de:

5.5.9.1. Conhecer todos os módulos e funções da Solução;
5.5.9.2. Efetuar ajustes de configuração da Solução;
5.5.9.3. Criar e utilizar interfaces com o usuário;
5.5.9.4. Criar e alterar regras de transformação e tratamento de mensagens e arquivos;
5.5.9.5. Integrar a Solução com os produtos da CONTRATANTE e sistemas legados, utilizando qualquer dos protocolos oferecidos;
5.5.9.6. Identificar a causa dos problemas mais comuns e sua solução;
5.5.9.7. Utilizar as ferramentas de monitoração e gerenciamento existentes;
5.5.9.8. Implementar, ajustar e tratar a detecção de mensagens indesejadas;
5.5.9.9. Implementar, ajustar e tratar as funcionalidades de listas restritivas;
5.5.9.10. Criar novas listas restritivas para uso da solução;

5.5.10. A capacitação deverá ser avaliada por meio de formulário de AVALIAÇÃO, constante no ANEXO II – do TR;
5.5.11. A CONTRATANTE poderá alterar o cronograma e o conteúdo da capacitação, caso julgue necessário, para o melhor aproveitamento de seus funcionários;
5.5.12. A capacitação somente será tida por aceito no caso de uma avaliação média deste pelos alunos for igual ou superior de 80%. No caso de avaliação abaixo de 80%, deverão ser realizados os seguintes procedimentos:

Item	Avaliação Média da Capacitação (A)	Procedimento a Ser Realizados
1	80% > A ≥ 70%	Ministrar aulas de reforço de 2 (duas) horas- aulas.

2	70% > A ≥ 60%	Ministrar aulas de reforço de 4 (quatro) horas- aulas.
3	A < 60%	Realizar nova capacitação sem ônus para a CONTRATANTE

5.6. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

5.6.1. O responsável pela capacitação deverá possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a ministrar treinamento na solução. O técnico que prestará o suporte da solução deverá possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a realizar as atividades de suporte e manutenção da solução.

5.7. REQUISITOS DE FORMAÇÃO DA EQUIPE

5.7.1. O técnico que prestará o suporte para implementação, suporte avançado e configuração da solução deverá possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a realizar as atividades de implementação, suporte avançado e configuração da solução.

5.8. REQUISITOS DE METODOLOGIA DE TRABALHO

5.8.1. A CONTRATANTE comunicará a CONTRATADA quando uma "Ordem de Serviço – OS", conforme ANEXO II – do TR, estiver sendo elaborada para que a mesma possa se manifestar no interesse para definição da execução da aquisição e consequentemente atualização e garantia da solução contratada;
5.8.2. Deve-se seguir a seguinte sequência de eventos:

5.8.2.1. Realização de Reunião Inicial antes da emissão da Ordem de Serviço, a ser marcada pelo Gestor do Contrato;
5.8.2.2. Emissão e entrega da Ordem de Serviço;
5.8.2.3. Entrega do Projeto de Implementação pela CONTRATADA;
5.8.2.4. Capacitação para uso de todas as ferramentas definidas na ordem de serviço;
5.8.2.5. Entrega, instalação e configuração da solução;
5.8.2.6. Execução das manutenções preventivas e corretivas, mediante abertura de chamado, ou de forma proativa através da instalação de atualizações de software e base de dados;
5.8.2.7. Aferição mensal dos indicadores de níveis de serviço.

5.8.3. A execução do projeto será realizada de acordo com o cronograma abaixo. Os prazos estabelecidos são os prazos máximos de duração de cada fase.

Item	Descrição do evento	Prazo Máximo	Responspavél
1.	Abertura da ordem de serviço	D1	CONTRATANTE
2.	Projeto de Implementação	D2 = D + 10	CONTRATADA
3.	Reunião Inicial de Projeto	D3 = D2 + 1	CONTRATANTE E CONTRATADA
4.	Entrega dos produtos	D4 = D1 + 10	CONTRATADA
5.	Treinamento	D5 = D4 + 30	CONTRATADA
6.	Instalação, configuração e implantação	D6 = D4 + 30	CONTRATADA

5.8.4. O projeto de implementação é de responsabilidade da CONTRATADA, mas deve ser elaborado em conjunto com a CONTRATANTE e levar em consideração as especificidades da CONTRATANTE. Deve considerar a instalação e configuração em etapas;
5.8.5. A CONTRATADA deverá elaborar e entregar Plano de Implementação descrevendo a estratégia de implementação da SOLUÇÃO, incluindo descrição das atividades e estratégia de implementação, dentro do prazo estipulado na tabela acima apresentada;
5.8.6. A CONTRATADA deverá elaborar dentro do prazo estipulado na tabela acima apresentada, Plano de Testes, incluindo roteiro completo de testes que serão realizados, visando a confirmação de que a implementação foi realizada com sucesso e de acordo com os planos desenvolvidos, e, após os testes, entregar documentação dos Planos de Implementação e Testes em mídias magnéticas;
5.8.7. A CONTRATANTE emitirá Termo de Recebimento Provisório, conforme ANEXO III do TR sendo confirmada a instalação dentro do especificado na ordem de serviço, nos termos deste Termo de Referência;
5.8.8. Após 30 (trinta) dias corridos da emissão do Termo de Recebimento Provisório, sendo confirmada sua operação e desempenho a contento, nos termos deste Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, conforme ANEXO IV – do TR;
5.8.9. Os serviços de suporte técnico serão realizados pelo telefone, web e por e-mail.
5.8.10. Operação Assistida

5.8.10.1. O órgão oficializará a solicitação deste apoio por meio da emissão de uma "Ordem de Serviço – OS";
5.8.10.2. A Ordem de Serviço deverá conter no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;
5.8.10.3. Os serviços prestados deverão estar no mínimo de acordo com as especificações constantes na Ordem de Serviço;
5.8.10.4. O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo órgão, durante a execução – com o acompanhamento e supervisão de responsáveis do órgão, e ao término da execução – com o fornecimento de "Relatórios de Atividade da Operação Assistida" pela CONTRATADA e atesto dos mesmos por responsáveis do órgão;
5.8.10.5. O "Relatório de Atividade da Operação Assistida" deverá conter:

5.8.10.5.1. Identificação do Relatório de Atividade Operação Assistida;
5.8.10.5.2. Data da Emissão;
5.8.10.5.3. Número do Contrato;
5.8.10.5.4. Descrição detalhada das atividades executadas e, se for o caso, o detalhamento da solução proposta para os problemas apresentados.

5.8.10.6. A partir da emissão da "Ordem de Serviço – OS", a CONTRATADA terá até 05 (cinco) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;
5.8.10.7. O órgão comunicará à CONTRATADA quando uma "Ordem de Serviço – OS" estiver sendo elaborada para que a CONTRATADA possa se manifestar no interesse de agendamento de reunião para definição de procedimentos e horas necessárias para execução dos serviços;
5.8.10.8. As horas e procedimentos previstos inicialmente quando da abertura da "Ordem de Serviço – OS" serão validados no final das atividades e poderão sofrer adequações para estarem de acordo com o que foi efetivamente executado.

5.9. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

5.9.1. Atendimento à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
5.9.2. A CONTRATADA obriga-se por seus empregados, sócios, diretores e mandatários, manter total sigilo e confidencialidade no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ela relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados;
5.9.3. A CONTRATADA irá gerenciar a segurança das informações e dados com os esforços necessários para restringir o acesso não autorizado. A CONTRATADA fará os esforços necessários para garantir que seus empregados e representantes estejam inteiramente cientes dos riscos associados com problemas e riscos inerentes à segurança da informação;
5.9.4. Ambas as partes concordam em manter a confidencialidade de toda a informação a respeito dos negócios, ideias, produtos, clientes ou serviços da outra parte, que podem ser consideradas como "informação confidencial";
5.9.5. A CONTRATANTE analisará a liberação dos acessos às dependências, equipamentos e sistemas que forem necessários à prestação dos serviços, a fim de que os serviços sejam prestados e mantidos em conformidade com os termos desta especificação;
5.9.6. Para tanto, a CONTRATADA deverá disponibilizar previamente as Informações necessárias para acesso aos ambientes e atender às normas e políticas de segurança utilizadas pela CONTRATANTE;

6. OBRIGAÇÕES DO CONTRATANTE (IN. 04/2014, Art. 18, inciso I, alíneas “a” à “i”)

6.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do Contrato para acompanhar e fiscalizar a execução do contrato;
6.2. Encaminhar formalmente a demanda, por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência;
6.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
6.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando se tratar de contrato oriundo de Ata de Registro de Preços;
6.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;
6.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação;
6.7. Definir produtividade ou capacidade mínima de fornecimento da Solução de Tecnologia da Informação por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;
6.8. Prever que os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração, justificando os casos em que isso não ocorrer.

7. OBRIGAÇÕES DA CONTRATADA (IN. 04/2014, Art. 18, inciso II, alíneas “a” à “i”)

7.1. Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;
7.2. Atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual;
7.3. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;
7.4. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;
7.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
7.6. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;
7.7. Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato;
7.8. Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito para fins de comprovação de atendimento das especificações técnicas; e
7.9. Acatar todas as diretrizes e normas estabelecidas pela CONTRATANTE, para execução plena do objeto deste Termo de Referência;
7.10. Submeter-se à fiscalização da CONTRATANTE, no tocante à prestação dos serviços, prestando esclarecimentos solicitados e atendendo imediatamente qualquer reclamação, caso venham a ocorrer;
7.11. Prestar as atividades objeto da licitação, utilizando de mão de obra qualificada e devidamente especializada, necessária à completa e perfeita execução dos serviços, em conformidade com as especificações deste Termo de Referência;
7.12. Aceitar nas mesmas condições contratuais os acréscimos ou supressões necessárias, até o limite previsto no § 1º, do art. 65, da Lei nº 8.666/93;
7.13. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, hospedagem e transporte, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto desta licitação;
7.14. Comunicar ao Fiscal do Contrato ou a seu substituto, indicado pela CONTRATANTE, por escrito, qualquer anormalidade que ponha em risco a execução dos serviços;
7.15. 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 a CONTRATANTE ou a não prestação satisfatória dos serviços;
7.16. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas reconhecendo serem estes de propriedade exclusiva da CONTRATANTE;
7.17. Substituir imediatamente, a critério da 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.
7.18. Assumir inteira responsabilidade por quaisquer danos ou prejuízos causados por seus empregados ou por terceiros sob sua responsabilidade, por negligência, imprudência ou imperícia, não se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pela CONTRATANTE;
7.19. Fornecer todos os documentos e manuais necessários para garantir o bom funcionamento, suporte e manutenção dos softwares fornecidos;
7.20. Refazer, sem ônus para a CONTRATANTE, dentro do prazo estabelecido, os serviços prestados que apresentem defeitos, erros, danos, falhas e/ou quaisquer outras irregularidades em razão de negligência, má execução, emprego de mão-de-obra e/ou ferramentas inadequadas;
7.21. Manter, durante o período de vigência do contrato, todas as condições que ensejaram a contratação, particularmente no que tange a regularidade fiscal, desempenho e capacidade técnica operativa;
7.22. Os profissionais disponibilizados pela CONTRATADA para a prestação dos serviços não terão nenhum vínculo empregatício com a CONTRATANTE e deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança da CONTRATANTE, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências;
7.23. Não ceder ou transferir a outra empresa, total ou parcialmente, os serviços contratados;
7.24. Responsabilizar-se por eventuais despesas de custeio com deslocamentos de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos;
7.25. Deverá ser fornecido documento que comprove a importação legal do software conforme Decreto nº 7.174, de 12 de maio de 2010, em seu artigo terceiro, inciso III;
7.26. Submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes na CONTRATANTE e abster-se de veicular publicidade ou qualquer outra informação acerca das atividades desempenhadas, sem prévia autorização da CONTRATANTE;
7.27. Providenciar a assinatura do Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na CONTRATANTE, pelo representante legal da CONTRATADA, conforme ANEXO V deste Termo de Referência;
7.28. Providenciar a assinatura do Termo de Ciência da Declaração de Manutenção de Sigilo e das Normas de Segurança vigentes na CONTRATANTE, por todos os empregados da CONTRATADA diretamente envolvidos na contratação, conforme ANEXO IV deste termo de referência.

8. OBRIGAÇÕES DO ÓRGÃO GERENCIADOR (IN. 04/2014, Art. 18, inciso III, alíneas “a” à “f”)

8.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
8.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
8.3. Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços;

8.4. Autorizar ou não o fornecimento da Solução de Tecnologia da Informação para órgão não participante da Ata de Registro de Preços, desde que prevista no instrumento convocatório, consultando o beneficiário da Ata e verificando as condições de fornecimento, de forma a evitar extrapolações dos limites de produtividade ou de capacidade mínima de fornecimento da Solução;
8.5. Definir mecanismos de comunicação com os órgãos participantes, não participantes, contendo:

8.5.1. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível;
8.5.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável, a exemplo de ordem de serviço ou fornecimento de bens, aplicação de sanções administrativas, alteração de item registrado em Ata por modelo equivalente ou superior;

8.6. Definir mecanismos de controle de fornecimento da Solução de Tecnologia da Informação, observando, entre outros:

8.6.1. A definição da produtividade ou da capacidade mínima de fornecimento da Solução de Tecnologia da Informação;
8.6.2. Regras para fornecimento da Solução de Tecnologia da Informação aos órgãos não participantes, desde que previsto no instrumento convocatório, cujo fornecimento não poderá prejudicar os compromissos já assumidos e as futuras contratações dos órgãos participantes do registro de preços;
8.6.3. Regras para gerenciamento da fila de fornecimento da Solução de Tecnologia da Informação aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela Contratada;
8.6.4. Regras para a substituição da Solução registrada por meio de apostilamento, garantida a realização de Prova de Conceito, observado o disposto no inciso III, alínea "e", item 2 deste artigo e desde que previsto o apostilamento, em função de atualizações tecnológicas existentes no seguimento de informática, na Ata de Registro de Preços; e
8.6.5. Previsão da exigência para realização de diligências e/ou Prova de Conceito com o licitante provisoriamente classificado em primeiro lugar para fins de comprovação de atendimento das especificações técnicas.

9. MODELO DE EXECUÇÃO (IN. 04/2014, Art. 19, inciso I)

9.1. ROTINAS DE EXECUÇÃO

9.1.1. PRAZOS, HORÁRIOS DE FORNECIMENTO DE BENS E PRESTAÇÃO DOS SERVIÇOS E LOCAIS DE ENTREGA, QUANDO APLICÁVEIS (IN. 04/2014, Art. 19, inciso I, alínea "a")

9.1.1.1. Após a assinatura do contrato, para cada módulo ou serviço, a CONTRATANTE emitirá ordem de serviço para solicitar a instalação completa ou realização de algum serviço. A CONTRATADA deverá instalar as licenças e os software no prazo máximo de 30 (trinta) dias corridos contados a partir da data de emissão da ordem de serviço. O prazo para realização de serviços será definido na ordem de serviço;
9.1.1.2. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

9.1.1.2.1. As licenças forem entregues e instaladas pela CONTRATADA atendendo às especificações contidas neste Termo de Referência;
9.1.1.2.2. A CONTRATADA emitir certificado de garantia de 60 meses para as licenças entregues;
9.1.1.2.3. A qualidade do serviço tiver sido avaliada e aceita pela área de TI da CONTRATANTE.

9.1.2. DOCUMENTAÇÃO EXIGIDA (IN. 04/2014, Art. 19, inciso I, alínea "b")

9.1.2.1. A documentação deverá ser fornecida em sua forma original ou copia;
9.1.2.2. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, através de documentos como catálogos, manuais, ficha de especificação técnica, sob pena, na falta destes, de desclassificação da Proposta de Preços da Licitante.

9.2. PAPEIS E RESPONSABILIDADES (IN. 04/2014, Art. 19, inciso I, alínea "c")

Papel		Responsabilidade
UFU	Gestor do Contrato	Declarar formalmente e periodicamente que os serviços estão sendo prestados conforme as especificações solicitadas; encaminhar indicação de sanções para a área administrativa; confeccionar e assinar o termo de recebimento definitivo para fins de pagamento; autorizar emissão de nota fiscal; encaminhar para a área administrativa, eventuais pedidos de modificação contratual; manter os registros formais de todas as ocorrências positivas e negativas da execução do contrato.
	Fiscal Técnico	Acompanhar a execução técnica do contrato em questão, auxiliando o gestor do contrato em todas as tarefas de gestão técnica.
	Fiscal Administrativo	Verificar aderência dos serviços aos termos contratuais e verificar as regularidades fiscais, trabalhistas e previdenciárias da CONTRATADA para fins de pagamento.
	Fiscal Requisitante	Avaliar e justificar a qualidade dos serviços realizados ou bens entregues; identificar a não conformidade com os termos contratuais; verificar a manutenção da necessidade, economicidade e oportunidade da contratação.
CONTRATADA	Preposto	Representar a empresa contratada, acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual, sem que exista a pessoalidade e a subordinação direta com a Administração Pública.
	Técnicos do Contrato	Empregados da contratada responsáveis pela execução contratual direta, pela manutenção e suporte à solução contratada e que poderão ter acesso físico ao ambiente computacional do UFU, sem que exista a pessoalidade e a subordinação direta com a Administração Pública.

9.3. ESTIMATIVA DE VOLUME DE BENS E SERVIÇOS (IN. 04/2014, Art. 19, inciso II)

Demanda Prevista				
Item	Bem/Serviço	Unidade de Medida	Quantidade	Período
01	Solução de Proteção de Estação de Trabalho, Servidores	Licenças de uso de software	5000	60 meses
02	Operação Assistida - Pacote de hores de suporte	Horas	1.000 horas	
03	Treinamento Oficial do Fabricante	Pessoas	02 pessoa	

9.4. MECANISMOS FORMAIS DE COMUNICAÇÃO (IN. 04/2014, Art. 19, inciso III)

9.4.1. A CONTRATANTE emitirá Ordem de Serviço ou Fornecimento de Bens, especificando os serviços e/ou produtos a serem entregues pela CONTRATADA;
9.4.2. Na reunião inicial, que marca o período de execução do contrato, a CONTRATADA deverá indicar formalmente preposto apto a representá-la junto a CONTRATANTE. Esse profissional fará a interação entre a CONTRATANTE e a CONTRATADA, e será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE;
9.4.3. Serão agendadas reuniões, conforme a necessidade, a fim de possibilitar a interação entre a CONTRATANTE e a CONTRATADA, devendo ser registradas pela CONTRATADA em atas as decisões tomadas;
9.4.4. Toda a comunicação entre a Administração Pública e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação;

Instrumento	Objetivo
Ata de Reunião	Apresentação, contextualização, definição de atividades, metas e objetivos, identificação de riscos e problemas.
Ofícios e E-mails	Estabelecer um canal de comunicação entre a CONTRATADA e a CONTRATANTE para tratamento de assuntos gerais e de interesse recíproco.

Ordem de Fornecimento Bens	Solicitação formal de entrega de bens na CONTRATANTE
Ordem de Serviço	Solicitação formal de prestação de serviço
Contato de Abertura de Chamado	Comunicação formal de ocorrência visando a correção de problemas detectados.

9.5. FORMA DE PAGAMENTO (IN. 04/2014, Art. 19, inciso IV)

9.5.1. O pagamento deverá ser efetuado mediante a apresentação de Nota Fiscal ou Fatura pela CONTRATADA, que deverá conter as informações necessárias à conferência do objeto fornecido, incluindo seu valor total, impostos, descontos, em conformidade com o preço contratado;
9.5.2. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 10 (dez) dias corridos, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir;
9.5.3. O pagamento será efetuado pela CONTRATANTE no prazo de 30(Trinta) dias úteis, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária;
9.5.4. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência, no prazo de até 05 (cinco) dias úteis;
9.5.5. Após 30 (trinta) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada sua operação e desempenho a contento, nos termos deste Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, conforme ANEXO IV – do TR;
9.5.6. O aceite/aprovação dos materiais/bens pelo CONTRATANTE, não exclui a responsabilidade civil da CONTRATADA por vícios de quantidade ou qualidade do produto ou disparidade com as especificações técnicas exigidas neste Termo de Referência ou atribuídas pela CONTRATADA verificados posteriormente, garantindo-se ao CONTRATANTE as faculdades previstas no art. 18 da Lei nO8.078/90 (Código de Defesa do Consumidor);
9.5.7. A CONTRATADA terá o prazo de 05 (cinco) dias úteis, contados a partir da comunicação de rejeição do material pelo Controle de Qualidade, para sua retirada. Decorrido este prazo, o CONTRATANTE procederá à sua destruição, não cabendo qualquer tipo de indenização a CONTRATADA;
9.5.8. Antes do pagamento, a CONTRATANTE verificará a regularidade fiscal da CONTRATADA através de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios oficiais;
9.5.9. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE;
9.5.10. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;
9.5.11. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa;
9.5.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF;
9.5.13. No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão os mesmos restituídos à CONTRATADA para as correções necessárias, não respondendo a CONTRATANTE por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes;
9.5.14. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes formulas:

I=(TX/100)/365
EM = I x N x VP, onde:
I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela em atraso".

10. MODELO DE GESTÃO CONTRATUAL (IN. 04/2014, Art. 20)

10.1. CRITÉRIOS DE ACEITAÇÃO DO OBJETO (IN. 04/2014, Art. 20, inciso I)

10.1.1. O aceite da solução deverá ser efetuado por servidores responsáveis pelo acompanhamento e fiscalização do contrato de acordo com critérios estabelecidos na Lei nº. 8.666/93;
10.1.2. O objeto licitado deverá ser entregue e instalado pela própria CONTRATADA ou por técnico (s) da empresa fabricante;
10.1.3. A Solução de Tecnologia da Informação fornecida poderá, a qualquer tempo, ser manuseada por técnicos habilitados da CONTRATANTE;
10.1.4. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

10.1.4.1. A Solução de Tecnologia da Informação for entregue e instalada, atendendo às especificações contidas neste Termo de Referência;
10.1.4.2. A CONTRATADA emitir certificado de garantia de 60 (sessenta) meses on-site para as licenças entregues; e
10.1.4.3. A qualidade do serviço for avaliada e aceita pela área de tecnologia da informação.

10.1.5. Termo de Recebimento Provisório será emitido no prazo de até 5 (cinco) dias corridos após a entrega dos bens;
10.1.6. Termo de Recebimento Definitivo, verificado o cumprimento de todos os requisitos e de acordo com os critérios de aceitação definidos, a CONTRATANTE dará o aceite definitivo, no prazo de até 10 (dez) dias após a implantação dos componentes/software da solução e entrega da documentação conforme previsto nos Requisitos Temporais deste Termo de Referência.

10.2. PROCEDIMENTOS DE TESTE E INSPEÇÃO (IN. 04/2014, Art. 20, inciso II)

10.2.1. Prova de Conceito

10.2.1.1. Caso seja solicitado pelo órgão, a licitante detentora da melhor proposta deverá entregar e instalar amostra do produto, deixando-a em plenas condições operacionais para avaliação, no prazo máximo de 5 (cinco) corridos, contados da convocação do Pregoeiro;
10.2.1.2. A ausência de representante da licitante para dar início ao trabalho de instalação e configuração da amostra em até 5 (cinco) corridos, contados da convocação do Pregoeiro, será motivo de desclassificação da proposta;
10.2.1.3. O produto de amostra deverá ser instalado e configurado em ambiente tornado disponível pelo órgão;
10.2.1.4. A licitante deverá apresentar pelo menos 1 (um) profissional especialista no produto para acompanhar e orientar a avaliação da amostra;
10.2.1.5. O produto de amostra apresentado será examinado no prazo máximo de 10 (dez) dias úteis, contados do recebimento pelo Pregoeiro da comunicação formal da licitante de que o produto de amostra está disponível para avaliação;
10.2.1.6. A amostra será avaliada por comissão formada por 3 (três) servidores do órgão designados para esta finalidade;
10.2.1.7. Será desclassificada a proposta cuja amostra de produto não atenda aos requisitos exigidos como nativos da solução, ou seja, aqueles que devem estar presentes na versão original do produto, sem a necessidade de customização por meio de linguagem de programação, sendo admitida apenas a configuração de parâmetros;
10.2.1.8. Não será aceita a proposta da licitante que:

10.2.1.8.1. Tiver amostra rejeitada;
10.2.1.8.2. Não entregar a amostra;
10.2.1.8.3. Entregar a amostra, mas não a instalar no prazo estabelecido;
10.2.1.8.4. Entregar e instalar a amostra, mas não a configurar no prazo estabelecido.

10.2.1.9. Não será aceita a proposta da licitante que não apresentar o profissional especialista para acompanhar e orientar a avaliação da amostra;
10.2.1.10. A apresentação de amostra poderá ser dispensada quando se tratar de produto oriundo de linha industrial de produção cujo exemplar já tenha sido aprovado em teste anterior realizado pelo órgão;
10.2.1.11. A apresentação de amostra falsificada ou deteriorada, como verdadeira ou perfeita, configura comportamento inidôneo, punível nos termos deste Termo de Referência.

10.2.2. Metodologia, formas de avaliação da qualidade e adequação da Solução de Tecnologia da Informação às especificações funcionais e tecnológicas, observando:

10.2.2.1. A primeira colocada deverá apresentar a documentação que será analisada pela equipe de planejamento (integrantes técnico, requisitante e administrativo), aferindo a qualidade e a aderência às especificações técnicas exigidas;
10.2.2.2. Os Requisitos Técnicos (especificação técnica da solução) serão avaliados por meio de prospecto/documentação;
10.2.2.3. Com o intuito de comprovação dos requisitos obrigatórios exigidos no Termo de Referência haverá o confronto entre Proposta Comercial/prospecto ou manual do fabricante da solução e os requisitos técnicos exigidos, e poderá haver na fase licitatória a promoção de diligência conforme § 3º, inciso VI, art. 43, da Lei 8666/93;
10.2.2.4. A qualidade da solução será avaliada em duas fases. A primeira avaliação será no aceite preliminar e definitivo. A segunda fase de avaliação será durante a execução contratual;
10.2.2.5. A qualidade da solução na fase de execução contratual será avaliada pelos fiscais do contrato que reportarão ao gestor possíveis falhas no atendimento dos requisitos pela solução;
10.2.2.6. Na fase contratual haverá somente o acompanhamento da execução dos serviços pelos fiscais Técnico, Requisitante, Administrativo e pelo Gestor do contrato, que eventualmente poderão solicitar da CONTRATADA comprovação relativa ao serviço que está sendo executado, além dos já previstos no item – Documentação mínima exigida;
10.2.2.7. A CONTRATANTE designará formalmente os Fiscais Requisitante, Técnico e Administrativo para realizar a fiscalização contratual em todas as suas fases de acordo com a Seção III da Instrução Normativa nº 04/2014-SLTI/MP, que trata da Gestão do Contrato;
10.2.2.8. Adoção de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores estabelecidos;
10.2.2.9. Não há necessidade de utilização de ferramentas computacionais para aferição e acompanhamento dos indicadores dos chamados de suporte e assistência técnica, que são baseados na medição do tempo de resolução dos chamados.
10.2.2.10. Origem e formas de obtenção das informações necessárias à gestão e à fiscalização do contrato, conforme disposto na alínea "b" do inciso I do art. 19 da Instrução Normativa nº 04/2014-SLTI/MP;
10.2.2.11. A CONTRATANTE manterá os seus próprios registros e anotações referentes à solução que servirão de base para a fiscalização contratual.
10.2.2.12. A diligências aplicáveis são as previstas conforme § 3º, inciso VI, art. 43, da Lei 8666/93;

10.3. ACORDO DE NÍVEIS DE SERVIÇO (IN. 04/2014, Art. 20, inciso II, alínea “a”)

10.3.1. DA INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

10.3.1.1. A CONTRATANTE disponibilizará o espaço no CTI e refrigeração suficiente para comportar os equipamentos que irá suportar a aplicação, infraestrutura elétrica até o quadro de energia com capacidades (corrente e tensão). A CONTRATANTE se responsabilizará por manter o ambiente que sofrerá intervenção com a última cópia de segurança completa (backup full), realizada e válida;
10.3.1.2. A CONTRATADA deverá instalar a solução ofertada nas instalações da CONTRATANTE.

10.3.2. CONDIÇÕES DE SUPORTE, GARANTIA E MANUTENÇÃO DA SOLUÇÃO

10.3.2.1. O suporte técnico deverá ser prestado para cada solução adquirida e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento "on-site", se requerido pelo CONTRATANTE, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Inicio de Atendimento	Prazo Máximo de Restauração do Serviço
Severidade 1 (ALTA)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor On-site.	Em até 8 horas
		Em até 15 min. um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Gerente técnico do fabricante deve estar disponível 8x5 e ser automaticamente notificado na abertura do caso	Entrega da Solução em até 6 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor On-site.	Em até 16 horas
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 8x5 e ser automaticamente notificado na abertura do caso.	Entrega da Solução em até 10 dias.
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado nas operações.	Em até 8 horas deve ter um técnico do fornecedor On-site.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução em até 15 dias ou na próxima atualização do Software.
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas
		No mesmo dia ou no próximo dia útil comercial	Entrega da Solução em até 20 dias ou considerado para as próximas atualizações do Software

10.3.2.2. O atendimento pelo fabricante deve estar disponível para os produtos de segurança, disponibilidade e pela combinação de ambos;
10.3.2.3. A CONTRATADA deverá disponibilizar 8x5x365 um recurso humano designado para fornecer assistência ao gerenciamento de todos os

incidentes de suporte cadastrados junto ao mesmo;
10.3.2.4. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto no item anterior (item 10.3.2.1), deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;
10.3.2.5. Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via e-mail;
10.3.2.6. Deverão ser executados por parte da CONTRATADA, relatórios trimestrais referentes ao histórico dos incidentes, independentes de seu estado (abertos, fechado e em andamento);
10.3.2.7. Para eventos caracterizados como Severidade 1 e/ou Severidade 2, conforme descritos no item 10.3.2.1, deverão ser disponibilizadas até 4 visitas presenciais solicitadas sob demanda no período de 60 (sessenta) meses em regime 8x5x365 para resolução dos chamados, atividades proativas com acesso as ferramentas de propriedade exclusivas do fabricante para análise de capacidade e reparos;
10.3.2.8. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos via telefone, e-mail, "website" do fabricante;
10.3.2.9. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;
10.3.2.10. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;
10.3.2.11. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;
10.3.2.12. Dentro do prazo máximo de atendimento, cabe a CONTRATADA dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;
10.3.2.13. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;
10.3.2.14. Os serviços de atendimento de suporte para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);
10.3.2.15. A CONTRATADA emitirá relatório sempre que solicitado pelo CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados de suporte abertos e fechados no período, incluindo:

10.3.2.15.1. Quantidade de ocorrências (chamados) registradas no período;
10.3.2.15.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
10.3.2.15.3. Data e hora de abertura;
10.3.2.15.4. Data e hora de inicio e conclusão do atendimento;
10.3.2.15.5. Identificação do técnico do CONTRATANTE que registrou o chamado;
10.3.2.15.6. Identificação do técnico do CONTRATANTE que atendeu o chamado de suporte;
10.3.2.15.7. Descrição do problema;
10.3.2.15.8. Descrição da solução;
10.3.2.15.9. Informações sobre eventuais escalações;
10.3.2.15.10. Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;
10.3.2.15.11. Total de chamados no mês e o total acumulado até a apresentação do relatório;

10.3.2.16. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante;
10.3.2.17. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;
10.3.2.18. Para esses problemas, A CONTRATADA deverá nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa e informar ao CONTRATANTE, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o CONTRATANTE;
10.3.2.19. Esta solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix;
10.3.2.20. As ferramentas e software necessários à manutenção serão de responsabilidade da CONTRATADA;
10.3.2.21. Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;
10.3.2.22. A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE, caso requeiram;
10.3.2.23. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;
10.3.2.24. Durante o período de garantia A CONTRATADA executará, sem ônus adicionais, correções de falhas (bugs) de hardware e software;
10.3.2.25. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.

10.4. Canais de Atendimento:

10.4.1. Será disponibilizado canal de atendimento e chamado técnico 08 (Oito) horas por dia, 5 (cinco) dias por semana através de site na Internet e/ou canal telefônico;
10.4.2. Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante, telefone, etc;
10.4.3. A CONTRATADA deve informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos do software, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso.

10.5. GARANTIA DA SOLUÇÃO DE TI

10.5.1. A CONTRATADA concederá ao CONTRATANTE garantia integral durante 60 (sessenta) meses, “on-site” com atendimento 08 horas por dia e cinco dias por semana, a contar da data de conclusão da instalação do produto, contra qualquer problema em toda a solução.
10.5.2. A CONTRATADA garante por, no mínimo, 60 (sessenta) meses o fornecimento dos componentes de software, para manutenções, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas;
10.5.3. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;
10.5.4. As manutenções preventivas e corretivas serão de responsabilidade da CONTRATADA, sem custos adicionais ao CONTRATANTE;

10.6. PROPRIEDADE, SIGILO E RESTRIÇÕES

10.6.1. A CONTRATADA deverá garantir a segurança das informações da CONTRATANTE e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido da CONTRATANTE no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal;
10.6.2. Toda a documentação gerada durante a vigência do contrato deve ser repassada a CONTRATANTE com todos os direitos de propriedade;
10.6.3. Todos os produtos fornecidos como resultado da execução do projeto serão de propriedade da CONTRATANTE, aplicando-se as restrições relativas aos direitos de propriedade intelectual e direitos autorais da solução de tecnologia da informação, conforme regula a lei nº 9.610/98;
10.6.4. A CONTRATADA deverá submeter-se à Política de Segurança da Informação e Comunicações da CONTRATANTE e abster-se de veicular

publicidade ou qualquer outra informação acerca das atividades desempenhadas, sem prévia autorização da CONTRATANTE;
10.6.5. Após a assinatura do contrato, os profissionais responsáveis pela execução dos serviços deverão assinar o Termo de Compromisso e Manutenção de Sigilo (ANEXO V – do TR), comprometendo-se a preservar as informações a que tiverem acesso em virtude dos serviços prestados.

10.7. DISPONIBILIZAÇÃO DE RECURSOS HUMANOS NECESSÁRIOS ÀS ATIVIDADES DE GESTÃO E FISCALIZAÇÃO DO CONTRATO (IN. 04/2014, Art. 20, inciso II, alínea "b")

Função	Cargo	Atribuições	QTDE
Gestor do Contrato da solução	Função Gerencial	Gestão do contrato conforme Seção III da IN STI/MPOG nº 04/2014.	1
Fiscal técnico do contrato	Analista de TI/ Técnico TI	Fiscalização do contrato quanto à parte técnica, conforme Seção III da IN STI/MPOG nº 04/2014.	1
Fiscal Administrativo do Contrato	Analista Administrativo	Fiscalização do contrato quanto à parte administrativa, conforme Seção III da IN STI/MPOG nº 04/2014.	1
Fiscal requisitante do contrato	Função Gerencial	Fiscalização do contrato quanto ao atendimento dos requisitos de negócio solicitados	1
Preposto	Amplo conhecimento da solução ofertada	Acompanhar e supervisionar a execução contratual e ser o elo entre a fiscalização da CONTRATANTE e a CONTRATADA	1

10.8. SANÇÕES APLICÁVEIS (IN. 04/2014, Art. 20, inciso IV)

10.8.1. Pela inexecução total ou parcial das condições pactuadas, erros de execução, demora na entrega dos materiais, a Administração poderá, garantida a prévia defesa, aplicar à CONTRATADA, as seguintes sanções, sem prejuízo da responsabilidade civil e criminal:

I. Advertência;
II. Multa (na forma do item 10.8.8);
III. Suspensão temporária do direito de participar, por prazo não superior a 02 (dois) anos, em licitação, e impedimento de contratar com o Órgão Sancionador;
IV. Declaração de inidoneidade para licitar ou contratar com o Órgão Sancionador enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior;
V. Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
VI. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados.

10.8.2. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isolada ou cumulativamente;
10.8.3. Caberá ainda ao fiscal, o papel de notificar a empresa CONTRATADA quando da inexecução total ou parcial do objeto;
10.8.4. As sanções previstas de advertência, suspensão temporária e declaração de inidoneidade podem ser aplicadas juntamente com as sanções de multa, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis;
10.8.5. A sanção de declaração de inidoneidade para licitar ou contratar, é de competência exclusiva do Ministro de Estado, do Secretário Estadual ou Municipal, conforme o caso, facultada a defesa do interessado no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação;
10.8.6. A suspensão temporária e o impedimento poderão ser aplicados quando ocorrer:

10.8.6.1. Apresentação de documentos falsos ou falsificados;
10.8.6.2. Reincidência de execução insatisfatória do contrato;
10.8.6.3. Atraso, injustificado, na execução/conclusão do fornecimento, contrariando o disposto no contrato;
10.8.6.4. Reincidência na aplicação das penalidades de advertência ou multa;
10.8.6.5. Irregularidades que ensejem a rescisão do contrato;
10.8.6.6. Condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos;
10.8.6.7. Prática de atos ilícitos visando prejudicar a execução do contrato;
10.8.6.8. Prática de atos ilícitos que demonstrem não possuir idoneidade para contratar com a CONTRATANTE;
10.8.6.9. Descumprimento das obrigações deste contrato, especialmente aquelas relativas às características dos materiais/bens, qualidade, quantidade, prazo ou recusa de fornecimento ou entrega;

10.8.7. Multa moratória de 0,33% por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 dias;
10.8.8. Multa compensatória de 12% sobre o valor total do contrato, no caso de inexecução total do objeto;
10.8.9. Abaixo consta a relação das inexecuções totais ou parciais:

Item	Descrição	Sanções aplicáveis por grau e por reincidência			
		1	2	3	4
1	Atrasar o fornecimento	1 Vez	1 Vez	1 Vez	1 Vez
2	Entregar os bens fora do prazo estipulado	1 Vez	1 Vez	1 Vez	1 Vez
3	Entregar os bens em locais diferentes dos estipulados.	1 Vez	1 Vez	1 Vez	1 Vez
4	Atrasar injustificadamente a entrega dos bens.	1 Vez	1 Vez	1 Vez	1 Vez
5	Entregar os bens em quantidades diferentes da estipulada no edital ou nota de empenho.	1 Vez	1 Vez	1 Vez	1 Vez
6	Entregar os bens com defeitos, avarias ou qualquer outro dano por manipulação incorreta ou falta de zelo	1 Vez	1 Vez	1 Vez	1 Vez
7	Não fornecer o objeto na forma estipulada no edital.	1 Vez	1 Vez	1 Vez	1 Vez
8	Não atender à solicitação de substituição dos materiais com defeitos, avarias ou fora da especificação.	1 Vez	1 Vez	1 Vez	1 Vez
9	Encaminhar nota fiscal em desconformidade com os bens ou quantidades diferentes da entregue na CONTRATANTE	1 Vez	1 Vez	1 Vez	1 Vez
10	Deixar de cumprir quaisquer dos itens do Edital e de seus Anexos, caso houver, não previstos nesta tabela de multas	1 Vez	1 Vez	1 Vez	1 Vez

10.8.10. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente;
10.8.11. As penalidades serão obrigatoriamente registradas no SICAF, e no caso de suspensão de licitar, a CONTRATADA deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste Termo de Referência ou Edital e seus Anexos e demais cominações legais;
10.8.12. Se o motivo ocorrer por comprovado impedimento ou por motivo de força maior, devidamente justificado e aceito pela Administração do CONTRATANTE, a CONTRATADA ficará isenta das penalidades mencionadas;
10.8.13. Aplicar-se-á advertência por faltas consideradas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;
10.8.14. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa;
10.8.15. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade;
10.8.16. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da

comunicação enviada pela CONTRATADA.
10.8.17. Também ficam sujeitas ás penalidades do art. 87, III e IV da Lei n° 8.666, de 1993, as empresas e os profissionais que:

- Tenham sofrido condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de quaisquer tributos;
- Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação
- Demonstrarem não possuir idoneidade para contratar com a administração em virtude de atos ilícitos praticados;

10.8.18. A aplicação de qualquer das penalidades previstas realiza-se-á em processo administrativo que assegurará o contraditório e a ampla defesa á CONTRATADA,
10.8.19. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado á Administração, observado no princípio da proporcionalidade.

10.9. PROCEDIMENTOS PARA EMISSÃO DE NOTA FISCAL E PAGAMENTO (IN. 04/2014, Art. 20, inciso V)

10.9.1. O pagamento será efetuado conforme tabela abaixo, mediante apresentação de Nota Fiscal/Fatura discriminativa referente ao escopo contratada, devidamente atestada pelo setor competente da CONTRATANTE:

Item	Descrição do evento	Percentual a ser pago
1.	Abertura da ordem de serviço	0% (ZERO)
2.	Projeto de Implementação	0% (ZERO)
3.	Reunião Inicial de Projeto	0% (ZERO)
4.	Entrega dos produtos	60% (Sessenta %)
5.	Treinamento	20% (Vinte %)
6.	Instalação, configuração e implantação	20% (Vinte %)

10.9.2. Nos casos onde não houver a necessidade de treinamento (item 5 da tabela acima), o correspondente percentual será acrescido ao item 6;
10.9.3. Os casos que envolverem serviços, como o item 4 do ANEXO I – do TR, serão vinculados 100% do pagamento com a conclusão e aceite do serviço especificado em ordem de serviço;
10.9.4. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência, no prazo de até 05 (cinco) dias úteis;
10.9.5. Após 30 (trinta) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada sua operação e desempenho a contento, nos termos deste Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, conforme ANEXO III – do TR;
10.9.6. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, devendo ser substituído no prazo de até 15 (quinze) dias úteis, à custa da CONTRATADA, sob pena de aplicação das penalidades previstas neste Termo de Referência; e
10.9.7. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do fornecimento, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos em Lei;
10.9.8. O pagamento será efetuado pela CONTRATANTE no prazo de 30 (Trinta) dias úteis, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária;

11. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO (IN. 04/2014, Art. 22)
12.

Grupo	Item	Descrição/Especificação	Qtde	VALOR MÉDIO UNITÁRIO R$
1	1	Solução de Proteção de Estação de Trabalho, Servidores Windows, Linux e mac Solução de Proteção de Estação de Trabalho para controle de aplicações Solução de Proteção de Estação de Trabalho contra vazamento de informações – DLP	5.000	382,00
	1	Implementação das soluções e transferência de tecnologia	01	
	1	Operação Assistida - Pacote de hores de suporte	240	
	1	Treinamento Oficial do Fabricante	02	
	1	Licença Banco de Dados SQL Server	02	
2	2	Operação Assistida	1.000 Horas	374,00
Total				

13. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

13.1. ESTIMATIVA DE IMPACTO ECONÔMICO-FINANCEIRO (IN. 04/2014, Art. 23, inciso I)

13.1.1. O impacto econômico-financeiro no orçamento ocorrerá no ano de 2017, haja vista que se trata de REGISTRO DE PREÇOS, sendo a gestão do orçamento total da Universidade Federal de Uberlândia - UFU.

13.2. CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRO (IN. 04/2014, Art. 23, inciso II)

13.2.1. O cronograma de execução físico e financeiro está previsto para 2017, as fases das entregas dos bens e serviços, os prazos e locais da entrega estão detalhadas nos itens REQUISITOS TEMPORAIS e REQUISITOS DE METODOLOGIA DE TRABALHO deste Termo de Referência.

14. REGIME DE EXECUÇÃO DO CONTRATO (IN. 04/2014, Art. 24)

14.1. PRAZOS E CONDIÇÕES

14.1.1. Após a assinatura do contrato, a CONTRATADA deverá instalar as licenças no prazo máximo de 60 (sessenta) dias corridos após a emissão da ordem de serviço;

14.1.2. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

I. As licenças e os Softwares forem entregues e instalados pela CONTRATADA atendendo às especificações contidas neste Termo de Referência;
II. A CONTRATADA emitir certificado de garantia de 60 meses para as licenças;
III. A qualidade do serviço tiver sido avaliada e aceita pela área de TI da CONTRATANTE.

14.1.3. A documentação deverá ser fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo;
14.1.4. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, através de documentos como catálogos, manuais, ficha de especificação técnica, sob pena, na falta destes, de desclassificação da Proposta de Preços da Licitante.

14.2. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE

14.2.1. Todos os produtos entregues e serviços prestados pela CONTRATADA estarão sujeitos à avaliação e controle de qualidade executados pela CONTRATANTE;
14.2.2. A avaliação da qualidade será realizada no momento da entrega dos produtos e por meio da verificação dos serviços durante e após a sua instalação e configuração;
14.2.3. O controle de qualidade será executado com base nos parâmetros definidos no item 10.3 - NÍVEIS DE SERVIÇO;
14.2.4. Durante a realização dos serviços, os Fiscais Técnicos verificarão a atuação dos profissionais da CONTRATADA quanto ao cumprimento dos roteiros, procedimentos e manuais operacionais, além do cumprimento das normas de segurança da informação da CONTRATANTE;
14.2.5. Todos os produtos deverão atender às especificações contidas neste Termo de Referência e a garantia deverá ser executada conforme as disposições aqui estabelecidas. Só será efetuado pagamento á CONTRATADA após o ateste por parte da CONTRATANTE quanto à adequação às especificações exigidas e à qualidade dos produtos adquiridos.

14.3. NÍVEL MINIMO DE SERVIÇO EXIGIDO (NMSE)

14.3.1. Conforme IN 02/2008 SLTI/MPOG, a verificação da adequação da prestação do serviço deverá ser realizada com base em Níveis de Serviço definido no instrumento convocatório. Níveis de serviço são indicadores mensuráveis estabelecidos pela Entidade capazes de aferir objetiva- mente os resultados pretendidos com as respectivas contratações;
14.3.2. O não cumprimento dos valores mínimos/máximos exigidos nos indicadores ensejará em sanções de acordo com o estipulado na Seção 10.10;
14.3.3. Para execução do contrato e atendimento às Ordens de Serviço, a CONTRATADA deverá atender aos níveis de serviço definidos. A apuração dos níveis de serviço não considerará os períodos justificados decorrentes de:

14.3.3.1. Períodos de interrupção previamente acordados;
14.3.3.2. Indisponibilidade de acesso ao ambiente e/ou aos sistemas da rede, motivada por razões incontroláveis;
14.3.3.3. Falhas da infraestrutura (exemplo: link de comunicação, equipamentos servidores, elementos de rede, etc), desde que não ocasionadas em virtude de ação/omissão por parte de profissional da CONTRATADA;
14.3.3.4. Motivos de força maior (exemplo: enchentes, terremotos ou calamidade pública).

14.3.4. Os Indicadores e definição dos Níveis Mínimos de Serviço Exigidos encontram-se listados a seguir.

INDICADOR PECS – Prazo de Entrega e Configuração da Solução		
Tópico	**Descrição**	
Finalidade	Atender de forma eficiente durante a vigência do contrato à demanda de instalação e configuração de cada módulo da Solução.	
Meta a cumprir	**PECS <= 30**	Cada Módulo deverá estar instalado e configurada em até 30 (trinta) dias contados do Recebimento da
Instrumento de medição	Ordem de Serviço, Relatório de Finalização de Instalação/Atualização e Configuração da Solução, a ser emitido pela CONTRATADA.	
Forma de acompanhamento	O acompanhamento será feito através da verificação do Relatório de Finalização de Instalação/Atualização e Configuração da Solução para	
Periodicidade	Por Ordem de Serviço	
Mecanismo de Cálculo (métrica)	PECS = TG Onde: PECS – Indicador de Prazo de Entrega e Configuração da Solução TG – Tempo Gasto, em dias, gasto para instalar/atualizar e configurar a Solução em todas as estações da CONTRATANTE, a partir do dia segu Observação: Prazos em dias corridos.	
Início de Vigência	Data da emissão da Ordem de Serviço.	
Faixas de ajuste no pagamento e Sanções	Serão aplicados os seguintes ajustes/sanções, caso a meta do indicador PECS não seja atingida: Se PECS for maior que 30 e menor que 40, a CONTRATADA receberá multa de 5% sobre o valor da Ordem de Serviço. Se PECS for maior ou igual a 40 e menor que 60, a CONTRATADA receberá multa de 10% sobre o valor da Ordem de Serviço. Para valor de PECS igual ou superior a 60, configura-se inexecução parcial do contrato por parte da empresa, ensejando a rescisão contratu	

INDICADOR NMA – Nota Mensal de Avaliação		
Tópico	**Descrição**	
Finalidade	Atender de forma eficiente durante a vigência do contrato às demandas de manutenção, atualização e assistência técnica, solicitadas por o	
Meta a cumprir	**NMA >= 9,5**	Efetuar o atendimento nos prazos estabelecidos, de forma que a avaliação mensal seja maior ou igual a 9,5.
Instrumento de medição	O tempo de atendimento iniciará a partir da abertura da solicitação, via telefone e registrado em sistema próprio de gestão de demandas d	
Forma de acompanhamento	O acompanhamento será feito através das ferramentas disponíveis, utilizadas pela CONTRATANTE ou por outras ferramentas que venham a comunicação formal, como e-mail. Mensalmente, o Fiscal Técnico do contrato realizará a consolidação dos Relatórios de Execução de Serviço, emitidos pela CONTRATADA e fa Mensal de Avaliação – NMA, considerando os pontos perdidos nas avaliações dos indicadores estabelecidos.	
Periodicidade	Mensal	
Mecanismo de Cálculo (métrica)	NMA = 10 – PP Onde: NMA – Indicador de Avaliação Mensal. PP – Pontos Perdidos (de todas as OS/chamados do referido mês).	

	Para o cálculo dos Pontos Perdidos, leva-se em consideração: Quando da ocorrência de um incidente, este deverá ser classificado conforme o estabelecido na Tabela de Criticidade (Item 10.3.2.1 do Ter classificação: - Se o início de atendimento correspondente não for realizado dentro do prazo estabelecido, será considerada uma avaliação insatisfatória - 0,3 (zero-vírgula-três) pontos perdido na Nota de Avaliação Mensal, para cada avaliação insatisfatória. Quando do início de atendimento de um incidente, conforme o estabelecido na Tabela de Criticidade (Item 10.3.2.1 do Termo de Referênci Tabela: - Se a apresentação da Solução, não for realizada dentro do limite de tempo estabelecido, será considerada uma avaliação insatisfatória pa - 0,3 (zero-vírgula-três) pontos perdido na Nota de Avaliação Mensal, para cada avaliação insatisfatória, e mais 0,1 pontos perdido para cad para solução completa do incidente. Observação: Todas as variáveis serão consideradas com uma casa decimal.
Início de Vigência	Data da emissão da Ordem de Serviço.
Faixas de ajuste no pagamento e Sanções	Serão aplicados os seguintes ajustes/sanções, caso a meta do indicador NMA não seja atingida: Sempre que a NMA for maior ou igual a 9,0 e menor que 9,5 a Contratada receberá advertência. Sempre que a NMA for maior ou igual a 8,5 e menor que 8,9 a Contratada receberá glosa de 0,5% sobre o valor total do contrato Sempre que a NMA for maior ou igual a 8,0 e menor que 8,4 a Contratada receberá glosa de 2% sobre o valor total do contrato. Sempre que a NMA for menor ou igual a 7,9 a Contratada receberá glosa de 5% sobre o valor total do contrato. Sempre que a Contratada acumular duas advertências consecutivas, receberá multa de 5% sobre o valor total do contrato.

15. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (IN. 04/2014, Art. 25)

15.1. O critério da seleção do fornecedor será o de MENOR PREÇO, a ser obtido por intermédio de realização de pregão na forma eletrônica;

15.2. CARACTERIZAÇÃO DA SOLUÇÃO

15.2.1. A aquisição objeto, desta licitação, está enquadrada na classificação de bens comuns, em atendimento ao disposto no Decreto nº 5.450/05, pois seus padrões de desempenho e qualidade podem ser objetivamente definidos neste Termo de Referência e no Edital, por meio de especificações usuais do mercado.

15.3. SISTEMA DE REGISTRO DE PREÇOS

15.3.1. O Art. 3º do Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15º da Lei nº 8.666/93, preconiza que:
"Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:
I - Quando, pelas características do bem ou serviço, houver necessidade de contratações freqüentes;
II - Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
III - Quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
IV - Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração".
15.3.2. Em função das características peculiares desta contratação, entre as quais destaca-se: a necessidade de contratações frequentes conforme as demandas dos diversos órgãos que compõem a estrutura da CONTRATANTE, esta licitação será realizada pelo Sistema de Registro de Preços – SRP.

15.4. MODALIDADE DE LICITAÇÃO

15.4.1. A licitação para registro de preços será realizada na modalidade PREGÃO ELETRÔNICO, do tipo MENOR PREÇO GLOBAL, em sessão pública realizada por meio do sistema eletrônico, no Portal de Compras do Governo Federal - COMPRASNET, sítio www.comprasnet.gov.br.

15.5. CRITÉRIOS TÉCNICOS DE HABILITAÇÃO

15.5.1. Atestado (s) de capacidade técnica emitido em nome da licitante, expedido por pessoa(s) jurídica(s) de direito público ou privado, que comprove que a licitante presta ou prestou serviços semelhantes para o desempenho de atividade pertinente e compatível em características e prazos com o objeto do Termo de Referência, conforme § 3º do art. 30 da Lei no 8.666/93;

15.5.1.1. Atestado de Capacidade Técnica apresentados deverão conter, ainda, a comprovação de suporte técnico em regime de 8x5x365 (vinte e quatro horas por dia, sete dias da semana e trezentos e sessenta e cinco dias no ano).

15.5.2. O(s) Atestado(s) de Capacidade Técnica deverão ser emitidos em papel timbrado do emitente e conter: Razão Social, CNPJ e Endereço Completo da Empresa Emitente; Razão Social da Licitante; Número e vigência do contrato; Objeto do contrato; Descrição do serviço realizado; Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento dos serviços contratados; Local e Data de Emissão; Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico); Assinatura do responsável pela emissão do atestado;
15.5.3. Todas as cópias dos atestados serão arquivadas no processo;
15.5.4. A licitante deverá comprovar ainda na fase de habilitação, cópia da declaração em papel timbrado da empresa, assinadas por pessoa responsável com indicação de cargo exercido na empresa, com firma reconhecida em cartório competente e ainda documento que comprove que a pessoa que está assinando tenha poderes para isso, que:

15.5.4.1. Que o fabricante ou a empresa possui central telefônica "própria" para abertura de chamados técnicos através de ligação gratuita (0800), além de identificar na declaração o número telefônico 0800;
15.5.4.2. Que o fabricante possui site na Internet disponibilizando atualizações de segurança dos produtos além de drivers ou outros softwares necessários para o perfeito funcionamento do produto proposto, além de identificar na declaração o endereço da página de Internet onde estão disponibilizados tais recursos de atualização;

15.5.5. Caso a licitante não seja revenda autorizada e, visando assegurar a CONTRATANTE que durante o período de garantia estes manterão conformidade à sua configuração inicial, ela deverá comprovar as condições de garantia da seguinte forma:

15.5.5.1. Provando ser assistência técnica autorizada, através de declaração emitida pelo fabricante, para os softwares ofertados ou;
15.5.5.2. Apresentar contrato (s) com empresa (s) de assistência técnica autorizada pelo fabricante que satisfaça (m) as condições exigidas neste

termo de referência em termos de período de garantia, locais e níveis de serviço de atendimento às ocorrências. Todas as localidades possíveis para instalação dos software deverão estar cobertas pelo (s) contrato (s);
15.5.5.3. Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante já forneceu, satisfatoriamente, produtos compatíveis com o objeto da presente licitação, cuja entrega ocorreu dentro do prazo, contendo informações que permitam estabelecer, por proximidade de características técnicas e quantitativas, comparação entre o objeto deste Termo de Referência e aquele fornecido, não sendo aceito atestado emitido pela própria licitante.

15.5.6. Todas as declarações exigidas deverão ser apresentadas cópias emitidas em papel timbrado da empresa fabricante, assinadas por pessoa responsável com indicação de cargo da exercido na empresa, com firma reconhecida em cartório competente e ainda documento que comprove que a pessoa que está assinando tenha poderes para isso;

15.5.6.1. Será aceito o somatório de atestados e/ou certidões que perfaçam a totalidade de 50% do quantitativo estimado para cada item.
15.5.6.2. Caso não atinja 50%, será aceito um único atestado que contemple, ao menos, 30% do quantitativo estimado para a contratação de cada item. Nesse caso não será necessário o somatório de atestados.
15.5.6.3. Em substituição ao atestado de Capacidade Técnico-Operacional a licitante poderá ser o próprio fabricante ou apresentar carta de solidariedade dele.

15.5.7. Somente serão considerados válidos atestados com timbre da entidade expedidora e com identificação do nome completo;
15.5.8. O atestado deverá ser datado e assinado por pessoa física identificada pelo seu nome e cargo exercido na entidade, bem como dados para eventual contato, estando às informações sujeitas à conferência pelo pregoeiro;
15.5.9. Todos os certificados/carta de solidariedade deverão obrigatoriamente ser apresentados em original ou através de cópia autenticada por cartório competente, com exceção de certificados emitidos através da internet, nos quais deverá constar obrigatoriamente a URL do site de origem;
15.5.10. As ME/EPP, por ocasião da participação em certames licitatórios, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição;
15.5.11. A LICITANTE deverá apresentar declaração datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá de profissionais com nível superior e com as seguintes certificações ou equivalentes:

15.5.11.1. No mínimo 01 (Um) técnicos profissionais capacitados e certificados na linha de produtos proposta;
15.5.11.2. Caso o fabricante não possua certificação específica para a linha de produtos serão aceitos profissionais comprovadamente capacitados e aprovados em treinamento formal do fabricante.

16. PROPOSTA COMERCIAL DE PREÇO

16.1. A proposta deverá ser redigida em língua portuguesa, salvo expressões técnicas de uso corrente, datilografadas ou impressas por meio eletrônico, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas. Dela deverão constar obrigatoriamente, sob pena de desclassificação:

16.1.1. Identificação social, número do CNPJ, assinatura do representante da proponente, referência a esta licitação, número do telefone, endereço, indicação de endereço eletrônico (e-mail) e fac-símile;
16.1.2. Descrição clara do objeto, de acordo com as especificações deste Termo de Referência.

16.2. Anexar juntamente com a proposta, sob a forma de volumes impressos e/ou em meio eletrônico, a documentação que comprove o atendimento aos itens do Edital ou deste Termo de Referência. Deverá ser indicado o local da documentação que comprove o atendimento específico de cada um dos itens, sob pena de desclassificação da proposta.
16.3. Deverá ser fornecida pela LICITANTE, uma grade, com o número das páginas de sua proposta onde contém a comprovação do atendimento dos requisitos exigidos;
16.4. Apresentar na proposta a indicação detalhada da solução ofertada citando o módulo, descrição do módulo e fabricante;
16.5. Apresentar tabela de comprovação técnica, conforme modelo abaixo, deverá ser parte obrigatória da proposta comercial:

16.5.1. A LICITANTE deverá apresentar tabela preenchida, composta de todos os itens contidos neste termo de referência, incluindo apresentação de documentação com indicação da página, onde deve se encontrar grifadas as comprovações de cada uma das funcionalidades e características exigidas listadas no ANEXO - I deste Termo de Referência;
16.5.2. A Tabela de Comprovação Técnica deve conter, ainda, nome do documento comprobatório emitido pelo Fabricante;

Nº do Item	Descrição da Característica/Funcionalidade exigida	Documento do Fabricante (Nome)	Página	Atende ao Requisito (Sim/Não)

16.6. Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais;
16.7. Todos os documentos devem estar completos e legíveis;
16.8. Apresentar catálogo (s), folheto (s) ou manual (is) preferencialmente em português, com especificações técnicas detalhadas dos módulos que compõem a solução ofertada, para comprovação de características técnicas obrigatórias, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática;
16.9. Havendo divergência entre as características técnicas descritas na proposta da empresa e as disponibilizadas pelo fabricante (como informes técnicos, manual técnico, que acompanha o material, folders ou prospectos técnicos), prevalecerão os informes do fabricante, salvo os casos específicos em que a LICITANTE esclareça os motivos da divergência e que sejam aceitos pela CONTRATANTE;
16.10. Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela LICITANTE, no canto inferior direito;
16.11. Além da indicação da página da documentação fornecida onde se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser necessariamente grifada.
16.12. Informar os meios de comunicação (e-mail, número de telefone 0800, serviço de abertura de chamado via web, ou outro indicado pela licitante, desde que aceito pela CONTRATANTE) para abertura de chamados;
16.13. Informar o site do fabricante do software na Internet, onde se possa efetuar consultas;
16.14. A proposta deverá ser apresentada com os valores unitários e globais, conforme planilha constante no item 11 - Estimativa de preço da contratação.

17. PARCELAMENTO DO OBJETO (IN. 04/2014, Art. 14, §2º, inciso I)

17.1. A contratação da solução de segurança de informação e gestão em um LOTE único justifica-se pela necessidade de integração entre os módulos, possibilitando uma visão unificada, rápida e precisa quanto ao estado de segurança que se encontra o Órgão, sem a necessidade de nenhum custo adicional referente à normatização das informações, pois todos os produtos trabalham dentro de um mesmo padrão de informação;
17.2. O parcelamento do objeto poderia trazer dificuldades na leitura de um cenário de segurança, onde cada software, aplicativo e/ou solução, que não sejam integráveis, poderiam ter metodologias, termos e interpretações distintas quando ao mesmo incidente de segurança ou a continuidade dele, o que acarreta em um trabalho administrativo muito grande e difícil para extrair uma informação consistente da leitura de varias informações de segurança;
17.3. Indiretamente há que se imputar custos referentes à necessidade de ainda implementar um trabalho de normatização dos logs de segurança para que se possa possibilitar um panorama mais claro quanto ao nível de segurança atingido pelo Órgão.

18. PARTICIPAÇÃO DE CONSÓRCIO OU SUBCONTRATAÇÃO DA STI (IN. 04/2014, Art. 14, §2º, inciso II)

18.1. Não será admitida a subcontratação do objeto licitatório;
18.2. JUSTIFICATIVA: a vedação de consórcio e da subcontratação justifica-se pelo fato de que se trata da aquisição de software que são entregues pelo fabricante já prontos e montados (hardware e software), e que não necessita da intervenção ou complementação de outros atores, e que a instalação será efetuada

pela empresa CONTRATADA que entregará toda a solução em funcionamento, e que posteriormente deverá prestar a garantia de suporte e manutenção para a solução.

19. ALTERAÇÃO SUBJETIVA DA CONTRATADA

19.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

20. AVALIAÇÃO DA NECESSIDADE DE LICITAÇÕES E CONTRATAÇÕES SEPARADAS POR ITENS (IN. 04/2014, Art. 14, §3º)

20.1. A licitação para registro de preços será realizada na modalidade PREGÃO ELETRÔNICO, do tipo MENOR PREÇO GLOBAL, em sessão pública realizada por meio do sistema eletrônico, no Portal de Compras do Governo Federal - COMPRASNET, sítio www.comprasnet.gov.br.

21. DISCRIMINAÇÃO SEPARADA DOS ITENS QUE COMPÕEM O LOTE (IN. 04/2014, Art. 14, §4º)

21.1. Não haverá separação dos itens 1 e 2 do LOTE UNICO.

Descrição Técnica da Solução de Endepoint

1. Proteção de Estações de Trabalho, Servidores

1.1. Características Gerenciais

1.1.1. O software de proteção do endpoint deve ter a capacidade de implementar, no mínimo, as seguintes funcionalidade:

- Reputação de Arquivos sejam locais como no acesso web;
- IPS de Próxima Geração (Next Generation IPS);
- Proteção de Navegadores (Browser Protection);
- Aprendizado de Máquinas (Machine Learning);
- Análise Comportamental (Behavioral Analysis);
- Mitigação da Exploração de Memória (Memory Exploit Mitigation);
- Controle de Aplicações (Application Control);
- Controle de Dispositivos (Device Control);
- Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas (Exploit Mitigation).

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

- Exploração de navegadores com reputação de URL;
- Websites infectados com reputação de URL;
- Office Exploits com reputação de URL;
- Arquivos anexos com reputação de arquivos;
- Download de arquivos com reputação de arquivos;
- Execução do instalador de software com classificação comportamental do instalador (boa e ruim);
- Execução do malware de software com classificação comportamental do instalador (boa e ruim);
- A funcionalidade de “Machine Learning” deve trabalhar baseado no mínimo nas seguintes premissas:
- Atualização da base de reputação das URL’s com a periodicidade mínima de 2,5 horas;
- Bloqueio de URL’s de má reputação;
- Bloqueio das instruções de “Command & Control”;
- Atualização da base de reputação de Arquivos com a periodicidade mínima de 2,5 horas;
- Bloqueio das ameaças polimorfas mesmo que arquivos desconhecidos;
- Prevenção de Falso Positivos;
- Bloqueio de malwares desconhecidos e suas variantes;
- Implementar a classificação comportamental dos arquivos;
- “Aprendizado” a partir dos indicadores de compromisso (IoC).

1.1.3. A funcionalidade de “Machine Learning” deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:

- Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;
- Arquivos de softwares mundialmente espalhados na rede mundial de computadores;
- Sites Web mundialmente espalhados pela rede mundial de computadores.

1.1.4. O software de proteção dos endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:

- Adobe PDF;
- Flash;
- Java;
- Navegadores (Internet Explorer, Chorme e Firefox).

1.1.5. O software de proteção do endpoint deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:

- SEHOP - Structured Exception Handler Overwrite Protection;
- Heap Spray (Exploits que iniciam através do HEAP);
- Java Exploit Protection.

1.1.6. O software de proteção do endpoint deve ter a capacidade de bloquear exploits que trabalham em nível de “shell code”, assim como, implementar a funcionalidade de “virtual patching” para as aplicações;

1.1.7. O software de proteção do endpoint deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros, possibilitando no mínimo:

- Capturas de Login e Logout na Gerencia Central;
- Captura dos detalhes das máquinas protegidas;
- Captura dos detalhes de Domínios implementados pelo software;
- Captura dos detalhes de Grupos implementados pelo software;
- Captura da lista de “Fingerprint” de aplicações (Blacklisting);
- Captura da atualização da lista de “Fingerprint” de aplicações (Blacklisting);

- Captura dos detalhes das políticas aplicadas;
- Captura das atualizações dos detalhes das políticas aplicadas;
- Captura da lista dos usuários administradores da solução;
- Criação de novos administradores da solução;
- Capacidade de mover clientes de endpoints entre grupos lógicos.

1.1.8. O software de proteção do endpoint deve ter a capacidade de receber instruções de comando e ações diretamente do módulo de proteção contra ataques de APT (Advanced Persistent Threats), sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos;
1.1.9. A contratada deverá fornecer a licença de Banco de Dados necessária para o funcionamento da solução ofertada, sem limitação de capacidade.
1.1.10. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

1.2. Gerenciamento

1.2.1. Deve ter administração centralizada por console único de gerenciamento;
1.2.2. Deve ter acesso a console de gerenciamento via tecnologia Web (HTTP e HTTPS);
1.2.3. Deve estabelecer uma correlação de eventos entre os softwares gerenciados, possibilitando priorização nas ações tomadas.
1.2.4. Deve ser do mesmo fabricante do agente de proteção de endpoints.
1.2.5. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para maquinas físicas e virtuais através da mesma console;
1.2.6. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
1.2.7. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;
1.2.8. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;
1.2.9. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;
1.2.10. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008 R2 ou superior;
1.2.11. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 64 bits suportando ambiente virtual XEN, VMWARE e Microsoft;
1.2.12. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;
1.2.13. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;
1.2.14. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

- IP e range de IP;
- Endereço de Servidores de DNS, DHCP e WINS;
- Conexão com o servidor de gerência;
- Conexões de rede como VPN, Ethernet, Wireless e Modem.

1.2.15. Possibilidade de aplicar regras diferenciadas por grupos de usuários e maquinas;
1.2.16. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server 2016 ou superior;
1.2.17. O licenciamento do Microsoft SQL Server deverá ser no mínimo de 4 núcleos;
1.2.18. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;
1.2.19. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;
1.2.20. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);
1.2.21. Possibilidade de instalação dos clientes em servidores, estações de trabalho e maquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;
1.2.22. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;
1.2.23. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;
1.2.24. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;
1.2.25. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
1.2.26. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicos e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;
1.2.27. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada um dos subitens de acesso as configurações do cliente;
1.2.28. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;
1.2.29. Instalação e atualização do software sem a intervenção do usuário;
1.2.30. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;
1.2.31. Suportar redirecionamentos dos logs para um servidor de Syslog;
1.2.32. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado.
1.2.33. Deve gerenciar atualizações de software, políticas, logins, alertas e configurações por meio de um console centralizado;
1.2.34. Deve integrar-se com os drivers do Windows e em várias aplicações para garantir a estabilidade, atividade conjunta e segurança, não permitindo a utilização da abordagem de rootkit;
1.2.35. Deve possibilitar a verificação com base em agente permitindo execução simultânea em um número ilimitado de endpoints;
1.2.36. Deve permitir implementar as mesmas políticas para verificações com e sem agente;
1.2.37. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados;
1.2.38. Deve permitir gerar relatórios de progresso da verificação em tempo real;
1.2.39. Deve ter a capacidade de verificar e executar somente quando a máquina está inativa;
1.2.40. Ser capaz de descobrir qualquer dispositivo que possua um endereço IP atribuído (computador, servidor, impressora, roteador, switch, hub e outros) independente de fabricante ou fornecedor;
1.2.41. Ser capaz de descobrir dispositivos por meio do protocolo SNMP (Simple Network Management Protocol);
1.2.42. Permitir o descobrimento pelos métodos:

- Range de IP através de subnets e VLANs;
- Domínio.

1.2.43. Descobrimento de portas habilitadas (port scan);
1.2.44. Descobrimento de portas críticas, definidas pelo administrador, que estiverem habilitadas nos computadores;
1.2.45. Fornecer informações sobre as mudanças que ocorrem em todas as estações de trabalho e servidores;

1.3. Provisionamento de Imagens de Sistema Operacional

1.3.1. Capturar e distribuir imagens incluindo formato EXE universal para auto extração;
1.3.2. Permitir provisionar dinamicamente uma imagem, configurações e software para os computadores que se conectarem a rede usando regras por

MAC Address, tipo de Hardware, Rede Local, e outros dados;
1.3.3. Com a capacidade de transmitir pacotes de multicast, o cliente deve receber a imagem e depois enviar via multicast para o resto dos clientes sem exigir configuração em roteadores para permitir a transmissão de pacotes de multicast ou um servidor na sub rede;
1.3.4. A solução deve permitir o encaminhamento de PXE, para que um cliente seja eleito para trafegar PXE sem ter de adicionar ou reconfigurar o hardware, sem requerem um servidor PXE separado em cada sub rede ou roteadores configurados para transmitir o tráfego PXE;
1.3.5. Gerenciar o computador remotamente mesmo que não tenha PXE e acesso físico através de partição de boot embutido.

1.4. Atualização de Vacinas

1.4.1. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus mecanismo de verificação (Engine) dos clientes da rede;
1.4.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;
1.4.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;
1.4.4. Atualização remota e incremental da versão do software cliente instalado;
1.4.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la;
1.4.6. Atualização automática das assinaturas do servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;
1.4.7. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;
1.4.8. Um único e mesmo arquivo de vacina de Vírus para todas as plataformas Windows e versões do antivírus.

1.5. Quarentena

1.5.1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;
1.5.2. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;
1.5.3. Forma automática de envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. Recebimento utilizando o mesmo método e aplicação da vacina recém-criada nas estações infectadas;
1.5.4. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;
1.5.5. Rastreamento agendado contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;
1.5.6. Rastreamento remoto contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear.

1.6. Cliente Gerenciado

1.6.1. Deve ter a capacidade de compor de forma nativa com a solução de APT do mesmo fabricante, sem a necessidade da implementação de scripts, utilizando apenas configurações realizadas na console padrão do produto;
1.6.2. Suportar máquinas com arquitetura 32-bit e 64-bit;
1.6.3. Possuir certificação FIPS 140-2;
1.6.4. Possuir certificação Common Criteria (CC) EAL2+;
1.6.5. O fabricante deverá possuir certificação ICSA Labs no mínimo nas plataformas Windows XP, Windows Vista e Windows 7, Windows 8.
1.6.6. O cliente para instalação em estações de trabalho deverá possuir compatibilidade com no mínimo os sistemas operacionais:

- Windows 2008, 2008 R2;
- Windows 2012;
- Windows 7;
- Windows 8;
- Windows 10;

1.7. Módulo de proteção anti-malware para estações Linux

1.7.1. Distribuições homologadas pelo fabricante
1.7.2. Suse linux enterprise 10,11 e 12;
1.7.3. Red Hat Enterprise Linux 4.0, 5.0,6.0 e 7.0;
1.7.4. Centos 4.0, 5.0, 6.0 e 7.0
1.7.5. O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante
1.7.6. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;
1.7.7. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;
1.7.8. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits, e outros;
1.7.9. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;
1.7.10. 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;
1.7.11. 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;
1.7.12. 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;
1.7.13. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;
1.7.14. As mensagens exibidas aos usuários devem ser traduzidas para o português do brasil;
1.7.15. Possuir integração com a Console de Gerenciamento Central para envio de informações de ameaças;
1.7.16. O cliente para instalação em servidores deverá possuir compatibilidade com os sistemas operacionais:

- Windows 2008, 2008 R2;
- Windows Small Business Server 2011 (64-bit);
- Windows Server 2012, 2012 R2;
- Windows 7.

1.7.17. Possuir certificação FIPS 140-2;
1.7.18. Possuir certificação Common Criteria (CC) EAL2+;
1.7.19. O fabricante deverá possuir certificação NSS Labs no mínimo nas plataformas Windows XP, Windows Vista e Windows 7.
1.7.20. O fabricante deverá possuir certificação AV-Tests no mínimo nas plataformas Windows XP, Windows Vista e Windows 7;

1.8. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades

1.8.1. Suporte aos protocolos TCP, UDP e ICMP;
1.8.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;
1.8.3. Possuir proteção contra exploração de buffer overflow;

1.8.4. Possuir proteção contra-ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;
1.8.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;
1.8.6. Possibilidade de agendar a ativação da regra de Firewall;
1.8.7. Possibilidade de criar regras diferenciadas por aplicações;
1.8.8. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;
1.8.9. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;
1.8.10. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;
1.8.11. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
1.8.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;
1.8.13. Gerenciamento integrado a console de gerência da solução.

1.9. Módulo de proteção anti-malware para estações MAC-OS

1.9.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

- Mac os x Lion 10 7.5.8 64 bits;
- Mac os x 10.8 (Mountain Lion) em processadores 32 e 64 bits;
- Mac os x 10.9 Mavericks em processadores 32 e 64 bits;
- Mac os x 10.10 Yosemite em processadores 32 e 64 bits;
- Mac os 10.11 El Capitan em processadores 32 e 64 bits;
- Mac os 10.12 Sierra em processadores 32 e 64 bits;

1.9.2. Suporte ao apple remote desktop para instalação remota da solução;
1.9.3. Gerenciamento integrado à console de gerência central da solução
1.9.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
1.9.5. Permitir a verificação das ameaças em real time, manual e agendada;
1.9.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
1.9.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;
1.9.8. Permitir habilitar scan-cache para otimizar a performance;
1.9.9. Possuir a verificação de URL's maliciosas para agentes internos e externos da rede;
1.9.10. Possuir a funcionalidade de Certified Safe Software para verificar se um software é legitimo;
1.9.11. 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;
1.9.12. Deve possuir no mecanismo de autoproteção as seguintes proteções:
1.9.13. Autenticação de comandos ipc;
1.9.14. Proteção e verificação dos arquivos de assinatura;
1.9.15. Proteção dos processos do agente de segurança;
1.9.16. Proteção das chaves de registro do agente de segurança;
1.9.17. Proteção do diretório de instalação do agente de segurança.
1.9.18. Possuir certificação FIPS 140-2;
1.9.19. Possuir certificação Common Criteria (CC) EAL2+;
1.9.20. O fabricante deverá possuir certificação ICSA Labs

1.10. Funcionalidade de Antivírus e Anti-Spyware:

1.10.1. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
1.10.2. Proteção Anti-Spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;
1.10.3. As configurações do Anti-Spyware deverão ser realizadas através da mesma console de todos os itens da solução;
1.10.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);
1.10.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;
1.10.6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixo, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;
1.10.7. Permitir que verificação das ameaças da maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;
1.10.8. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;
1.10.9. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Thunderbird e POP3/SMTP;
1.10.10. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);
1.10.11. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;
1.10.12. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;
1.10.13. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e Microsoft, para no mínimo:

- Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;
- Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:
    - Proteção de Anti-vírus e Anti-Spyware;
    - Proteção de heurística e reputação de arquivos em tempo real (real-time);
    - Proteção de IPS de rede e "host";
    - Controle de dispositivos e aplicações;
- Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;
- Capacidade de verificar "templates" de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (template);.

1.10.14. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
1.10.15. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
1.10.16. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo às seguintes características:

- Origem confiável;
- Origem não confiável;
- Tempo de existência do arquivo na internet;
- Comportamento do arquivo;
- Quantidade mínima de usuários que baixaram o arquivo da internet.

1.10.17. Capacidade de implementar regras distintas por grupo (ex. Departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;
1.10.18. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possa ser reparado no cliente;
1.10.19. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;
1.10.20. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;
1.10.21. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados por ZIP, LHA e ARJ, tendo como abrangência até o 10º (décimo) nível de compactação;
1.10.22. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;
1.10.23. A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin, execução de arquivo ou módulo adicional;
1.10.24. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;
1.10.25. Gerenciamento integrado à console de gerência da solução;
1.10.26. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;
1.10.27. Capacidade de executar varreduras em tempo real (real-time) contra-ataques dirigidos à vulnerabilidades do navegador (browser);

1.11. Detecção Proativa de reconhecimento de novas ameaças

1.11.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;
1.11.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;
1.11.3. Capacidade de detecção keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
1.11.4. Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;
1.11.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;
1.11.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Pró-Ativa com a base de reputação do fabricante;
1.11.7. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
1.11.8. Possibilidade de agendar o escaneamento da detecção Pró-Ativa com periodicidade mínima por minuto e em todos os novos processos;

1.12. Funcionalidade de Controle de Dispositivos

1.12.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);
1.12.2. Controlar o uso de dispositivos com comunicação infravermelho, FireWire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;
1.12.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;
1.12.4. Gerenciamento integrado a console de gerência da solução;
1.12.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
1.12.6. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

1.13. Relatórios e Monitoramentos com as funcionalidades

1.13.1. Possuir, pelo menos, 25 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;
1.13.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
1.13.3. Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status (com vírus, desatualizada etc.);
1.13.4. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

- As 10 máquinas com maior ocorrência de códigos maliciosos;
- Os 10 usuários com maior ocorrência de códigos maliciosos;
- Localização dos códigos maliciosos;
- Sumários das ações realizadas;
- Número de infecções detectadas diário, semanal e mensal;
- Códigos maliciosos detectados.

1.14. Console avançada de distribuição e relatórios

1.14.1. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;
1.14.2. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;

1.14.3. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:

- CA;
- ESET;
- F-Secure;
- Kaspersky;
- McAfee;
- Sophos;
- Symantec;
- Trend Micro.

1.14.4. Permitir a remoção de outros softwares não desejados;
1.14.5. Criar tarefas de migração baseadas no resultado do inventário de antivírus;
1.14.6. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;
1.14.7. Possibilidade de recuperar instalação em clientes em caso de falha;
1.14.8. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;
1.14.9. Os seguintes cubos devem ser disponibilizados para criação de relatórios:

- Alertas;
- Clientes;

- Políticas;
- Rastreamento;

1.14.10. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança;
1.14.11. Exportar os relatórios criados nos formados xls, pdf e HTML.

1.15. Funcionalidades do Controle de Acesso à Rede

1.15.1. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

- Computador deve possuir antivírus, atualizados e ativo;
- Computador deve possuir firewall ativo;
- Computador deve possuir Anti-Spyware, atualizado e ativo;
- Computador deve possuir patches instalados, ativos e atualizados.

1.15.2. Deve ter a capacidade de iniciar à auto remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;
1.15.3. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso a rede;
1.15.4. A auto remediação deve suportar download de programas e arquivos por links de HTTP, FTP e UNC;
1.15.5. Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação;
1.15.6. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não utilizam o agente (Máquinas não gerenciadas);
1.15.7. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não estiverem em conformidade com as políticas do controle de acesso a rede;

1.16. Módulo para controle de aplicações

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

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
- Windows Server 2012 e Windows Server 2012 R2;
- Windows Server 2016;
- Windows XP sp3 (x86/x64);
- Windows XP sp2 (x64);
- Windows Embedded Xpe;
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows 7 (x86/x64);
- Windows Embedded POSReady 7;
- Windows Embedded Standard 7;
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64);

1.16.2. Permitir a criação de políticas de segurança personalizadas;
1.16.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:
1.16.4. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
1.16.5. Range de endereços IPS;
1.16.6. Sistema operacional;
1.16.7. Grupos de máquinas espelhados do Active Directory;
1.16.8. Usuários ou grupos do Active Directory;
1.16.9. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;
1.16.10. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:
1.16.11. Nenhum;
1.16.12. Somente bloqueios;
1.16.13. Somente regras específicas;
1.16.14. Todas as aplicações executadas;
1.16.15. As políticas de segurança devem permitir o controle do intervalo de envio dos logs;
1.16.16. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;
1.16.17. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;
1.16.18. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;
1.16.19. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;
1.16.20. As políticas de segurança devem permitir o controle através de regras de aplicação;
1.16.21. As regras de controle de aplicação devem permitir as seguintes ações:
1.16.22. Permissão de execução;
1.16.23. Bloqueio de execução;
1.16.24. Bloqueio de novas instalações;
1.16.25. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
1.16.26. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:
1.16.27. Assinatura sha-1 do executável;
1.16.28. Atributos do certificado utilizado para assinatura digital do executável;
1.16.29. Caminho lógico do executável;
1.16.30. Base de assinaturas de certificados digitais válidos e seguros;
1.16.31. As regras de controle de aplicação devem possuir categorias de aplicações;
1.16.32. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.
1.16.33. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
1.16.34. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;
1.16.35. 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;
1.16.36. Deve possuir a funcionalidade de instalação remota do agente usando a mesma comunicação do Antivírus;

1.17. Módulo de proteção contra vazamento de informações – DLP

1.17.1. A solução contra vazamento de dados deve ter a capacidade de verificação contra vazamento de informações sigilosas originadas a partir das soluções de edição de texto e correio eletrônico, ambos na nuvem (cloud);
1.17.2. Deve ter a capacidade de bloquear a captura de tela (print screen) integral, ou seja, mesmo que seja de uma janela NÃO ativa no momento da captura;
1.17.3. Deve ter a capacidade de inspecionar e bloquear o envio de dados sigilosos para ambientes de compartilhamento de diretórios virtuais na nuvem;

1.17.4. Deve ter a capacidade de monitorar e prevenir a transferência de dados sensíveis através de LanMan (LAN Manager) e RDP (Remote Desktop Protocol);

1.18. Console de Gerenciamento

1.18.1. Deve ter administração centralizada por console único de gerenciamento;
1.18.2. As configurações de todos os módulos de detecção e criação de relatórios deverão ser realizadas através da mesma console;
1.18.3. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS);
1.18.4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
1.18.5. Microsoft Windows 2003 Server;
1.18.6. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado;
1.18.7. Deve possuir integração com Active Directory, para autenticação de usuários da solução;
1.18.8. Deve ter a capacidade de realizar atualização de versão e patches nos componentes da solução através da própria console de gerenciamento;
1.18.9. Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação;
1.18.10. Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;
1.18.11. Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;
1.18.12. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;
1.18.13. Deve permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);
1.18.14. Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;
1.18.15. Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;
1.18.16. Deve possuir logs detalhados de auditoria de alterações de políticas;
1.18.17. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;

1.19. Resposta a Incidentes

1.19.1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política;
1.19.2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações;
1.19.3. Deve ser possível a notificar automaticamente o remetente e o gerente ou superior hierárquico do usuário envolvido no incidente;
1.19.4. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

- Bloqueio de mensagem;
- Quarentena de arquivo;
- Notificação ao usuário;
- Bloqueio do acesso web, bloqueio de cópia e impressão.

1.19.5. Deve disponibilizar interface de resposta totalmente personalizável que permita combinações de várias ações de reparo e reação, através do acionamento de um único botão na interface gráfica do Incidente;
1.19.6. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis;
1.19.7. Deve exibir todos os detalhes do incidente em uma única página;
1.19.8. Deve permitir destacar (highlight) na tela do incidente os dados confidenciais detectados;
1.19.9. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida (“preview”) na tela do incidente, sem a necessidade de usar software externo;
1.19.10. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente;
1.19.11. Deve possibilitar a exibição na tela do Incidente no console um link que possibilite o download e a abertura destes itens usando um software externo;
1.19.12. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente;
1.19.13. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema (incluindo políticas, relatórios, funções e workflow);
1.19.14. A solução deve possuir integrada a console a funcionalidade de workflow para tratamento e escalação dos incidentes;
1.19.15. Deve ser possível utilizar no workflow características, para no mínimo: severidade, status, filas de tratamento e atributos dos incidentes;
1.19.16. As informações detectadas nos incidentes devem ser possíveis de ser visualizadas através da console de gerenciamento;
1.19.17. Deve ser possível ocultar a visualização de evidencias de acordo com o nível de permissão atribuído ao operador da ferramenta;
1.19.18. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente, para no mínimo:

- Timestamp;
- Método de detecção;
- Remetente e destinatário;
- Mensagens e anexos;
- Protocolo e endereço IP.

1.19.19. Deve agregar diversos incidentes em um caso para investigação mais detalhada;
1.19.20. Deve possibilitar exportar incidentes para formato HTML, de forma que não exista necessidade de credenciais de acesso a solução para visualização off-line das informações;
1.19.21. Deve segregar acesso aos incidentes de acordo com características, para no mínimo:

- Unidade de negócio;
- País;
- Gerente do usuário envolvido;
- Severidade.

1.20. Relatórios

1.20.1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:

- Timestamp;
- Tamanho e data do arquivo;
- Endereço IP de origem e destino;
- Histórico de incidentes e detalhes;
- Remetente e destinatário.

1.20.2. Deve fornecer relatórios de tendências com gráficos distribuídos em uma linha de tempo;
1.20.3. Deve exportar relatórios para formato HTML e CSV;
1.20.4. Deve agendar relatórios para envio automático através de e-mail (datas específicas e periodicamente);
1.20.5. Deve apresentar um painel (“dashboard”) para visualização executiva dos relatórios;
1.20.6. Deve permitir gerar relatórios resumidos por níveis, agrupados, sumarizados e com capacidade de detalhamento (drill-down);
1.20.7. Deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP;
1.20.8. Deve ter a capacidade para configurar, salvar relatórios e painéis de visualização (“dashboards”) personalizados por usuário;
1.20.9. Deve possibilitar a execução de relatórios em todo o histórico de incidentes armazenados na base de dados, via console web e via API.

1.21. Monitoramento em Estações de Trabalho

1.21.1. O cliente para instalação em estações de trabalho deverá possuir compatibilidade, no mínimo, com os sistemas operacionais:

- Windows XP;
- Windows 2003;
- Windows Vista;
- Windows 7, em versões 32 e 64 bits;
- Citrix XenApp;
- Citrix XenServer.

1.21.2. Deve permitir a distribuição do agente através de ferramentas de terceiros, no mínimo:

- Microsoft System Center;
- IBM Tivoli;
- Symantec Altiris.

1.21.3. O agente deve possuir mecanismos para evitar que o usuário interrompa os serviços do agente;
1.21.4. Deve ter a capacidade de monitorar e bloquear tentativas de cópia de conteúdo confidencial para no mínimo os dispositivos:

- Drives USB;
- CD/DVD;
- Impressoras e fax.

1.21.5. Deve monitorar tentativas de cópia de conteúdo confidencial para o disco rígido;
1.21.6. Deve identificar a movimentação de fragmentos de informações confidenciais mesmo através de operações do tipo "copiar e colar" em tipos de documentos diferentes, para no mínimo:

- Arquivos de editores de texto *.doc e *.docx para e-mail;
- Arquivos de planilhas eletrônicas *.xls e *.xlsx para arquivos de apresentações *.ppt e *.pptx.

1.21.7. Atualizações dos agentes devem ser enviadas diretamente pela console de gerenciamento;
1.21.8. Deve exibir alerta "pop-up" na tela do usuário em caso de violação de política;
1.21.9. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta, reportando para a console de gerenciamento, categorizadas no console para posterior geração de relatórios por categoria de justificativa;
1.21.10. Deve, para um grupo pré-determinado de usuários ("VIPs"), permitir o envio de informação confidencial, apresentando um “pop-up” de alerta quanto da criticidade da informação e solicitando confirma da ação, a qual deve ser logada na console central;
1.21.11. Todas as políticas devem estar ativas mesmo se a estação estiver fora da rede;
1.21.12. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial;
1.21.13. Deve permitir monitorar e bloquear transmissão HTTP;
1.21.14. Deve permitir monitorar e bloquear transmissão HTTPS, integrando-se a, no mínimo com os browsers;

- Internet Explorer;
- Mozilla Firefox;
- Google Chrome.

1.21.15. Deve permitir monitorar e bloquear e-mails, integrando-se via plug-in ao cliente, no mínimo:

- Microsoft Outlook;
- Lotus Notes.

1.21.16. Deve permitir monitorar e bloquear transmissão FTP;
1.21.17. Deve permitir monitorar e bloquear dados enviados a um fax local e de rede;
1.21.18. Deve executar todas as funções através de um único agente, inclusive a verificação do endpoint e a monitoração e bloqueio de dados que saem do endpoint;
1.21.19. Deve permitir definir limites em % da CPU, disco, e a largura de banda utilizada pelo agente;
1.21.20. Deve gerenciar atualizações de software, políticas, logins, alertas e configurações por meio de um console centralizado;
1.21.21. Deve integrar-se com os drivers do Windows e em várias aplicações para garantir a estabilidade, atividade conjunta e segurança, não permitindo a utilização da abordagem de rootkit;
1.21.22. Deve possibilitar a verificação com base em agente permitindo execução simultânea em um número ilimitado de endpoints;
1.21.23. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados;
1.21.24. Deve permitir gerar relatórios de progresso da verificação em tempo real;
1.21.25. Deve ter a capacidade de verificar e executar somente quando a máquina está inativa.

2. Operação Assistida

2.1. As horas de Operação Assistida serão utilizadas sob demanda, a critério do órgão, para realização de atividades relacionadas à solução de segurança, tais como, mas sem se limitar a:

- Procedimentos em conjunto com o fabricante da solução, para situações em que o site do órgão esteja com previsão e/ou sofrendo ataque, destinado a prover o conhecimento para as medidas necessárias à defesa do ambiente;
- Procedimentos de ajuste para manter a solução adquirida pelo órgão provendo a melhor utilização de suas funcionalidades;
- Reuniões técnicas, mensais ou a critério do órgão, para planejamento e execução de serviços com vistas à melhoria do ambiente instalado;
- Reuniões gerenciais, mensais ou a critério do órgão, para avaliação e acompanhamento dos serviços oferecidos;

2.2. Sempre que necessário, o fornecedor deverá efetuar vistoria técnica nas dependências do órgão de modo a realizar análise e implementar as alterações necessárias;
2.3. O serviço de operação assistida deverá ser prestado de forma presencial no endereço local do órgão ou outro indicado por ele;
2.4. Para atendimento ao serviço de operação assistida, o fornecedor somente poderá empregar profissionais capacitados e certificados nos produtos fornecidos;
2.5. As horas efetivamente utilizadas nos procedimentos executados serão computadas de acordo com os dias e horários de entrada e saída do responsável do fornecedor às dependências do órgão;
2.6. Este serviço deve estar disponível para acionamento no sistema 8 horas por dia x 5 dias por semana.

Documento assinado eletronicamente por **Vitor de Oliveira Campos**, **Coordenador(a)**, em 09/11/2017, às 13:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luís Fernando Faina**, **Diretor(a)**, em 09/11/2017, às 13:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.