CONTRATO Nº 021/2018

CONTRATO DE FORNECIMENTO QUE ENTRE SI FAZEM, DE UM LADO, COMO CONTRATANTE, A AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB, E DE OUTRO LADO, COMO CONTRATADA, A EMPRESA CORE SERVIÇOS E INFORMÁTICA EIRELI – ME, EM CONFORMIDADE COM O PROCESSO Nº 2017.01031.006807-53 – SEI 201700031000181.

Por este instrumento particular, as partes abaixo mencionadas e qualificadas, acordam entre si firmar o presente Contrato de fornecimento, conforme as cláusulas e condições a seguir elencadas:

1 – Qualificação das Partes

AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB** , sociedade de economia mista, portadora do CNPJ nº 01.274.240/0001-47, com sede na Rua 18-A nº 541, Setor Aeroporto, Goiânia – GO, neste ato representada por seu Presidente **Cleomar Dutra Ferreira**, brasileiro, casado, portador da Carteira de Identidade nº 1716672 – SSP GO, e do CPF nº 349.423.431-00, residente e domiciliado em Anápolis – Go, por seu Diretor Administrativo **Joel Gomes Ribeiro**, brasileiro, casado, portador da Carteira de Identidade nº 224015 – 2ª via – DGPC – GO e do CPF nº 067.834.301-20, residente e domiciliado em Anápolis e por seu Diretor Financeiro **Amauri Batista Regis**, brasileiro, casado, portador da Carteira de Identidade nº M 1.464.004- MG e do CPF nº 326.720.476-34, residente e domiciliado em Aparecida de Goiânia - GO, doravante designada simplesmente **CONTRATANTE.

***CORE SERVIÇOS E INFORMÁTICA EIRELI – ME,** pessoa jurídica de direito privado, situada na Rua 105-D, nº 104, Setor Sul, Goiânia – Goiás, inscrita no CNPJ sob o nº 11.527.773/0001-47, neste ato representada por **Francisco Hilário Colino de Magalhães,** brasileiro, casado, portador da Cédula de Identidade nº 2775099 SSP/PA e do CPF nº 251.260.752-68, residente e domiciliado nesta capital, doravante designada simplesmente **CONTRATADA**.*

DO FUNDAMENTO LEGAL

Este contrato decorre da licitação realizada na modalidade Pregão Eletrônico nº 007/2018, de acordo com a Lei Federal nº 10.520, de 17 de julho de 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto Estadual nº 7.468, de 20 de outubro de 2011, Decreto Estadual nº 7.466 de 18 de outubro de 2011, Lei Estadual nº 17.928/2012, Lei Complementar 117/2015, aplicando-se subsidiariamente, no que couberem, as disposições da Lei Federal nº 8.666, de 23 de junho de 1993, e demais normas regulamentares aplicáveis à espécie, conforme termo de Homologação e processo administrativo nº 2017.01031.006807-53, regendo-o no que for omisso.

CLÁUSULA PRIMEIRA – DO OBJETO E SUA DESCRIÇÃO

1.1. O presente contrato tem por finalidade o fornecimento de solução de proteção Endpoint (Antivírus), serviço de implantação e treinamento visando atender as necessidades da AGEHAB, conforme descrições contidas no Termo de Referência e Proposta da Contratada,

conforme quadro abaixo:

ITEM 01	Licenciamento, manutenção e suporte de Solução de Proteção ENDPOINT (ANTIVIRUS) - por 36 meses
ITEM 02	Instalação de Solução de Proteção ENDPOINT (ANTIVIRUS)
ITEM 03	Treinamento de Solução de Proteção ENDPOINT (ANTIVIRUS)

1.2. Todas as funcionalidades solicitadas deverão ser atendidas por uma única solução/produto, não sendo aceitas composições de soluções;

1.3. As Licenças deverão ser fornecidas através de Download;

1.4. Os preços cotados do objeto da presente licitação deverão ser expressos em moeda corrente nacional, neles inclusos os acréscimos e despesas, como impostos, sem inclusão de qualquer encargo financeiro ou previsão inflacionária, sem que sofra correção ou reajuste durante o período de execução;

1.5. A solução ofertada após a assinatura do contrato, deverá ser a versão mais atual das ferramentas descritas no Termo de Referência;

1.6. SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA (COMPATIBILIDADE)
1.6.1. Microsoft Windows Server 2008 x64 e R2;
1.6.2. Microsoft Windows Small Business Server 2008 (Todas edições);
1.6.3. Microsoft Windows Server 2012 e R2 (Todas edições);
1.6.4. Microsoft Windows Server 2016 R2 (Todas edições);
1.6.5. Microsoft Windows XP Professional SP3 ou superior;
1.6.6. Microsoft Windows XP Professional x64 SP2 ou superior;
1.6.7. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
1.6.8. Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;
1.6.9. Microsoft Windows 7 Professional / Enterprise / Ultimate;
1.6.10. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
1.6.11. Microsoft Windows 8 Professional / Enterprise;
1.6.12. Microsoft Windows 8 Professional / Enterprise x64;
1.6.13. Microsoft Windows 8.1 Professional / Enterprise;
1.6.14. Microsoft Windows 8.1 Professional / Enterprise x64;
1.6.15. Microsoft Windows 10 Professional / Enterprise x64.

1.7. SUPORTA AS SEGUINTES PLATAFORMAS VIRTUAIS:
1.7.1. VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0 e superior;
1.7.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2 e 2016;
1.7.3. Oracle VM VirtualBox 4.0.4 e Superior (Somente logon como convidado);
1.7.4. Citrix XenServer 6.0 e Superior.

1.8. CARACTERÍSTICAS:
1.8.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.8.2. Console deve ser baseada no modelo cliente/servidor;
1.8.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.8.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

1.8.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
1.8.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.8.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.8.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.8.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.8.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.8.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.8.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
1.8.13. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
1.8.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.8.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
1.8.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
1.8.17. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
1.8.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença econfigurações do produto;
1.8.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.8.20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
1.8.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.8.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.8.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou ENDPOINT instalado utilizando os seguintes parâmetros:

- **1.8.23.1.** Nome do computador;
- **1.8.23.2.** Nome do domínio;
- **1.8.23.3.** Range de IP;
- **1.8.23.4.** Sistema Operacional;
- **1.8.23.5.** Máquina virtual.

1.8.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.8.25. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
1.8.26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.8.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
1.8.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
1.8.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos X dias, etc.;
1.8.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
1.8.31. Deve fornecer as seguintes informações dos computadores:
1.8.31.1. Deve fornecer as seguintes informações dos computadores:
a) Se o antivírus está instalado;
b) Se o antivírus está iniciado;
c) Se o antivírus está atualizado;
d) Minutos/horas desde a última conexão da máquina com o servidor administrativo;
e) Minutos/horas desde a última atualização de vacinas;
f) Data e horário da última verificação executada na máquina;
g) Versão do antivírus instalado na máquina;
h) Se é necessário reiniciar o computador para aplicar mudanças;
i) Data e horário de quando a máquina foi ligada;
j) Quantidade de vírus encontrados (contador) na máquina;
k) Nome do computador;
l) Domínio ou grupo de trabalho do computador;
m) Data e horário da última atualização de vacinas;
n) Sistema operacional com Service Pack;
o) Quantidade de processadores;
p) Quantidade de memória RAM;
q) Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory);
r) Endereço IP;
s) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
t) Atualizações do Windows Updates instaladas;
v) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
w) Vulnerabilidades de aplicativos instalados na máquina.
1.8.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.8.33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.8.33.1. Alteração de Gateway Padrão;
1.8.33.2. Alteração de subrede;
1.8.33.3. Alteração de domínio;
1.8.33.4. Alteração de servidor DHCP;
1.8.33.5. Alteração de servidor DNS;
1.8.33.6. Alteração de servidor WINS;

1.8.33.7. Alteração de subrede;
1.8.33.8. Resolução de Nome;
1.8.33.9. Disponibilidade de endereço de conexão SSL.
1.8.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.8.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.8.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.8.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.8.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.8.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.8.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.8.41. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.8.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.8.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.8.44. Deve possuir compatibilidade com Cisco Network AdmissionControl (NAC);
1.8.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);
1.8.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
1.8.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.8.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.8.49. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
1.8.49.1. Nome do vírus;
1.8.49.2. Nome do arquivo infectado;
1.8.49.3. Data e hora da detecção;
1.8.49.4. Nome da máquina ou endereço IP;
1.8.49.5. Ação realizada.
1.8.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.8.51. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.8.52. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.8.53. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

1.9. ESTAÇÕES WINDOWS – COMPATIBILIDADE:
1.9.1. Microsoft Windows Embedded 8.0 Standard x64;
1.9.2. Microsoft Windows Embedded 8.1 Industry Pro x64;
1.9.3. Microsoft Windows Embedded Standard 7 x86 / x64 SP1;
1.9.4. Microsoft Windows XP Professional x86 SP3 e superior;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

1.9.5. Microsoft Windows Vista x86 / x64SP2 e posterior;
1.9.6. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
1.9.7. Microsoft Windows 8 Professional/Enterprise x86 / x64;
1.9.8. Microsoft Windows 8.1 Pro / Enterprise x86 / x64 (Todas as Versões);
1.9.9. Microsoft Windows 10 Pro / Enterprise x86 / x64 (Todas as Versões).

1.10. CARACTERÍSTICAS:

1.10.1. Deve prover as seguintes proteções:

1.10.1.1. Deve prover as seguintes proteções:

* Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

* Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

* Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

* Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, MSN, por exemplo);

* O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

* Firewall com IDS;

* Autoproteção (contra-ataques aos serviços/processos do antivírus);

* Controle de dispositivos externos;

* Controle de acesso a sites por categoria;

* Controle de acesso a sites por horário;

* Controle de acesso a sites por usuários;

* Controle de execução de aplicativos;

* Controle de vulnerabilidades do Windows e dos aplicativos instalados;

* Controle de vulnerabilidades do Windows e dos aplicativos instalados;

* Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

* As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários em no máximo, 02 (duas) em 02 (duas) horas independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

* Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

* Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

* Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

* Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

* Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

* Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

* Capacidade de verificar somente arquivos novos e alterados;

* Capacidade de verificar objetos usando heurística;

* Capacidade de agendar uma pausa na verificação;

* Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

* Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

* O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou bloquear acesso ao objeto.

* Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

* Caso positivo de desinfecção: Restaurar o objeto para uso;

* Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

* Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

* Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

* Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

* Capacidade de verificar links inseridos em e-mails contra phishings;

* Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome, Opera, etc.;

* Capacidade de verificação de corpo e anexos de e-mails usando heurística;

* O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou bloquear o e-mail.

* Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

* Caso positivo de desinfecção: Restaurar o e-mail para o usuário;

* Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

* Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

* Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

* Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

* Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

* Deve ter suporte total ao protocolo IPv6;

* Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

* Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

a) Perguntar o que fazer, ou bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

b) Permitir acesso ao objeto.

* O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

a) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em temporeal, ou;

b) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

* Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

* Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

* Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

1.10.1.2. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

1.10.1.3. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-PhishingWorkingGroup (http://www.antiphishing.org/);

1.10.1.4. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

1.10.1.5. Deve possuir módulo IDS (IntrusionDetection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

1.10.1.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

* Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

* Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, coma possibilidade de escolher quais portas e protocolos poderão ser utilizados.

1.10.1.7. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

* Discos de armazenamento locais;
* Armazenamento removível;
* Impressoras;
* CD/DVD;
* Drives de disquete;
* Modems;
* Dispositivos de fita;
* Dispositivos multifuncionais;
* Leitores de smartcard;
* Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
* Wi-Fi;
* Adaptadores de rede externos;
* Dispositivos MP3 ou smartphones;
* Dispositivos Bluetooth;
* Câmeras e Scanners.

1.10.1.8. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

1.10.1.9. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

1.10.1.10. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

1.10.1.11. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

1.10.1.12. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

1.10.1.13. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.);

1.10.1.14. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

1.10.1.15. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

1.10.1.16. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

1.10.1.17. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

1.11. ESTAÇÕES MAC OS X - COMPATIBILIDADE:

1.11.1. Mac OS X 10.11 (El Capitan);
1.11.2. Mac OS X 10.10 (Yosemite);
1.11.3. Mac OS X 10.9 (Mavericks);
1.11.4. Mac OS X 10.8 (Mountain Lion);
1.11.5. Mac OS X 10.7 (Lion).

1.12. CARACTERÍSTICAS:

1.12.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
1.12.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.12.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
1.12.4. Deve possuir suportes a notificações utilizando o Growl;
1.12.5. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.12.6. Capacidade de voltar para a base de dados de vacina anterior;
1.12.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
1.12.8. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.12.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.12.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.12.11. Capacidade de verificar somente arquivos novos e alterados;
1.12.12. Capacidade de verificar objetos usando heurística;
1.12.13. Capacidade de agendar uma pausa na verificação;

1.12.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

1.12.14.1. Perguntar o que fazer, ou bloquear acesso ao objeto;

1.12.15. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador):

1.12.15.1. Caso positivo de desinfecção: Restaurar o objeto para uso;

1.12.15.2. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

1.12.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

1.12.17. Capacidade de verificar arquivos de formato de email;

1.12.18. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

1.12.19. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

1.13. ESTAÇÕES DE TRABALHO LINUX - COMPATIBILIDADE (PLATAFORMA 32 E 64 BITS):

1.13.1. Red Hat Enterprise Linux 6.2 Desktop e Superiores;

1.13.2. Fedora 16 e Superiores;

1.13.3. CentOS-6.2 e Superiores;

1.13.4. SUSE Linux Enterprise Desktop 10 SP4 e Superiores;

1.13.5. OpenSUSE Linux 12.2 e Superiores;

1.13.6. Debian GNU/Linux 6.0.5 e Superiores;

1.13.7. Mandriva Linux 2011 e Superiores;

1.13.8. Ubuntu 10.04 LTS e Superiores;

1.13.9. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

1.13.9.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

1.13.9.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

1.13.9.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

b) Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

c) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

d) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

1.13.9.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

1.13.9.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

1.13.9.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.13.9.7. Capacidade de verificar objetos usando heurística;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

1.13.9.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

1.13.9.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

1.13.9.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux.

1.14. SERVIDORES WINDOWS

1.14.1. COMPATIBILIDADE COM PLATAFORMA 32-BITS:

1.14.1.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.1.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

1.14.2. COMPATIBILIDADE COM PLATAFORMA 64-BITS:

1.14.2.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.5. Microsoft Windows Storage Server 2008 R2;

1.14.2.6. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);

1.14.2.7. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

1.14.2.8. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

1.14.2.9. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

1.14.2.10. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

1.14.2.11. Microsoft Windows Storage Server 2012 (Todas edições);

1.14.2.12. Microsoft Windows Storage Server 2012 R2 (Todas edições);

1.14.2.13. Microsoft Windows Storage Server 2016 (Todas edições);

1.14.2.14. Microsoft Windows Hyper-V Server 2012;

1.14.2.15. Microsoft Windows Hyper-V Server 2012 R2;

1.14.2.16. Microsoft Windows Hyper-V Server 2016.

1.15. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

1.15.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

1.15.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

1.15.3. Firewall com IDS;

1.15.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

1.15.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

1.15.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

1.15.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

b) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
c) Leitura de configurações;
d) Modificação de configurações;
e) Gerenciamento de Backup e Quarentena;
f) Visualização de relatórios;
g) Gerenciamento de relatórios;
h) Gerenciamento de chaves de licença;
i) Gerenciamento de permissões (adicionar/excluir permissões acima);

1.15.8. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

1.15.9. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

1.15.10. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

1.15.11. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

1.15.12. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);

1.15.13. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

1.15.14. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

1.15.15. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

1.15.16. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

1.15.17. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

1.15.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

1.15.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

1.15.20. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

1.15.21. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.15.22. Capacidade de verificar somente arquivos novos e alterados;

1.15.23. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

1.15.24. Capacidade de verificar objetos usando heurística;

1.15.25. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

1.15.26. Capacidade de agendar uma pausa na verificação;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

1.15.27. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
1.15.28 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
a) Perguntar o que fazer, ou boquear acesso ao objeto;
1.15.29. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.15.30. Caso positivo de desinfecção: Restaurar o objeto para uso;
1.15.31. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
1.15.32. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.15.33. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
1.15.34. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
1.15.35. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

1.16. SERVIDORES LINUX
1.16.1. COMPATIBILIDADE PLATAFORMA 64-BITS:
a) Red Hat Enterprise Linux Server 7 e Superiores;
b) CentOS-7.0 e Superiores;
c) SUSE Linux Enterprise Server 12 e Superiores;
d) Novell Open Enterprise Server 11 SP2 e Superiores;
e) Ubuntu Server 14.04 LTS e Superiores;
f) Ubuntu Server 14.10 e Superiores;
g) Oracle Linux 6.5 e Superiores;
h) Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores;
i) openSUSE® 13.1 e Superiores.

1.16.2. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:
a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
c) Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
* Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
* Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
* Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
* Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
* Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
* Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

* Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

* Capacidade de verificar objetos usando heurística;

* Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

* Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

* Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

1.17. SMARTPHONES E TABLETS – COMPATIBILIDADE

1.17.1. Apple iOS 7.0 – 8.X;

1.17.2. Windows Phone 8.1;

1.17.3. Android OS 2.3 – 5.1;

1.17.4. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

a) Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

* Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

b) Deverá isolar em área de quarentena os arquivos infectados;

c) Deverá atualizar as bases de vacinas de modo agendado;

d) Deverá bloquear spams de SMS através de Black lists;

e) Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

f) Capacidade de desativar por política: Wi-fi, Câmera, Bluetooth;

g) Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

h) Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

i) Deverá ter firewall pessoal (Android);

j) Capacidade de tirar fotos quando a senha for inserida incorretamente;

k) Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

l) Capacidade de enviar comandos remotamente de:

* Localizar;

* Bloquear;

m) Capacidade de detectar Jailbreak em dispositivos iOS;

n) Capacidade de bloquear o acesso a site por categoria em dispositivos;

o) Capacidade de bloquear o acesso a sites phishing ou malicioso;

p) Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

q) Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

r) Capacidade de configurar White e blacklist de aplicativos;

s) Capacidade de localizar o dispositivo quando necessário;

t) Permitir atualização das definições quando estiver em "roaming";

u) Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

v) Capacidade de enviar URL de instalação por e-mail;

w) Capacidade de fazer a instalação através de um link QRCode;

x) Capacidade de executar as seguintes ações caso a desinfecção falhe:

* Deletar;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

* Ignorar;
* Quarentenar;
* Perguntar ao usuário.

1.18. GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) - COMPATIBILIDADE:

1.18.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:

a) Apple iOS;
b) Windows Phone;
c) Android;
d) Dispositivos com suporte ao Apple PushNotification (APNs);
e) Apple iOS 3.0 ou superior.

1.18.2. CARACTERÍSTICAS:

a) Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

b) Capacidade de ajustar as configurações de:
* Sincronização de e-mail;
* Uso de aplicativos;
* Senha do usuário;
* Criptografia de dados;
* Conexão de mídia removível.
* Capacidade de instalar certificados digitais em dispositivos móveis;
* Capacidade de, remotamente, resetar a senha de dispositivos iOS;
* Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
* Capacidade de, remotamente, bloquear um dispositivo iOS.

1.19. CRIPTOGRAFIA - COMPATIBILIDADE:

1.19.1. Microsoft Windows Vista Business/Enterprise/ultimate sp2;
1.19.2. Microsoft Windows Vista Business/Enterprise/ultimate x64 sp2;
1.19.3. Microsoft Windows 7 Professional/Enterprise/ultimate;
1.19.4. Microsoft Windows 7 Professional/Enterprise/ultimate x64;
1.19.5. Microsoft Windows 8 Professional/Enterprise;
1.19.6. Microsoft Windows 8 Professional/Enterprise x64;
1.19.7. Microsoft Windows 8.1 Professional / Enterprise;
1.19.8. Microsoft Windows 8.1 Professional / Enterprise x64;
1.19.9. Microsoft Windows 10 Pro x86 / x64;
1.19.10. Microsoft Windows 10 Enterprise x86 /x64.

1.20. CARACTERÍSTICAS:

1.20.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
1.20.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.20.3. Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.20.4. Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot;
1.20.5. Permitir criar vários usuários de autenticação pré-boot;
1.20.6. Deve ter a capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.20.7. Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

* Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

* Criptografar todos os arquivos individualmente;

* Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

* Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.20.8. Deve ter a capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

1.20.9. Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

1.20.10. Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

1.20.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

1.20.12. Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia;

1.20.13. Bloquear o reuso de senhas;

1.20.14. Bloquear a senha após um número de tentativas pré-estabelecidas;

1.20.15. Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

1.20.16. Permitir criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo;

1.20.17. Permitir criptografar as seguintes pastas pré-definidas: "meus documentos", "favoritos", "desktop", "arquivos temporários" e "arquivos do outlook";

1.20.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;

1.20.19. Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.;

1.20.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;

1.20.21. Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações;

1.20.22. Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento.

1.21. Gerenciamento de Sistemas

1.21.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

1.21.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

1.21.3. Capacidade de gerenciar licenças de softwares de terceiros;

1.21.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

1.21.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;

1.21.6. Possibilita fazer distribuição de software de forma manual e agendada;

1.21.7. Suporta modo de instalação silenciosa;

1.21.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

1.21.9. Possibilita fazer a distribuição através de agentes de atualização;

1.21.10. Utiliza tecnologia multicast para evitar tráfego na rede;

1.21.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

1.21.12. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no c;
1.21.13. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.21.14. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.21.15. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.21.16. Permite baixar atualizações para o computador sem efetuar a instalação;
1.21.17. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atua;
1.21.18. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.21.19. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.21.20. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

CLÁUSULA SEGUNDA – DA GARANTIA

2.1. GARANTIA TÉCNICA

2.1.1. Os objetos deverão possuir garantia técnica mínima de 36 meses, sob a responsabilidade do fornecedor. O fornecedor deverá disponibilizar assistência técnica no período da garantia técnica.

2.2. ASSISTÊNCIA TÉCNICA

2.2.1. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses.

2.2.2. A CONTRATADA deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico, acesso remoto, e-mail ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise (Zero-day).

2.2.3. Os prazos relativos aos chamados deverão obedecer ao seguinte nível mínimo de serviço: 8 x 5 (oito horas por dia, cinco dias por semana em dias úteis e no horário comercial).

2.3. O SERVIÇO DE SUPORTE TÉCNICO GARANTE:

2.3.1. Reinstalação, reconfiguração, e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados.

2.3.2. O direito de receber toda e qualquer atualização de todos os softwares ou patches corretivos de componentes adquiridas após a assinatura do contrato, para a versão mais atual das ferramentas.

2.3.3. A CONTRATADA deverá prestar atendimento técnico em regime de garantia.

CLÁUSULA TERCEIRA – DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

3.1. Todas as licenças deverão ser registradas em nome do Agência Goiana de Habitação S/A, CNPJ: 01.274.240/0001-47, tendo como sede a localização na Rua 18 A nº 541 – Setor Aeroporto – Goiânia-GO, CEP: 74.070-060.

3.2. A data para efetivo início da execução dos serviços não poderá exceder 15 (quinze) dias depois da publicação do Contrato.

3.3. A entrega será feita de forma única contemplando Licenciamento dos objetos e Entrega da Documentação.

3.4. Os equipamentos deverão ser entregues em até 30 (trinta) dias a contar da publicação do contrato ou instrumento equivalente, à sede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060.

3.5. O prazo máximo para entrega do serviço, incluindo licenciamento, instalação, treinamento e Entrega da Documentação, será de no máximo 30 (trinta) dias, contados a partir da data de publicação do contrato.

CLÁUSULA QUARTA – DA EXECUÇÃO

4.1. Licenciamento e Instalação da solução:

4.1.1. A instalação e configuração deve ser implementada On-site conforme cenário fornecido pela Agência Goiana de Habitação S/A após a emissão e recebimento da assinatura do contrato.

4.1.2. A empresa CONTRATADA deverá realizar toda a instalação da solução adquirida e quaisquer outras providências que tenham relação direta com a instalação do serviço em questão.

4.1.3. Criar senha de acesso com privilégio administrativo para a AGEHAB.

4.1.4. Após a assinatura do contrato, a CONTRATADA deverá apresentar, no prazo máximo de 10 (dez) dias, os requisitos de infraestrutura para instalação da solução, o Plano de instalação, testes e ativação incluindo o Cronograma Detalhado de Execução dos Serviços, prevendo as datas de início e término da instalação de todos os licenciamentos.

4.1.5. O Cronograma da CONTRATADA deverá ser submetido à Gerência de Tecnologia da Informação (GETI) da AGEHAB, observado o respectivo serviço e somente será válido após aprovação. Depois de validado, a Contratada será notificada para dar início à execução do cronograma aprovado pela GETI - AGEHAB.

4.1.6. O fornecedor deverá entregar a solução instalada e customizada de acordo com os padrões fornecidos pela equipe técnica da Gerência de Tecnologia da Informação (GETI).

4.2. TREINAMENTO (REPASSE TECNOLÓGICO)

4.2.1. O treinamento abordará no mínimo: o uso da ferramenta, instalação, configuração, backup e restauração de configuração, gerenciamento, resolução de problemas e procedimentos de isolamento de rede em caso de infecção.

4.2.2. O treinamento deverá contemplar todos os recursos e configurações existentes na solução ofertada.

4.2.3. A AGEHAB se encarregará de disponibilizar as instalações físicas para a realização do treinamento, tais como: projetores, tela para apresentação, computador, mesas e poltronas.

4.2.4. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização dos treinamentos, além de impressos e quaisquer outras despesas diretas ou indiretas.

4.2.5. O treinamento será com uma turma de até 05 (cinco) alunos e o treinamento será realizado nas dependências da AGÊNCIA GOIANA DE HABITAÇÃO S/A, que irá ceder uma sala para sua realização.

4.2.6. O treinamento deverá ser organizado em módulos e suas ementas e conteúdos programáticos devem ser previamente disponibilizados a AGEHAB para aprovação.

4.2.7. O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso.

4.2.8. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder carga horária diária de 8 (oito) horas. Os horários e datas dos treinamentos serão definidos pela equipe técnica da AGEHAB e comunicados a contratada com antecedência de 10 (dez) dias consecutivos.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

5.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos do Termo de Referência, a:
5.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;
5.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;
5.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
5.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;
5.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência.
5.5. São expressamente vedadas à CONTRATADA, Ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;
5.6. Os funcionários da CONTRATADA, responsáveis pela instalação do serviço e treinamento aos colaboradores da Gerência de Tecnologia da Informação - GETI, deverão estar devidamente identificados com crachá e/ou outros identificadores quando nas instalações da AGEHAB;
5.7. Ficarão por conta da Contratada as possíveis despesas de transporte e hospedagem necessárias à execução do objeto;
5.8. Refazer, às suas expensas, todo e qualquer trabalho realizado em desconformidade com as determinações da AGEHAB ou, ainda, os que apresentarem defeitos, vícios ou incorreções;
5.9. Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação técnica apresentadas no processo licitatório, compatíveis com as obrigações assumidas neste Contrato;
5.10. Utilizar empregados habilitados e com conhecimentos compatíveis com os necessários para executar os serviços que lhes forem atribuídos, em conformidade com as normas e determinações em vigor;
5.11. Responder inteiramente por todos os encargos trabalhistas, previdenciários, fiscais, comerciais, seguro de acidentes, impostos e quaisquer outros que forem devidos e referentes aos serviços oriundos da contratação;
5.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência;
5.13. Executar os serviços de acordo com as condições, especificações, quantidades e demais detalhamentos no Termo de Referência – Anexo I.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

6.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc.
6.3. Efetuar o pagamento conforme execução dos serviços/produtos, desde que cumpridas todas as formalidades e exigências do contrato;
6.4. Exercer a fiscalização do contrato;
6.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;
6.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

CLÁUSULA SÉTIMA – DO LOCAL DE ENTREGA

7.1. Todos os produtos licitados serão entregues na sede da Agência Goiana de Habitação S/A - AGEHAB, situadas na Rua 18 A nº 541 – Setor Aeroporto – Goiânia – GO – CEP 74070-060.
7.2. A proposta comercial deverá considerar todos os custos relativos a logística e entrega dos equipamentos na cidade de Goiânia – GO.

CLÁUSULA OITAVA – DA VIGÊNCIA

8.1. O prazo de vigência do contrato é de 12 (doze) meses, contados da assinatura deste contrato, sendo que sua eficácia se dará a partir da publicação na imprensa oficial.

CLÁUSULA NONA – DO VALOR E DA FORMA DE PAGAMENTO

9.1. O valor global do presente contrato é de R$ 71.000,00 (setenta e um mil reais).
9.2. O pagamento será procedido mediante a apresentação da Nota Fiscal/Fatura, que deverá ser eletrônica em original ou a primeira via e original atestada, com a data e contendo a identificação do gestor do contrato que a atestou, após o fechamento do mês e a quitação até o 10º (décimo) dia útil do mês seguinte.
9.3. As nota(s) fiscal (is)/faturas deverão conter no mínimo os seguintes dados:
a) Data de emissão;
b) Estar endereçada a Agência Goiana de Habitação - AGEHAB, situada a Rua 18-A nº 541, Setor Aeroporto - Goiânia/GO, CNPJ nº 01.274.240/0001-47;
c) Preços unitários;
d) Descrição dos serviços;
9.4. O pagamento será efetuado após atesta pela autoridade competente assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e municipal.
9.5. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 9.2 passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa.
9.6. Se houver treinamento na sede da AGEHAB, deverá a Contratada apresentar, cópias legíveis pagas das guias de recolhimento do INSS, do FGTS com cópia do arquivo da SEFIP dos funcionários que tiveram o referido recolhimento e dos contracheques ou da folha de pagamento dos funcionários, que prestarem serviços para a Contratante, devidamente quitados e assinados, referente ao mês anterior ao do pagamento, além das Certidões Negativas de Débitos, do INSS, da Prefeitura Municipal, Trabalhista e do CRF do FGTS.

CLÁUSULA DÉCIMA – DA GARANTIA DO CONTRATO

10.1. A CONTRATADA deverá apresentar à AGEHAB, no prazo máximo de até 15 (quinze) dias uteis, contado da data de assinatura do CONTRATO, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor atualizado do total do contrato, nos termos do art. 56, da Lei nº 8.666, de 1993 e instruções complementares definidas no Edital.

10.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

10.3. Não serão admitidos, como garantia, os títulos da dívida pública, emitidos por pessoas jurídicas de direito público no período de 1850 a 1930, assim como aqueles de duvidosa liquidez, ao critério do CONTRATANTE, além de pedras preciosas, ainda que portadoras de certificado de conformação geológica.

10.4. A garantia, se prestada na forma de fiança bancária ou seguro-garantia, deverá ter validade durante a vigência do contrato.

10.5. Em se tratando de garantia prestada através de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal - CEF, conforme determina o art. 82 do Decreto nº 93872, de 23 de dezembro de 1986, sendo esta devolvida atualizada monetariamente, nos termo do §§ 4º, art. 56, da Lei nº 8.666/93.

10.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

10.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada nas mesmas condições.

10.8. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias úteis, contados da data em que tiver sido notificada.

10.9. A garantia prestada pela CONTRATADA será liberada, após o término da vigência do Contrato, depois de certificado pelo Gestor deste Contrato que o mesmo foi Totalmente realizado a contento, dentro do prazo de 10 (dez) dias úteis.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO DO CONTRATO

11.1. Será gestor deste contrato o empregado Sr. **SAULO DE TARSO GARCIA VITOY.** Este ficará responsável pelo acompanhamento da execução bem como pela fiscalização do presente instrumento, por meio de relatórios, inspeções, visitas, atestado da satisfatória realização do objeto e outros procedimentos que julgar necessário.

CLÁUSULA DÉCIMA SEGUNDA – DOS RECURSOS FINANCEIROS

12.1. As despesas decorrentes do presente contrato correrão à conta de **Recursos Próprios da AGEHAB.**

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES E MULTAS

13.1. Pela inexecução contratual, atraso injustificado na execução do contrato, sujeitará a Contratada, além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade da infração, obedecida os seguintes limites máximos:

1) 10% (dez por cento) sobre o valor do contrato em caso de descumprimento total da obrigação;

   a) Multa de até 0,1% (um décimo por cento) por semana de atraso, calculado sobre a respectiva etapa do serviço de implantação;

   b) No caso de atraso superior a 90 (noventa) dias, será aplicada penalidade adicional de até (um por cento) sobre a respectiva etapa do serviço de implantação, por mês, até o limite de 10 (dez) meses;

   c) No caso do não cumprimento ou cumprimento irregular dos serviços de Manutenção e Evolução Tecnológica dos Softwares ERPI; Suporte Técnico das Soluções Implementadas ERP; Treinamento nos softwares ERP será aplicada multa de até 0,2% (dois décimos por cento) sobre o valor total do Contrato, por dia de atraso, até o limite de 5% (cinco por cento);

2) 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

3) 0,7% (sete décimos por cento) sobre o valor do fornecimento não realizado, por cada dia subseqüente ao trigésimo.

4) suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração Pública, por prazo não superior a 05 (cinco) anos;

5) 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 o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

13.2. A multa será descontada dos pagamentos eventualmente devidos, ou ainda, quando for o caso, cobrada judicialmente.

13.3. Qualquer das penalidades aqui previstas e aplicadas será registrada junto ao CADFOR.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. A rescisão do presente contrato poderá ser:

14.1.1. Determinada por ato motivado da Administração, após processo regular, assegurado o contraditório e a ampla defesa, nos casos do artigo 78, incisos I a XII, XVII e parágrafo único e inciso XVIII, da Lei Federal nº 8.666 de 21/06/1993.

14.1.2. Amigável, por acordo entre as partes, reduzida a termo, desde que haja conveniência para a Contratante.

14.1.3. Judicial, nos termos da legislação.

CLÁUSULA DÉCIMA QUINTA – DAS DISPOSIÇÕES GERAIS

15.1. O presente contrato reger-se-á pelas suas cláusulas e normas consubstanciadas na Lei Federal nº 8.666/93.

15.2. Fica declarado competente o foro da Comarca de Goiânia, para dirimir quaisquer dúvidas referentes a este contrato.

15.3. Os casos omissos serão resolvidos de acordo com a Lei nº 8.666/93, e demais normas aplicáveis.

E por estarem justos e contratados, os representantes das partes assinam o presente instrumento, na presença de testemunhas conforme abaixo, em 03(três) vias de igual teor e forma, para um só efeito.

Goiânia, 28 de maio de 2018.

CLEOMAR DUTRA FERREIRA
Presidente

JOEL GOMES RIBEIRO
Diretor Administrativo

AMAURI BATISTA REGIS
Diretor Financeiro

FRANCISCO HILÁRIO COLINO DE MAGALHÃES
CORE Serviços e Informática EIRELI – ME
Contratada

Testemunhas:

1 - _____

CPF: 307.227.621-72

2 - _____

CPF: 002.934.011-70