ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA ECONOMIA

Contrato 024/2023 /ECONOMIA

PROCESSO Nº 202300004000910 – CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DE GOIÁS, POR INTERMÉDIO DA SECRETARIA DE ESTADO DA ECONOMIA, E A EMPRESA GLOBAL SEC. TECNOLOGIA & INFORMAÇÃO LTDA, PARA O FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DE PROTEÇÃO AVANÇADA DE ENDPOINTS (ESTAÇÕES DE TRABALHO E SERVIDORES) COM CARACTERÍSTICAS DE DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA, SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO E TREINAMENTO, COM DIREITO A ATUALIZAÇÃO E SUPORTE TÉCNICO, POR 36 (TRINTA E SEIS) MESES.

O **ESTADO DE GOIÁS**, pessoa jurídica de direito público interno, por intermédio da **SECRETARIA DE ESTADO DA ECONOMIA**, inscrita no CNPJ sob o nº 01.409.655/0001-80, com sede à Av. Vereador José Monteiro, nº 2.233, Complexo Fazendário Meia Ponte, Setor Nova Vila, nesta capital, doravante denominada **CONTRATANTE**, ora representada por seu Chefe de Gabinete, nos termos do art. 84-A da Lei estadual nº 17.928/2012 incluído pela Lei complementar nº 164, de 7 de julho de 2021 e conforme regulamento do Decreto estadual nº 9.898/2021 e da Portaria de Delegação nº 279, de 28 de julho de 2023, o Sr. **DANILLO CAETANO SOARES CARDOSO**, portador da CI nº 4516429 DGPC/GO e do CPF nº 011.174.661-24, residente e domiciliado em Goiânia – GO e do outro lado a empresa **GLOBAL SEC. TECNOLOGIA & INFORMAÇÃO LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 31.862.002/0001-13, com sede ao Setor Comercial Norte, Quadra 04 Bloco B, Sala 702, Edifício Varig - Asa Norte, Brasília-DF, CEP: 70.714-020, doravante denominada **CONTRATADA**, neste ato representada na forma de seus estatutos pelo Sr. **DENIS MÁRIO REIS DA SILVA**, brasileiro, Diretor Comercial, portador da CI nº 4273813 DGPC/GO e do CPF nº 011.808.681-29, residente e domiciliado em Taguatinga, Brasília - DF, resolvem firmar o presente contrato, para o FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DE PROTEÇÃO AVANÇADA DE ENDPOINTS (ESTAÇÕES DE TRABALHO E SERVIDORES) COM CARACTERÍSTICAS DE DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA, SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO E TREINAMENTO, COM DIREITO A ATUALIZAÇÃO E SUPORTE TÉCNICO**,** por 36 (trinta e seis) meses, de acordo com o Edital e seus anexos, resultante do Pregão Eletrônico nº 014/2023, objeto do Processo nº **202300004000910 de 04/01/2023**, estando as partes sujeitas aos preceitos da Lei Federal nº 10.520/2002, Lei Federal 8.666/1993, Lei Estadual nº 17.928/2012, Lei Estadual nº 18.989/2015, Decreto Estadual nº 9.666/2020 e Decreto Estadual nº 7.466/2011 e demais normas regulamentares aplicáveis à espécie, e às cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

Parágrafo 1º - O presente contrato tem por objeto o **FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DE PROTEÇÃO AVANÇADA DE ENDPOINTS (ESTAÇÕES DE TRABALHO E SERVIDORES) COM CARACTERÍSTICAS DE DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA, SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO E TREINAMENTO, COM DIREITO A ATUALIZAÇÃO E SUPORTE TÉCNICO, POR 36 (TRINTA E SEIS) MESES,** de acordo com as especificações estabelecidas no Edital e seus anexos, Proposta Comercial da **CONTRATADA** e nas cláusulas e condições abaixo relacionadas.

Parágrafo único – A **CONTRATADA** ficará obrigada a aceitar, nas mesmas condições aqui contratadas, acréscimos ou supressões do objeto do presente contrato, em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, conforme art. 65 da Lei nº 8.666/93 e alterações posteriores.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES

Parágrafo 1°– Geral

I - Todas as licenças de software deverão ser perpétuas, ou seja, expirado o período de validade, deverão permanecer funcionais para a proteção contra códigos maliciosos, excetuando-se as atualizações, usando as versões dos softwares e base de assinaturas que a CONTRATANTE possua ao final do período de validade. Portanto, serão aceitas reduções nas funcionalidades de detecção de novos códigos maliciosos após expiração das licenças, contanto que essa proteção e o gerenciamento da solução continuem ativos.

Parágrafo 2º - Servidor de Administração e Console Gerenciamento

I - Compatibilidade

a) Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64;

b) Microsoft Windows Server 2016 Standard / Core / Datacenter x64;

c) Microsoft Windows Server 2019 Standard / Core / Datacenter x64;

d) Microsoft Windows Server 2022 Standard / Core / Datacenter x64 ou superior;

e) Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

f) Microsoft Windows 8 Professional / Enterprise x64;

g) Microsoft Windows 8.1 Professional / Enterprise x32/x64;

h) Microsoft Windows 10 x32/x64;

i) Windows 11 Home / Pro / Enterprise / Education x64.

II - Suporte às seguintes plataformas virtuais

a) Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;

b) Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64.

III - Características

a) A console deve ser acessada via WEB (HTTPS) ou MMC;

b) A console deve suportar arquitetura on-premise e arquitetura cloud-based;

c) A console deve ser baseada no modelo cliente/servidor;

d) A console deve suportar autenticação de dois fatores;

e) Deve possuir compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

f) O servidor de administração deve possuir modelo de cluster ativo-passivo;

g) Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

h) Deve permitir incluir usuários do AD para logarem na console de administração;

i) A console deve ser totalmente integrada com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos móveis;

j) As licenças deverão ser perpétuas, ou seja, expirado a validade das mesmas o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração das licenças;

k) Deverá ser possível buscar novos produtos e soluções a partir da console;

l) Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

m) Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD;

n) Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

o) Deve armazenar histórico das alterações feitas em políticas;

p) Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

q) Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

r) A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

s) Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

t) A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

u) 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;

v) Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

w) Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

x) Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

y) Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

z) Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

aa) 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;

ab) A comunicação entre o cliente e o servidor de administração deve ser criptografada;

ac) Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

ad) Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

ad.1) Nome do computador;

ad.2) Nome do domínio;

ad.3) Range de IP;

ad.4) Sistema Operacional;

ad.5) Máquina virtual.

ae) Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

af) Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

af.1) Pesquisa de rede (Windows pooling);

af.2) Pesquisa ativa do AD (AD pooling);

af.3) Pesquisa de IP (IP pooling);

af.4) Pesquisa de rede (Zeroconf pooling).

ag) 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;

ah) Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

ai) 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 à proteção;

aj) 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;

ak) 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 2 (dois) dias, etc;

al) 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;

am) Deve fornecer as seguintes informações dos computadores:

am.1) Se o antivírus está instalado;

am.2) Se o antivírus está iniciado;

am.3) Se o antivírus está atualizado;

am.4) Minutos/horas desde a última conexão da máquina com o servidor administrativo;

am.5) Minutos/horas desde a última atualização de vacinas;

am.6) Data e horário da última verificação executada na máquina;

am.7) Versão do antivírus instalado na máquina;

am.8) Se é necessário reiniciar o computador para aplicar mudanças;

am.9) Data e horário de quando a máquina foi ligada;

am.10) Quantidade de vírus encontrados (contador) na máquina;

am.11) Nome do computador;

am.12) Domínio ou grupo de trabalho do computador;

am.13) Data e horário da última atualização de vacinas;

am.14) Sistema Operacional com Service Pack;

am.15) Quantidade de processadores;

am.16) Quantidade de memória RAM;

am.17) Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

am.18) Endereço IP;

am.19) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

am.20) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

am.21) Vulnerabilidades de aplicativos instalados na máquina.

an) Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

ao) Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

ao.1) Alteração de Gateway Padrão;

ao.2) Alteração de subrede;

ao.3)Alteração de domínio;

ao.4) Alteração de servidor DHCP;

ao.5) Alteração de servidor DNS;

ao.6) Alteração de servidor WINS;

ao.7) Resolução de Nome;

ao.8) Disponibilidade de endereço de conexão SSL.

ap) Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud;

aq) 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;

ar) 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;

as) Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

at) Capacidade de monitoramento do sistema através de um SNMP client;

au) Capacidade enviar eventos através de protocolo de syslog;

av) Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF;

aw) Deve ser capaz de enviar os eventos para sistemas de SIEM em canal encriptado;

ax) Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk;

ay) Capacidade de enviar e-mails para contas específicas em caso de algum evento;

az) Listar em um único local, todos os computadores não gerenciados na rede;

ba) Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

bb) Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

bc) 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;

bd) Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

be) Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

bf) Deve permitir a configuração de senha no endpoint e configurar quando será necessário utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

bg) Deve ser capaz de configurar quais eventos serão armazenados localmente (nos eventos do Windows) ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

bh) Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

bi) Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

bi.1) Nome do vírus;

bi.2) Nome do arquivo infectado;

bi.3) Data e hora da detecção;

bi.4) Nome da máquina ou endereço IP;

bi.5) Ação realizada.

bj) Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

bk) Capacidade de listar updates nas máquinas com o respectivo link para download;

bl) Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

bm) Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

bn) Capacidade de realizar resumo de hardware de cada máquina cliente;

bo) Capacidade de diferenciar máquinas virtuais de máquinas físicas.

Parágrafo 3º - Sistemas Operacionais Windows

I - Compatibilidade

a) Sistemas para estações de trabalho

a.1) Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

a.2) Microsoft Windows 8 Professional/Enterprise;

a.3) Microsoft Windows 8.1 Professional / Enterprise;

a.4) Microsoft Windows 10 Pro / Enterprise / Home / Education;

a.5) Microsoft Windows 11 Pro / Enterprise / Home / Education.

b) Sistemas servidores

b.1) Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

b.2) Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

b.3) Windows Server 2016 Essentials / Standard / Datacenter;

b.4) Windows Server 2019 Essentials / Standard / Datacenter;

b.5) Microsoft Windows Server 2022 Standard / Core / Datacenter x64 ou superior.

II - Suporte às seguintes plataformas virtuais

a) Vmware Workstation 16.2.3 ou superior;

b) Vmware ESXi 7.0 ou superior.

III - Características

a) Deve prover as seguintes proteções:

a.1) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

a.2) Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

a.3) Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

a.4) O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

a.5) Deve possui módulo dedicado contra prevenção de intrusão, prevenção de intrusão do host;

a.6) Autoproteção (contra-ataques aos serviços/processos do antivírus);

a.7) Controle de dispositivos externos;

a.8) Controle de acesso a sites por categoria, ex: bloquear conteúdo adulto, sites de jogos, etc;

a.9) Controle de acesso a sites por horário;

a.10) Controle de acesso a sites por usuários;

a.11) Controle de acesso a websites por dados, ex: bloquear websites com conteúdos de vídeo e áudio;

a.12) Controle de execução de aplicativos;

a.13) Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

c) 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);

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

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

f) 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;

g) Deverá possuir módulo dedicado para proteção contra port scanning;

h) Deverá possuir módulo dedicado para proteção contra network flooding;

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

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

k) 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 à partir da extensão do arquivo;

l) Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

m) Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas;

n) Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint;

o) Deverá realizar scanner de firmaware em busca de rootkits;

p) Ao detectar uma ameaça, a solução deve exibir informações:

p.1) Do objeto SHA256;

p.2) Do objeto MD5.

q) Capacidade de verificar somente arquivos novos e alterados;

r) Capacidade de verificar objetos usando heurística;

s) Capacidade de agendar uma pausa na verificação;

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

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

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

v.1) Perguntar o que fazer, ou;

v.2) Bloquear acesso ao objeto;

v.2.1) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

v.2.2) Caso positivo de desinfecção:

v.2.2.1) Restaurar o objeto para uso.

v.2.3) Caso negativo de desinfecção:

v.2.3.1) Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

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

x) Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

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

z) Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e análise de heurística bloqueado arquivos, sites de phishing e URL maliciosas;

aa) Capacidade de verificação de corpo e anexos de e-mails usando heurística;

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

ab.1) Perguntar o que fazer, ou;

ab.2) Bloquear o e-mail;

ab.2.1) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

ab.2.2) Caso positivo de desinfecção:

ab.2.2.1) Restaurar o e-mail para o usuário.

ab.2.3) Ab.Caso negativo de desinfecção:

ab.2.3.1) Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

ac) Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

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

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

af) Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Trafego de rede por aplicativo.

ag) Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

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

ah.1) Perguntar o que fazer, ou;

ah.2) Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

ah.3) Permitir acesso ao objeto.

ah.4) O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

ah.4.1) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

ah.4.2) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

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

aj) 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;

ak) 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;

al) Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas;

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

an) Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

ao) Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

ap) Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário;

aq) O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

aq.1) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

aq.2) 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.

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

ar.1) Discos de armazenamento locais;

ar.2) Armazenamento removível;

ar.3) Impressoras;

ar.4) CD/DVD;

ar.5) Drives de disquete;

ar.6) Modems;

ar.7) Dispositivos multifuncionais;

ar.8) Leitores de smart card;

ar.9) Wi-Fi;

ar.10) Adaptadores de rede externos;

ar.11) Dispositivos MP3 ou smartphones;

ar.12) Dispositivos Bluetooth;

ar.13) Câmeras e Scanners.

as) 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;

at) Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

au) Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

av) Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras;

aw) Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc;
5.3.3.50 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

ax) 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);

ay) Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado;

az) Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

ba) O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

ba.1) Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras;

ba.2) White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

bb) Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

bc) 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;

bd) 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;

be) 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;

bf) Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware;

bg) Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

bh) Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);

bi) Capacidade de integração com a Antimalware Scan Interface (AMSI);

bj) Deve permitir realizar o gerenciamento por meio de integração via REST API;

bk) Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

Parágrafo 4º - Sistemas Operacionais GNU/Linux

I - Compatibilidade

a) Plataforma 32-bits:

a.1) Red Hat Linux 6.7 e superiores;

a.2) CentOS 6.7 e superiores;

a.3) Debian 9.4 e superiores.

b) Plataforma 64-bits:

b.1) Ubuntu 18.04 e superiores;

b.2) Red Hat Enterprise Linux 6.7 e superiores;

b.3) CentOS 6.7 e superiores;

b.4) Debian 9.4 e superiores;

b.5) SUSE Server 12 e superiores;

b.6) Oracle Linux 7.3 e superiores;

b.7) Oracle Linux 8.0 e superiores.

II - Características

a) Deve prover as seguintes proteções:

a.1) Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

b) Deve permitir gerenciamento, no mínimo, das seguintes formas:

b.1) Via linha de comando;

b.2) Via console administrativa;

b.3) Via GUI;

b.4) Via web (remotamente).

c) Deve possuir funcionalidade de scan de drives removíveis, tais como:

c.1) CDs;

c.2) DVDs;

c.3) Discos blu-ray;

c.4) Flash drives (pen drives);

c.5) HDs externos.

d) Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

d.1) Por tipo de dispositivo;

d.2) Por barramento de conexão.

e) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

f.1) Capacidade de criar exclusões por local, máscara e nome da ameaça;

f.2) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

f.3) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

f.4) Leitura de configurações;

f.5) Modificação de configurações;

f.6) Gerenciamento de Backup;

f.7) Visualização de logs;

f.8) Gerenciamento de logs;

f.9) Gerenciamento de ativação da aplicação;

f.10) Gerenciamento de permissões (adicionar/excluir permissões acima);

f.11) Capacidade de criar exclusões por local, máscara e nome da ameaça;

f.12) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

f.13) 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;

f.14) Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

f.15) Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

f.15.1) Alta;

f.15.2) Média;

f.15.3) Baixa;

f.15.4) Recomendado.

f.16) Gerenciamento de quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

f.17) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);análise de arquivos; desinfecção ou remoção de objetos infectados;

f.18) Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

f.19) Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

f.20) Deverá ser possível priorizar a execução de tarefas;

f.21) Capacidade de verificar objetos usando heurística;

f.22) Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

f.23) Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário;

f.24) O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

f.24.1) Detecção de phishing e sites maliciosos;

f.24.2) Bloqueio de download de arquivos maliciosos;

f.24.3) Bloqueio de adware.

f.25) Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

f.26) Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

f.27) Deverá fornecer informações de todas os executáveis das aplicações;

f.28) Deve possuir módulo de proteção contra criptografia maliciosa;

f.29) Deverá possuir controle de execução de aplicações;

f.30) O módulo de controle de aplicação deverá possuir as seguintes funcionalidades:

f.30.1) Criação de lista de bloqueio de aplicação;

f.30.2) Criação de lista de permissão de aplicação.

f.31) Deverá realizar busca de ameaças em setores críticos do sistema operacional:

f.31.1) Setor de inicialização;

f.31.2) Objetos de inicialização;

f.31.3) Processos de memória;

f.31.4) Memória do kernel.

Parágrafo 5º - Servidores Windows legados x32 ou x64

I - Compatibilidade

a) Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

b) Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior.

II - Características

a) Deve prover as seguintes proteções:

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

b.1) Auto-proteção contra-ataques aos serviços/processos do antivírus;

b.2) Firewall com IDS;

b.3) Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

d) Deve permitir gerenciamento, no mínimo, das seguintes formas:

d.1) Via console administrativa;

d.2) Via web (remotamente).

e) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

f) Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo;

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

g.1) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

g.2) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

g.3) Leitura de configurações;

g.4) Modificação de configurações;

g.5) Gerenciamento de backup;

g.6) Visualização de logs;

g.7) Gerenciamento de logs;

g.8) Gerenciamento de ativação da aplicação;

g.9) Gerenciamento de permissões (adicionar/excluir permissões acima);

g.10) Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

h) O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

h.1) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

h.2) 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.

i) 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;

j) Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

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

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

m) Deve possuir funcionalidade de análise personalizada de logs do Windows;

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

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

p) Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

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

r) 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: “WannaCry”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

s) 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;

t) Capacidade de verificar somente arquivos novos e alterados;

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

v) Capacidade de verificar objetos usando heurística;

w) Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

x) Capacidade de agendar uma pausa na verificação;

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

y.1) Perguntar o que fazer, ou;

y.2) Bloquear acesso ao objeto;

y.2.1) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

y.2.2) Caso positivo de desinfecção:

y.2.2.1) Restaurar o objeto para uso.

y.2.3) Caso negativo de desinfecção:

y.2.3.1) Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

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

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

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

ac) Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

ac.1) Executar os procedimentos pré-configurados pelo administrador;

ac.2) Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

ad) Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

ae) Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

af) Capacidade de detectar anomalias no comportamento de um software usando análise heurística e aprendizado de máquina (machine learning);

ag) Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta;

ah) Deve possuir controle de dispositivos externos.

Parágrafo 6º - Criptografia

I - Características

a) 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;

b) Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

c) Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

d) Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

e) Permitir criar vários usuários de autenticação pré-boot;

f) Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

g) Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

h) Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

h.1) Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

h.2) Criptografar todos os arquivos individualmente;

h.3) Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

h.4) Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.

i) Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;

j) Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

k) Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

l) Verifica compatibilidade de hardware antes de aplicar a criptografia;

m) Possibilita estabelecer parâmetros para a senha de criptografia;

n) Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

o) Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

p) Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

q) Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

r) Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;

s) Permite criar um grupo de extensões de arquivos a serem criptografados;

t) Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

u) Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;

v) Capacidade de deletar arquivos de forma segura após a criptografia;

w) Capacidade de criptografar somente o espaço em disco utilizado;

x) Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

y) Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

z) Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

aa) Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

ab) Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

ac) Capacidade de fazer “Hardware encryption”.

Parágrafo 7º - Gerenciamento de Sistemas

a) Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

b) Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

c) Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

d) 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;

e) Capacidade de gerenciar licenças de softwares de terceiros;

f) Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

g) Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);

h) Possibilita fazer distribuição de software de forma manual e agendada;

i) Suporta modo de instalação silenciosa;

k) Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

l) Possibilita fazer a distribuição através de agentes de atualização;

m) Utiliza tecnologia multicast para evitar tráfego na rede;

n) Possibilita criar um inventário centralizado de imagens;

o) Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

p) Suporte a WakeOnLan para deploy de imagens;

q) Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

r) Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

s) Capacidade de gerar relatórios de vulnerabilidades e patches;

t) Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

u) Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

v) Permite baixar atualizações para o computador sem efetuar a instalação;

w) Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

x) Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

y) Permite selecionar produtos a serem atualizados pela console de gerenciamento;

z) Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

aa) Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

ab) Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

ac) Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

ad) Deve permitir selecionar o idioma das aplicações que serão atualizadas;

ae) Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

Parágrafo 8º - Detecção e Resposta a incidentes

I - Compatibilidade

a) Estações de trabalho e Notebooks

a.1) Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

a.2) Microsoft Windows 8 Professional/Enterprise;

a.3) Microsoft Windows 8.1 Professional / Enterprise;

a.4) Microsoft Windows 10 Pro / Enterprise / Home / Education;

a.5) Microsoft Windows 11 Pro / Enterprise / Home / Education ou superior.

b) Servidores

b.1) Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

b.2) Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

b.3) Windows Server 2016 Essentials / Standard / Datacenter;

b.4) Windows Server 2019 Essentials / Standard / Datacenter;

b.5) Microsoft Windows Server 2022 Standard / Core / Datacenter x64 ou superior.

II - Características

a) As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

b) A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

b.1) O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

b.2) Deve fornecer graficamente a visualização da cadeia do ataque;

b.3) Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC);

b.4) A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

b.4.1) Isolar o host;

b.4.2) Iniciar uma varredura nas áreas críticas;

b.4.3) Quarentenar o objeto;

b.4.4) A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

b.4.4.1) Visibilidade das detecções provenientes de endpoint;

b.4.4.2) Processos;

b.4.4.3) Conexões remotas;

b.4.4.4) Alterações de registros;

b.4.4.5) Objetos baixados.

b.5) Capacidade de integração com a solução de sandbox;

b.6) Deverá possuir informações de assinaturas digitais da ameaça;

b.7) Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

b.8) Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

b.9) Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

b.10) A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

b.10.1) Detecções provenientes da solução de endpoint;

b.10.2) Detecções provenientes da solução de sandbox;

b.10.3) Processos;

b.10.4) Alterações de registro;

b.10.5) DLL's;

b.10.6) Conexões remotas;

b.10.7) Criação de arquivos;

b.10.8) Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador;

b.10.9) Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

b.11) A solução deve oferecer no mínimo as seguintes opções de resposta:

b.11.1) Prevenir a execução de um arquivo;

b.11.2) Quarentenar um arquivo;

b.11.3) Iniciar uma varredura por IoC;

b.11.4) Parar um processo;

b.11.5) Executar um processo.

b.12) Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

b.12.1) A opção de isolamento deve estar disponível junto a visualização do incidente;

b.12.2) Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra.

b.13) Na análise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

b.14) As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações;

b.15) Deverá ser possível remover a máquina do isolamento a partir do incidente;

b.16) A visualização da cadeia de ataque deve conter informações setorizadas por módulos do incidente;

b.17) Deve possuir as seguintes opções de gerenciamento:

b.17.1) Via console administrativa;

b.17.2) Via interface web;

b.17.3) Gerenciamento baseado em nuvem;

b.17.4) Gerenciamento via linha de comando.

b.18) Deve oferecer informações de inteligência de ameaças do próprio fabricante;

b.19) Deve possuir detecção baseada em sandbox do tipo cloud;

b.20) Deve suportar IoC de terceiros em formatos OpenIOC;

b.21) Deve fornecer a opção de proteger a aplicação por senha;

b.22) A opção de proteção por senha deve permitir especificar uma força mínima para a senha da aplicação.

III - Implantação e configuração da solução (incluindo Hands On)

a) Caberá a CONTRATADA a prestação dos serviços de implantação e configuração da Solução de segurança desejada;

b) Os serviços desejados poderão ser realizados de forma presencial ou remota, desde que sejam utilizadas ferramentas de acesso remoto seguro ao ambiente da CONTRATANTE;

c) Deverá ser ministrado um treinamento do tipo “hands on” durante a implantação da atualização do produto, de forma a ocorrer a transferência de tecnologia do produto para o corpo técnico do Secretaria de Estado da Economia.

IV - Treinamento oficial do fabricante

a) O treinamento a ser realizado deverá ser Oficial do fabricante em idioma português;

b) O treinamento deve ser realizado em horário comercial;

c) É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização dos treinamentos;

d) O treinamento deverá ser ministrado por instrutor qualificado tecnicamente;

e) O treinamento deverá ser ministrado na modalidade presencial, ou remota, desde que em tempo real e com a anuência da CONTRATANTE;

f) O treinamento deverá ocorrer em local a ser definido pela CONTRATANTE;

g) O treinamento deverá ser ministrado para turma de até 05 (cinco) alunos, de acordo com a conveniência da CONTRATANTE;

h) Deverá ter duração mínima de até 20 (vinte) horas, sendo dividido em turnos e dias a serem agendados previamente, de acordo com a conveniência da CONTRATANTE;

i) Deverá ser fornecido certificado de participação no treinamento contendo carga horária e ementa aplicada.

CLÁUSULA TERCEIRA – FORMA DE ENTREGA

A entrega das subscrições de licenças, bem como o início da instalação, configuração e implementação (incluindo *Hands On*) de toda solução deverá ocorrer no prazo máximo de 15 (quinze) dias corridos, a contar da SOLICITAÇÃO feita pela Gerência de Suporte Técnico da Superintendência de Tecnologia da Informação, conforme necessidade da CONTRATANTE, devendo a entrega do referido produto ser através de mídia digital via Internet ou E-mail.

CLÁUSULA QUARTA – CRITÉRIOS DE RECEBIMENTO

Parágrafo 1º - A solução será recebida provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização, mediante assinatura do Termo de Recebimento Provisório, para efeito de posterior verificação da quantidade, qualidade e conformidade com as especificações constantes neste Contrato, no prazo de até 10 (dez) dias após o término da implantação da solução e entrega de relatório pela CONTRATADA;

Parágrafo 2º - Caso sejam identificadas irregularidades, os produtos serão recusados e devolvidos à empresa fornecedora que, por sua vez, deverá substituí-los também no prazo máximo de 05 (cinco) dias úteis, sem qualquer ônus para a CONTRATANTE;

Parágrafo 3º - A solução será recebida definitivamente em até 10 (dez) dias da emissão do Termo de Recebimento Provisório, salvo se existirem pendências a serem saneadas, após validação operacional do ambiente, onde se dará a verificação da perfeita execução das obrigações contratuais (qualidade e/ou quantidade, etc), ocasião em que a CONTRATANTE emitirá o Termo de Recebimento Definitivo;

Parágrafo 4º - Para os serviços de treinamento, o recebimento provisório ocorrerá mediante recibo, após finalizada sua execução e recebimento da fatura, para posterior verificação da sua conformidade com a especificação. O recebimento definitivo ocorrerá em até 15 (quinze) dias corridos após verificação da adequação dos serviços às especificações, com consequente atesto na fatura;

Parágrafo 5º - A execução do serviço pela CONTRATADA e o recebimento provisório pelo CONTRATANTE, não implica em sua aceitação definitiva;

Parágrafo 6º - São critérios de aceitação definitiva da solução:

I - Verificação da quantidade, qualidade e conformidade dos serviços e produtos com as especificações constantes no Contrato, no Termo de Referência e seus anexos;

II - Realização de procedimento de validação e testes no ambiente para comprovação de que a solução atende todos os requisitos técnicos e de negócio previsto no Contrato, no Termo de Referência e seus anexos;

III - Após a validação operacional da implantação e migração por unidade do CONTRATANTE, que ocorrerá de forma independente, devendo estar os bens destinados à unidade instalados, configurados, testados e que tenham funcionado ininterruptamente durante o período de validação operacional.

IV - São critérios de aceitação dos treinamentos:

V - Deverá haver comprovação de que o índice de satisfação dos participantes foi superior ou igual a 70% (setenta por cento), índice que, caso não alcançado, obrigará a CONTRATADA a ministrar novo treinamento para a referida turma, sem ônus para o CONTRATANTE.

Parágrafo 7º - O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

CLÁUSULA QUINTA - GARANTIA E ASSISTÊNCIA TÉCNICA

Parágrafo 1º - A garantia deverá considerar o período mínimo de 36 (trinta e seis) meses contados a partir da data de recebimento definitivo e contemplar a prestação dos seguintes serviços:

I - Atualização de versão do software e acesso ao sítio do fabricante (por intermédio de usuário/senha) para o download de patches e fixes de correção (de código), service packs, novas versões de manutenção geral, versões de determinadas funcionalidades, releases e builds, documentação atualizada e o acesso a base de conhecimento do fabricante.

Parágrafo 2º - A modalidade de atendimento deverá ser em regime 8x5 (oito horas por dia x cinco dias da semana), de segunda a sexta-feira, das 8h às 18h - é considerado dia útil aquele com expediente normal na Secretaria da Economia de Goiás;

Parágrafo 3º - A garantia e o suporte técnico deverão ser fornecidos contra defeitos de software sem custos além daqueles constantes da proposta de preço e pelo prazo de garantia ofertado;

Parágrafo 4º - A abertura de chamados consistirá em esclarecimento de dúvidas, orientação no uso do software, configuração do(s) produto(s), solução de problemas, dentre outras solicitações;

Parágrafo 5º - A abertura de chamados poderá ter origem em decorrência de configuração e instalação/desinstalação de funcionalidades ou outro problema detectado pela equipe técnica da Secretaria da Economia;

Parágrafo 6º - As atividades relacionadas ao suporte técnico devem ser realizadas por meio de contato telefônico e/ou troca de mensagens eletrônicas. Os chamados poderão ser atendidos de forma remota;

Parágrafo 7º - Não haverá limite de quantidade de chamados durante a vigência do contrato;

Parágrafo 8º - As atividades relacionadas ao suporte técnico devem ser realizadas por profissionais certificados pelo fabricante;

Parágrafo 9º - Em todas as atividades relacionadas ao suporte técnico deverá ser empregada a língua portuguesa falada e escrita do Brasil. Serão admitidas as seguintes exceções a esta exigência:

I - O uso de termos técnicos em inglês, por meio de contato telefônico e/ou troca de mensagens eletrônicas;

II - O acesso a sítios com conteúdo na língua inglesa, para consulta a bases de conhecimento ou download de módulos do software.

Parágrafo 10º - A garantia e o suporte técnico deverão ser fornecidos por intermédio dos seguintes canais de atendimento para abertura dos chamados:

I - Sítio na internet e telefone (preferencialmente 0800) ou Sítio na internet e call center.

Parágrafo 11º - O Sítio na internet deverá permitir acompanhar os chamados de suporte técnico e deverá possuir informações relacionadas ao histórico do(s) atendimento(s);

Parágrafo 12º - Deverão ser considerados os seguintes prazos e níveis de severidade para os chamados de suporte técnico:

Severidade	Descrição	Tempo para Solução
Severidade 1 (um)	Impacto crítico sobre o negócio. Quando ocorre a perda ou paralisação de serviços relevantes prestados pela CONTRATANTE ou atividades exercidas pela mesma, configurando-se como situação de emergência. Uma solicitação de serviço de Severidade 1 (um) pode possuir uma ou mais das seguintes características: · Dados corrompidos; · Uma função crítica não está disponível; · O sistema se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos; · O sistema falha repetidamente após tentativas de reinicialização.	4 (quatro) horas*
Severidade 2 (dois)	Impacto significativo sobre o negócio. Problema grave, prejudicando a operação do sistema. Quando se verifica uma grave perda de funcionalidades em programas ou sistemas da CONTRATANTE, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço.	8 (oito) horas*
Severidade 3 (três)	Pouco impacto sobre o negócio. Problemas que criam algumas restrições a operação do sistema. Quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas da CONTRATANTE, causando apenas inconveniências para a devida prestação dos serviços pela CONTRATANTE.	12 (doze) horas*
Severidade 4 (quatro)	Dúvidas que não afetam a operação do sistema. Quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas, porém sem prejudicar diretamente a operação dos programas ou sistemas da CONTRATANTE.	24 (vinte e quatro) horas*
*em regime 8x5 (oito horas por dia x cinco dias da semana (UTC – 3)), de segunda a sexta-feira - é considerado dia útil aquele com expediente normal na CONTRATANTE.		

Parágrafo 13º - A atualização e configuração das licenças deverão ocorrer nas datas e horários definidos pela equipe técnica da Gerência de Suporte Técnico da Superintendência de Tecnologia da Informação da Secretaria de Estado da Economia, que supervisionará os trabalhos;

Parágrafo 14º - As atualizações das licenças deverão ser fornecidas durante o período de vigência contratual, incluindo novas versões corretivas ou evolutivas dos softwares, sem ônus adicionais para a CONTRATANTE;

Parágrafo 15º - Caso sejam detectados bugs ou falhas no software, a fabricante ou empresa técnica autorizada, deverá fornecer atualizações necessárias à correção do problema;

Parágrafo 16º - Os serviços a serem executados pela CONTRATADA ou fabricante incluem atividades de manutenção Evolutiva, Preventiva e Corretiva de software, inclusive serviços relacionados à prevenção de incidentes o melhoria do ambiente;

Parágrafo 17º - Toda e qualquer despesa decorrente do suporte técnico, atualizações, manutenções preventivas e corretivas, realizados durante o período de vigência das licenças será de responsabilidade da CONTRATADA, não restando ônus para a Secretaria da Economia;

Parágrafo 18º - Os procedimentos destinados a prevenir e/ou corrigir a ocorrência de erros e defeitos das licenças, bem como quaisquer outras atividades para a sua devida operação em perfeito estado de uso deverão ser realizados de acordo com os manuais e as normas técnicas específicas;

Parágrafo 19º - Todas as solicitações feitas pela CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços, de modo a permitir a produção de relatórios gerenciais referentes a todo o período de execução do contrato;

Parágrafo 20º - Um chamado técnico somente poderá ser fechado após confirmação de um responsável técnico pelo contrato na Gerência de Suporte Técnico e o término de atendimento se dará com a disponibilidade da licença em perfeitas condições de funcionamento;

Parágrafo 21º - A CONTRATANTE reserva-se o direito de efetuar auditoria e vistoria nos serviços realizados, aplicando as apenações previstas, caso seja constatada a prática de procedimentos inadequados ou não recomendados pelo fabricante;

Parágrafo 22º - A CONTRATANTE rejeitará, no todo ou em parte, os serviços/entregas executados em desacordo com as condições estabelecidas neste Contrato.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA

Parágrafo 1º - A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

I - Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

II - O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada, quando for o caso;

III - Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

IV - Substituir, reparar ou corrigir, às suas expensas, no prazo fixado no Termo de Referência, o objeto com avarias ou defeitos;

V - Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

VI - Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

VII - Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

VIII - Responsabilizar-se pelo custeio das despesas referente ao transporte, embalagem e seguro quando da entrega dos materiais e por todos encargos decorrentes da execução deste contrato, tais como: obrigações civis, trabalhistas, fiscais, previdenciárias ou quaisquer outras, serão de exclusiva responsabilidade da CONTRATADA;

IX - Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993;

X - Indicar preposto para representá-la durante a execução do contrato;

XI - Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da CONTRATANTE ou da nova empresa que continuará a execução dos serviços;

Parágrafo 2º - A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo a instalação do software e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

Parágrafo 3º - Seguir e manter operante, durante a execução contratual, o Programa de Integridade nos termos da Lei Estadual nº 20.489/2019.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATANTE

Parágrafo 1º - São obrigações da CONTRATANTE:

I - Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

II - Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

III - Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

IV - Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

V - Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

VI - Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

VII - Não praticar atos de ingerência na administração da CONTRATADA, tais como:

a) exercer o poder de mando sobre os empregados da CONTRATADA, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

b) direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

c) promover ou aceitar o desvio de funções dos trabalhadores da CONTRATADA, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e

d) considerar os trabalhadores da CONTRATADA como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

Parágrafo 2º - A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA OITAVA – CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

Parágrafo 1º - A CONTRATADA deverá comprometer-se, por si e por seus colaboradores, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança, mantendo estrita conformidade com as Políticas e Normas de Tecnologia e Segurança da Informação em vigor na CONTRATANTE ou que vierem a ser estabelecidas no período de vigência contratual, bem como os normativos vigentes e as boas práticas relativas à segurança da informação, especialmente as que forem indicadas pela Subsecretaria de Tecnologia da Informação da Secretaria-Geral de Governo - STI/SGG, e normas de sigilo fiscal, estabelecidas na Instrução Normativa nº 1.455/2020-GSE - que dispõe sobre o sigilo fiscal no âmbito da Secretaria de Estado da Economia -, em todas as atividades executadas.

Parágrafo 2º - Os serviços deverão ser prestados em conformidade com leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicação.

Parágrafo 3º - É de total responsabilidade da CONTRATADA qualquer ocorrência de transferência, remanejamento dos seus colaboradores envolvidos diretamente na execução dos serviços objeto do presente certame. Se isto ocorrer, no entanto, a CONTRATANTE deverá ser comunicada com antecedência mínima de 5 (cinco) dias úteis e a CONTRATADA deverá providenciar a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da ECONOMIA.

Parágrafo 4º - A CONTRATADA firmará por meio de Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança da Informação, conforme Modelo no ANEXO I deste Contrato, o compromisso de manter total sigilo e preservar a segurança das informações, assim como obterá por meio do Termo de Ciência Individual de Sigilo e Segurança da Informação, conforme modelo no ANEXO II, a ciência de cada colaborador a serviço da CONTRATADA que irá prestar os serviços constantes nesta contratação.

Parágrafo 5º - Todo e qualquer profissional a serviço da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional da CONTRATANTE não poderá ser utilizada para fins particulares, sendo que quaisquer ações que tramitem em sua rede poderão ser auditadas.

Parágrafo 6º - Todas as informações, documentos e especificações técnicas as quais a CONTRATADA (representantes, empregados e colaboradores) tiver acesso em função da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação a terceiros, devendo esta zelar pela manutenção do sigilo absoluto do conhecimento adquirido em razão dos serviços executados, de acordo com o firmado no Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança da Informação.

Parágrafo 7º - A CONTRATADA é integralmente responsável pela manutenção de sigilo sobre quaisquer dados e informações fornecidos pela CONTRATANTE, ou contidos em quaisquer documentos e mídias aos quais venha a ter acesso durante a etapa de implantação, de configuração, de execução dos serviços e de encerramento contratual, não podendo, sob qualquer pretexto e forma, divulgá-los, reproduzi-los ou utilizá-los para fins alheios à exclusiva necessidade dos serviços contratados.

I - A CONTRATADA deve guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados, observando os princípios do art. 6º da Lei nº 13.709/2018 (LGPD), bem como da relação contratual mantida com a CONTRATANTE.

CLÁUSULA NONA – DO VALOR E DOS RECURSOS ORÇAMENTÁRIOS

LOTE ÚNICO	ITEM	DESCRIÇÃO	MÉTRICA	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01	01	Licença de Software de proteção para estações de trabalho, dispositivos móveis (notebooks) e servidores, com módulo de EDR, implantação e configuração da solução (incluindo *Hands On*), garantia e suporte por no mínimo 36 meses	Unidade	3.500	R$ 282,85	R$ 989.975,00
	02	Treinamento oficial do fabricante do software (para até 5 pessoas)	Serviço	1	R$ 15.000,00	R$ 15.000,00
Valor Total						**R$ 1.004.975,00**

Parágrafo 1º – O valor total do presente contrato de acordo com a Proposta Comercial da **CONTRATADA** é de R$ 1.004.975,00 (um milhão, quatro mil novecentos e setenta e cinco reais).

Parágrafo 2º – Os quantitativos pretendidos devem ser capazes de sustentar de forma adequada a infraestrutura que compõem o parque computacional da Secretaria de Estado da Economia, totalizando o quantitativo de 3.500 (três mil e quinhentas) licenças, distribuídas da seguinte forma:

I - 2.798 desktops e notebooks;

II - 500 desktops virtuais (VDI);

III - 114 servidores virtuais;

IV - Margem de segurança de 2,6%

Parágrafo 3º – As despesas decorrentes da execução deste contrato correrão neste exercício, à conta das verbas nº 2023.17.01.04.122.4200.4243.03, fonte 15000100, e nº 2023.17.01.04.122.4200.4243.04, fonte 25000100, do vigente Orçamento Estadual, conforme Notas de Empenho nº 00316, de 28/07/2023, no valor de R$ 15.000,00 (quinze mil reais), e nº 00004, de 27/07/2023, no valor de R$ 989.975,00 (novecentos e oitenta e nove mil novecentos e setenta e cinco reais), emitidas pela Seção competente da Secretaria de Estado da Economia.

CLÁUSULA DÉCIMA - CONDIÇÕES DE PAGAMENTO, REAJUSTE, ACRÉSCIMOS E SUPRESSÕES

Parágrafo 1º – O pagamento à CONTRATADA será efetuado pelos serviços efetivamente prestados, no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, acompanhada da comprovação da regularidade fiscal, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA

Parágrafo 2º - Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal ou Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

Parágrafo 3º – Considera-se ocorrido o recebimento da Nota Fiscal ou Fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

Parágrafo 4º - Havendo erro na apresentação da Nota Fiscal ou Fatura ou dos documentos pertinentes à contratação ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

Parágrafo 5º – Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

Parágrafo 6º – Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionada a taxa de atualização financeira devida pelo CONTRATANTE, mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo

I = (TX/100), assim apurado: I = (6/100) I = 0,00016438
365 365

Em que:

I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual = 6%;
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.

Parágrafo 7º – Os preços inicialmente contratados dos serviços poderão ser reajustados mediante prévia negociação entre as partes, observados os preços praticados no mercado, bem como a periodicidade mínima de 01 (um) ano, contada da data de apresentação da proposta ou, no caso de novo reajuste, a data a que a anterior tiver se referindo, tendo como limite máximo a variação do IPCA/IBGE, ou em conformidade com outros dispositivos legais que venham a ser editados pelo Poder Público.

Parágrafo 8º – Os reajustes a que a CONTRATADA fizer jus e não forem solicitadas durante a vigência do Contrato, serão objeto de preclusão com a assinatura da prorrogação contratual ou com o encerramento do Contrato.

Parágrafo 9º - A CONTRATADA ficará obrigada a aceitar nas mesmas condições aqui contratadas, acréscimos ou supressões do objeto do presente contrato, em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, conforme § 1º do Art. 65 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIGÊNCIA CONTRATUAL

Parágrafo 1º – O contrato vigorará por 36 (trinta e seis) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por 24 meses, limitado a 60 (sessenta) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, da Lei nº 8.666, de 1993.

Parágrafo 2º – A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

CLÁUSULA DÉCIMA SEGUNDA - DA GARANTIA DE EXECUÇÃO DO CONTRATO

Parágrafo 1º - A CONTRATADA apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, em valor correspondente a 5% (cinco por cento) do valor total do contrato, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação.

Parágrafo 2º - A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

I - O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666 de 1993.

Parágrafo 3º - A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

I - prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

II - prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

III - multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e

IV - obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

Parágrafo 4º - A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem anterior, observada a legislação que rege a matéria.

Parágrafo 5º - A garantia em dinheiro deverá ser efetuada em conta bancária em nome da CONTRATANTE, com correção monetária.

Parágrafo 6º - 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 pela Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

Parágrafo 7º - No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

Parágrafo 8º - No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

Parágrafo 9º - Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 30 (trinta) dias úteis , contados da data em que for notificada.

Parágrafo 10º - A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

Parágrafo 11º - Será considerada extinta a garantia:

I - Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

II - no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação.

Parágrafo 12º - O garantidor não é parte para figurar em processo administrativo instaurado pela CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

Parágrafo 13º - A CONTRATADA autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no neste documento e no Contrato.

CLÁUSULA DÉCIMA TERCEIRA – DO GERENCIAMENTO E DA FISCALIZAÇÃO DO CONTRATO

Parágrafo 1º – Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

Parágrafo 2º – O recebimento de material de valor superior a R$ 176.000,00 (cento e setenta e seis mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

Parágrafo 3º – A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios e, na ocorrência desta, não implica corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

Parágrafo 4º – O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

Parágrafo 5º - Fica designado como Gestor deste Contrato o servidor **WIRIS SERAFIM DE MENEZES**, conforme Portaria nº 365 - SGI, de 09 de maio de 2023, emitida pela autoridade competente desta Pasta, sendo que a sua substituição poderá se dar mediante nova Portaria, a ser anexada aos autos.

CLÁUSULA DÉCIMA QUARTA – DAS PENALIDADES

Parágrafo 1º – Constituem ilícitos administrativos, sem prejuízo das sanções penais cabíveis, além da prática dos atos previstos nos arts. 81 e 86 da Lei federal nº 8.666, de 21 de junho de 1993, a prática dos atos previstos no art. 7º da Lei federal nº 10.520, de 17 de julho de 2002, ou em dispositivos de normas que vierem a substituí-los, cabendo as sanções previstas nos arts. 86 e incisos I e II do art 87 da Lei federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei federal nº 10.520, de 17 de julho de 2002.

Parágrafo 2º – Nas hipóteses previstas no Parágrafo 1º, o interessado poderá apresentar sua defesa no prazo de 10 (dez) dias úteis, contado da notificação do ato, sendo facultada a produção de todas as provas admitidas em direito, por iniciativa e a expensas daquele que as indicou.

I - Quando necessárias, as provas serão produzidas em audiência previamente designada para este fim.

II - Concluída a instrução processual, a comissão designada ou, quando for o caso, o serviço de registro cadastral, dentro de 15 (quinze) dias, elaborará o relatório final e remeterá os autos para deliberação da autoridade competente para aplicar a penalidade, após o pronunciamento da área jurídica.

Parágrafo 3º – Sem prejuízo do expresso no Parágrafo 1º acima, poderão ser aplicadas, a critério da **CONTRATANTE**, as seguintes penalidades:

I - Ficará impedido de licitar e de contratar com o Estado e será descredenciado no CADFOR, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em Edital e no contrato ou instrumento equivalente, além das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

a) não assinar o contrato ou instrumento equivalente ou a ata de registro de preços;

b) não entregar a documentação exigida no edital;

c) apresentar documentação falsa;

d) causar o atraso na execução do objeto;

e) não mantiver a proposta;

f) falhar na execução do contrato ou instrumento equivalente;

g) fraudar a execução do contrato ou instrumento equivalente;

h) comportar-se de modo inidôneo;

i) declarar informações falsas; e

j) cometer fraude fiscal.

II - A inexecução contratual, inclusive por atraso injustificado na execução do contrato ou instrumento equivalente, sujeitará a **CONTRATADA**, além das penalidades previstas no Parágrafo 1º, a multa de mora, graduada de acordo com a gravidade da infração, obedecidos aos seguintes limites máximos:

a) 10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em firmar o contrato ou instrumento equivalente, ou retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;

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

c) 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento ou serviço não realizado, por cada dia subsequente ao trigésimo.

Nota: A multa a que se refere o Inciso I, não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas em Lei.

III - Para os casos não previstos no Parágrafo 3º - I, a penalidade de suspensão será aplicada, conforme determinação do art. 81 da lei estadual nº 17.928 de 27 de dezembro de 2012.

Parágrafo 4º – As sanções previstas nesta cláusula décima terceira poderão ser aplicadas juntamente às do parágrafo 3º, inciso II).

Parágrafo 5º – Conforme Decreto Estadual nº 9142 de 22 de janeiro de 2018 serão inscritas no CADIN Estadual – Goiás as pessoas físicas ou jurídicas que tenham sido impedidas de celebrar ajustes com a Administração Estadual, em decorrência da aplicação de sanções previstas na legislação pertinente a licitações e contratos administrativos ou em legislações de parcerias com entes públicos ou com o terceiro setor.

Parágrafo 6º – Antes da aplicação de qualquer penalidade será garantido à **CONTRATADA** o contraditório e a ampla defesa. A multa será descontada dos pagamentos eventualmente devidos pela **CONTRATANTE** ou ainda, quando for o caso, cobrada judicialmente.

CLÁUSULA DÉCIMA QUINTA – DA CONCILIAÇÃO E MEDIAÇÃO

Parágrafo 1º – As controvérsias eventualmente surgidas quanto à formalização, execução ou encerramento deste ajuste, serão submetidas à tentativa de conciliação ou mediação no âmbito da Câmara de Conciliação, Mediação e Arbitragem da Administração Estadual (CCMA), na forma da Lei nº 9.307, de 23 de setembro de 1996 e da Lei Complementar Estadual nº 144, de 24 de julho de 2018.

CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO

Parágrafo 1º – A rescisão do presente contrato poderá ser:

I - determinada por ato unilateral e escrito da CONTRATANTE, nos casos enumerados nos incisos I a XII e XVII do art. 78 da Lei Federal nº 8.666/93 e suas alterações posteriores;

II - amigável, por acordo entre as partes, desde que haja conveniência para a **CONTRATANTE**;

III - judicial, nos termos da legislação.

Parágrafo 2º – A inexecução total ou parcial do contrato ensejará a sua rescisão, conforme o disposto nos artigos 77 e 78 da Lei Federal nº 8.666/93 e suas alterações posteriores. Na hipótese de rescisão serão assegurados à **CONTRATADA** o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES GERAIS

Parágrafo 1º - Fica eleito o foro de Goiânia para dirimir as questões oriundas da execução deste contrato.

Parágrafo 2º - E, por estarem justas e acordadas, as partes firmam o presente contrato, assinado eletronicamente, para que produza os necessários efeitos legais.

GABINETE DA SECRETARIA DE ESTADO DA ECONOMIA.

Pela **CONTRATANTE:**

DANILLO CAETANO SOARES CARDOSO

Chefe de Gabinete, Portaria Nº 279/2023, de 28/07/2023

Pela **CONTRATADA**:

DENIS MÁRIO REIS DA SILVA

GLOBAL SEC. TECNOLOGIA & INFORMAÇÃO LTDA

ANEXO I DO CONTRATO

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E RESPEITO ÀS NORMAS DE SEGURANÇA DA INFORMAÇÃO

A empresa **GLOBAL SEC. TECNOLOGIA & INFORMAÇÃO LTDA**, pessoa jurídica com sede em Setor Comercial Norte, Quadra 04 Bloco B, Sala 702, Edifício Varig - Asa Norte, Brasília-DF, CEP: 70.714-020, inscrita no CNPJ/MF com o n.º 31.862.002/0001-13, neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente CONTRATADA, por tomar conhecimento de informações sobre o ambiente computacional da Secretaria de Estado da Economia, denominada CONTRATANTE, aceita as regras, condições e obrigações constantes do presente Termo.

O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva da CONTRATANTE reveladas à CONTRATADA em razão da execução dos serviços objeto do **Contrato nº 024/2023**, doravante denominado simplesmente CONTRATO, bem como assegurar o respeito às normas de segurança vigentes na CONTRATANTE durante a realização dos serviços.

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

A CONTRATADA compromete-se a não reproduzir e/ou dar conhecimento a terceiros, sem a anuência formal e expressa da CONTRATANTE, das informações restritas reveladas.

A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no CONTRATO, as informações restritas reveladas.

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

A CONTRATADA declara conhecer e se compromete a seguir e divulgar entre seus colaboradores envolvidos na execução do CONTRATO a Política de Segurança da Informação da CONTRATANTE e normativos correlatos.

A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo, conforme especificado no instrumento convocatório do processo licitatório que deu origem ao CONTRATO.

A CONTRATADA obriga-se a informar imediatamente a CONTRATANTE qualquer violação das regras de sigilo estabelecidas neste Termo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa da CONTRATANTE, possibilitará a imediata rescisão de qualquer contrato firmado entre a CONTRATANTE e a CONTRATADA sem qualquer ônus para a CONTRATANTE. Nesse caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo administrativo e/ou judicial.

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

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a CONTRATADA assina o presente através de seu representante legal.

Goiânia, ___ de _____ de 202_.

_____

Assinatura do Representante Legal da CONTRATADA

ANEXO II DO CONTRATO

TERMO DE CIÊNCIA INDIVIDUAL DE SIGILO E SEGURANÇA DA INFORMAÇÃO

Eu **nome, nacionalidade, estado civil, cargo inscrito(a) no CPF sob** o nº XXX.XXX.XXX-XX, assumo o compromisso de manter a confidencialidade sobre todas as informações por mim acessadas em função da prestação dos serviços objeto do contrato Nº _____/20__ pela CONTRATADA junto a CONTRATANTE.

Por este termo de confidencialidade e sigilo comprometo-me:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;

3. A não apropriar para mim ou para outrem de material confidencial e/ou sigiloso da tecnologia que venha a ser disponibilizado;

4. A não repassar o conhecimento das informações confidenciais, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações, por meu intermédio, e obrigando-me, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

Informação Confidencial incluirá, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a apresentação da tecnologia, projetos ou produtos.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste Termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste Termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

_____

Assinatura e Data

Documento assinado eletronicamente por **Denis Mario Reis da Silva**, **Usuário Externo**, em 01/08/2023, às 11:46, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **DANILLO CAETANO SOARES CARDOSO**, **Chefe de Gabinete**, em 01/08/2023, às 12:48, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **50141024** e o código CRC **A35738DE**.

Referência: Processo nº 202300004000910 SEI 50141024