Zimbra **lazaro.queiroz@tjam.jus.br**

Network Secure - Proposta Comercial e Documentos de Habilitação - PE 026/2019 (Parte 03)

De : Aline Bandeira <aline.bandeira@networksecure.com.br>
Qui, 25 de jul de 2019 10:26
3 anexos

Assunto : Network Secure - Proposta Comercial e Documentos de Habilitação - PE 026/2019 (Parte 03)

Para : cpl@tjam.jus.br

Cc : G_MAIL_LICITACOES <licitacoes@networksecure.com.br>

Prezado Pregoeiro,

Bom dia!

REF.: PE 026/2019

A Network Secure Segurança da Informação Ltda, inscrita sob o CNPJ 05.250.796/0001-54, vem por meio deste apresentar nossos Documentos de Habilitação e Proposta Comercial, ajustada ao ultimo lance.

(PARTE 03)

Por gentileza, confirmar recebimento deste e-mail.

Atenciosamente,

De: Aline Bandeira
Enviado: quinta-feira, 25 de julho de 2019 11:13
Para: cpl@tjam.jus.br <cpl@tjam.jus.br>
Cc: G_MAIL_LICITACOES <licitacoes@networksecure.com.br>
Assunto: Network Secure - Proposta Comercial e Documentos de Habilitação - PE 026/2019 (Parte 01)

Prezado Pregoeiro,

Bom dia!

REF.: PE 026/2019

A Network Secure Segurança da Informação Ltda, inscrita sob o CNPJ 05.250.796/0001-54, vem por meio deste apresentar nossos Documentos de Habilitação e Proposta Comercial, ajustada ao ultimo lance.

(PARTE 01)

Por gentileza, confirmar recebimento deste e-mail.

Atenciosamente,

PE 0262019 - PROPOSTA COMERCIAL.pdf
6 MB

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

AO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS (TJAM)
COMISSÃO PERMANENTE DE LICITAÇÃO (CPL)

REF.: PREGÃO ELETRÔNICO/SRP Nº. 026/2019-TJAM

ANEXO III – Formulário de Proposta de Preços

RAZÃO SOCIAL: NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA		
CNPJ: 05.250.796/0001-54	**TELEFONE(S):** (85) 3195-2200/0800-073-2222	
ENDEREÇO: RUA CAPITÃO MELO, N° 3373 – JOAQUIM TÁVORA CEP: 60.120-220 FORTALEZA/CE.		
BANCO: BRADESCO - 237	**AGÊNCIA:** 0564-9	**CONTA CORRENTE:** 78934-8
BANCO: BRASIL	**AGÊNCIA:** 3515-7	**CONTA CORRENTE:** 7028-9

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	MÍNIMO POR CONTRATAÇÃO	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	Licença de uso de Software Antivírus para Servidores e Estações de Trabalho, Estações Móveis e Smartphones com atualização continuada por 36 meses. Fabricante: Kaspersky Lab. Versão: Kaspersky Endpoint Security for Business Select.	UND.	4.000	1.000	R$ 59,70	R$ 238.800,00
VALOR TOTAL (R$)						**R$ 238.800,00**

Total: Duzentos e trinta e oito mil e oitocentos reais.

Validade da proposta: 60 (sessenta) dias.

Observação[1]: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

NETWORK
SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

Observação[2]: A proposta terá validade de 60 (sessenta) dias, contados da data de abertura da sessão pública. Decorrido o prazo de validade da proposta, sem convocação para contratação, ficamos liberados dos compromissos assumidos.

Fortaleza, 25 de Julho de 2019.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
RUA CAPITÃO MELO, Nº 3373
JOAQUIM TÁVORA - CEP: 60.120-220
FORTALEZA CEARÁ

Alarico Isaias de Sousa Guimarães
CPF: 620.143.313-91
Representante Legal

NETWORK SECURE
CNPJ: 05.250.796/0001-54

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

ANEXO I - ESPECIFICAÇÕES TÉCNICAS

A solução deve compreender, com total compatibilidade com a atualmente implantada, a atualização das assinaturas de ameaça s e dos softwares componentes, pelo prazo de 36 (trinta e seis) meses.
Todo suporte deve ser prestado por técnico habilitado pelo fabricante do produto com a certificação na solução ofertada, dentro do prazo de validade, ou por outra equivalente que venha a ser anunciada como substituta pelo mesmo.
Como requisitos externos, a solução ofertada deve respeitar os seguintes aspectos legais:

- Constituição Federal, art. 5º, inciso X. Direito à privacidade;
- Constituição Federal, art. 5º, inciso XII. Direito à privacidade das
- comunicações. Sigilo dos dados telemáticos e das comunicações privadas;
- Constituição Federal, art. 5º, inciso XIV. Resguardo do sigilo profissional em
- caso de ofício que exige a ampla confidência no interesse de quem
- confidencia. Sigilo das informações relacionadas à intimidade ou à vida
- privada de alguém;
- Constituição Federal, art. 37, caput. Vinculação da Administração Pública aos
- princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência;
- Consolidação das Leis do Trabalho - CLT, art. 482, alínea "g". Rescisão de
- contrato de trabalho de empregado que viola segredo da empresa;
- Código Penal, art. 151. Dos crimes contra a inviolabilidade de
- correspondência. Proteção do sigilo, integridade e disponibilidade das
- informações de caráter pessoal veiculadas através dos meios de
- comunicação;
- Código Penal, art. 153, § 1º-A. Proteção do sigilo das informações
- classificadas constantes nos sistemas ou bancos de dados da Administração
- Pública;
- Código Penal, art. 154-A. Proteção à violação de equipamentos e sistemas,
- sejam eles conectados ou não à internet, com intenção de destruir dados ou
- informações, ou instalar vulnerabilidades;
- Código Penal, art. 297. Proteção da integridade e autenticidade dos
- documentos públicos;
- Código Penal, art. 305. Proteção da disponibilidade e integridade das
- informações constantes nos órgãos e entidades públicos;
- Lei nº 7.170/83, art. 13. Proteção das informações sigilosas relacionadas à
- segurança nacional;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Lei nº 7.232/84, art. 2o, inciso VIII. Sigilo dos dados relacionados à intimidade,
- vida privada e honra, especialmente dos dados armazenados através de
- recursos informáticos;
- Lei n.º 12.737/12, de 30 de novembro de 2012. Dispõe sobre a tipificação
- criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de
- dezembro de 1940 - Código Penal; e dá outras providências;
- Decreto nº 3.505/00. Institui a Política de Segurança da Informação nos
- órgãos e entidades da Administração Pública Federal. Pressupostos básicos
- da segurança da informação.
- Servidor de Administração e Console Administrativa

  - Compatibilidade:

    - Microsoft Windows Server 2003 SP2 (Todas edições);
    - Microsoft Windows Server 2003 x64 SP2 (Todas edições);
    - Microsoft Windows Server 2008 (Todas edições);
    - Microsoft Windows Server 2008 x64 SP1 (Todas edições);
    - Microsoft Windows Server 2008 R2 (Todas edições);
    - Microsoft Windows Server 2012 (Todas edições);
    - Microsoft Windows Server 2012 R2 (Todas edições);
    - Microsoft Windows Small Business Server 2003 SP2 (Todas edições);
    - Microsoft Windows Small Business Server 2008 (Todas edições);
    - Microsoft Windows Small Business Server 2011 (Todas edições);
    - Microsoft Windows XP Professional SP2 ou superior;
    - Microsoft Windows XP Professional x64 SP2 ou superior;
    - Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
    - Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;
    - Microsoft Windows 7 Professional / Enterprise / Ultimate;
    - Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
    - Microsoft Windows 8 Professional / Enterprise;
    - Microsoft Windows 8 Professional / Enterprise x64;
    - Microsoft Windows 8.1 Professional / Enterprise;
    - Microsoft Windows 8.1 Professional / Enterprise x64.

  - Suportar as seguintes plataformas virtuais:

    - VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0.
    - Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

- KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
- Microsoft VirtualPC 6.0.156.0;
- Parallels Desktop 7 e superior;
- Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
- Citrix XenServer 6.1, 6.2.

○ Características:

▪ A console deve ser acessada via WEB (HTTPS) ou MMC;
▪ Console deve ser baseada no modelo cliente/servidor;
▪ Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
▪ Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
▪ Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
▪ As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
▪ Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
▪ Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
▪ Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
▪ A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
▪ Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
▪ Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
▪ Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
▪ A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
▪ 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;
▪ Capacidade de gerenciar estações de trabalho e servidores de

arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
▪ Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
▪ Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
▪ Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
▪ 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;
▪ A comunicação entre o cliente e o servidor de administração deve ser criptografada;
▪ Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
▪ Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

▪ Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
▪ 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;
▪ Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
▪ Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
▪ 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;
▪ 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 dias, etc;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

▪ 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;
▪ Deve fornecer as seguintes informações dos computadores:

- Se o antivírus está instalado;
- Se o antivírus está iniciado;
- Se o antivírus está atualizado;
- Minutos/horas desde a última conexão da máquina com o servidor
- administrativo;
- Minutos/horas desde a última atualização de vacinas;
- Data e horário da última verificação executada na máquina;
- Versão do antivírus instalado na máquina;
- Se é necessário reiniciar o computador para aplicar mudanças;
- Data e horário de quando a máquina foi ligada;
- Quantidade de vírus encontrados (contador) na máquina;
- Nome do computador;
- Domínio ou grupo de trabalho do computador;
- Data e horário da última atualização de vacinas;
- Sistema operacional com Service Pack;
- Quantidade de processadores;
- Quantidade de memória RAM;
- Usuário(s) logado(s) naquele momento, com informações de
- contato (caso disponíveis no Active Directory);
- Endereço IP;
- Aplicativos instalados, inclusive aplicativos de terceiros, com
- histórico de instalação, contendo data e hora que o software foi
- instalado ou removido;
- Atualizações do Windows Updates instaladas;
- Informação completa de hardware contendo: processadores,
- memória, adaptadores de vídeo, discos de armazenamento,
- adaptadores de áudio, adaptadores de rede, monitores, drives de
- CD/DVD;
- Vulnerabilidades de aplicativos instalados na máquina;

▪ Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
▪ Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

- Alteração de Gateway Padrão;
- Alteração de subrede;
- Alteração de domínio;
- Alteração de servidor DHCP;

- Alteração de servidor DNS;
- Alteração de servidor WINS;
- Alteração de subrede;
- Resolução de Nome;
- Disponibilidade de endereço de conexão SSL;

▪ Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizarse via internet;
▪ Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
▪ Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
▪ Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
▪ 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;
▪ 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;
▪ Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
▪ Capacidade de gerar traps SNMP para monitoramento de eventos;
▪ Capacidade de enviar e-mails para contas específicas em caso de algum evento;
▪ Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
▪ Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
▪ Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
▪ 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;
▪ Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
▪ Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

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

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

▪ Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

▪ Capacidade de diferenciar máquinas virtuais de máquinas físicas.

- Estações Windows

▪ Compatibilidade:

- Microsoft Windows Embedded 8.0 Standard x64;
- Microsoft Windows Embedded 8.1 Industry Pro x64;
- Microsoft Windows Embedded Standard 7* x86 / x64 SP1;
- Microsoft Windows Embedded POSReady 7* x86 / x64;
- Microsoft Windows XP Professional x86 SP3 e superior;
- Microsoft Windows Vista x86 / x64SP2 e posterior;
- Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e
- posterior;
- Microsoft Windows 8 Professional/Enterprise x86 / x64;
- Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- Microsoft Windows 10 Pro / Enterprise x86 / x64.
- ▪ Características:
- Deve prover as seguintes proteções:
- Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou
- modificado;
- Antivírus de Web (módulo para verificação de sites e downloads
- contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e
- enviados, assim como seus anexos);
- Antivírus de Mensagens Instantâneas (módulo para verificação de
- mensagens instantâneas, como ICQ, MSN, IRC, etc);
- O Endpoint deve possuir opção para rastreamento por linha de
- comando, parametrizável, com opção de limpeza;
- Firewall com IDS;
- Autoproteção (contra-ataques aos serviços/processos do antivírus);
- Controle de dispositivos externos;
- Controle de acesso a sites por categoria;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Controle de acesso a sites por horário;
- Controle de acesso a sites por usuários;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos
- instalados;

▪ Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
▪ 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);
▪ Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
▪ Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
▪ Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
▪ Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
▪ Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
▪ Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
▪ Capacidade de verificar somente arquivos novos e alterados;
▪ Capacidade de verificar objetos usando heurística;
▪ Capacidade de agendar uma pausa na verificação;
▪ Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
▪ Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
▪ O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
  - Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

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

- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
- Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- Capacidade de verificar links inseridos em e-mails contra phishings;
- Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
- Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
  - Perguntar o que fazer, ou;
  - Bloquear o e-mail;
    - Apagar o objeto ou tentar desinfectá-lo (de acordo com a
    - configuração pré-estabelecida pelo administrador);
    - Caso positivo de desinfecção:
      - Restaurar o e-mail para o usuário;
    - Caso negativo de desinfecção:
      - Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- Capacidade de filtrar anexos de e-mail, apagando-os ou renomeandoos de acordo com a configuração feita pelo administrador;
- Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- Deve ter suporte total ao protocolo IPv6;
- Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
  - Perguntar o que fazer, ou;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Bloquear o acesso ao objeto e mostrar uma mensagem sobre o
- bloqueio, ou;
- Permitir acesso ao objeto;

▪ O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
▪ Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
▪ Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
▪ Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
▪ 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;
▪ Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
▪ Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
▪ Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
▪ O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

- Filtragem de pacotes: onde o administrador poderá escolher portas,
- protocolos ou direções de conexão a serem
- bloqueadas/permitidas;
- Filtragem por aplicativo: onde o administrador poderá escolher qual
- aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de
- aplicativo ou nome de aplicativo terá acesso a rede, com a
- possibilidade de escolher quais portas e protocolos poderão ser
- utilizados.

▪ Deve possuir módulo que habilite ou não o funcionamento dos

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

seguintes dispositivos externos, no mínimo:

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

▪ 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;
▪ Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
▪ Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
▪ Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
▪ Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;
▪ 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);
▪ Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
▪ 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;
▪ 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;
▪ 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.

- Estações Mac OS X

▪ Compatibilidade:
▪ Mac OS X 10.11 (El Capitan);
▪ Mac OS X 10.10 (Yosemite);
▪ Mac OS X 10.9 (Mavericks).
▪ Mac OS X 10.8 (Mountain Lion)
▪ Mac OS X 10.7 (Lion)

- Características:

▪ Deve prover proteção residente para arquivos (anti-spyware, antitrojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
▪ Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
▪ A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
▪ Deve possuir suportes a notificações utilizando o Growl;
▪ 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);
▪ Capacidade de voltar para a base de dados de vacina anterior;
▪ Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
▪ Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
▪ Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
▪ Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
▪ Capacidade de verificar somente arquivos novos e alterados;
▪ Capacidade de verificar objetos usando heurística;
▪ Capacidade de agendar uma pausa na verificação;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
    - Perguntar o que fazer, ou;
    - Bloquear acesso ao objeto;
        - Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
        - Caso positivo de desinfecção:
        - Restaurar o objeto para uso;
        - Caso negativo de desinfecção:
        - Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
    - Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
    - Capacidade de verificar arquivos de formato de email;
    - Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
    - Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
- Estações de trabalho Linux
    - Compatibilidade:
        - Plataforma 32-bits:
            - Canaima 3;
            - Red Flag Desktop 6.0 SP2;
            - Red Hat Enterprise Linux 5.8 Desktop;
            - Red Hat Enterprise Linux 6.2 Desktop;
            - Fedora 16;
            - CentOS-6.2;
            - SUSE Linux Enterprise Desktop 10 SP4;
            - SUSE Linux Enterprise Desktop 11 SP2;

- openSUSE Linux 12.1;
- openSUSE Linux 12.2;
- Debian GNU/Linux 6.0.5;
- Mandriva Linux 2011;
- Ubuntu 10.04 LTS;
- Ubuntu 12.04 LTS.

Plataforma 64-bits:

- Canaima 3;
- Red Flag Desktop 6.0 SP2;
- Red Hat Enterprise Linux 5.8;
- Red Hat Enterprise Linux 6.2 Desktop;
- Fedora 16;
- CentOS-6.2;
- SUSE Linux Enterprise Desktop 10 SP4;
- SUSE Linux Enterprise Desktop 11 SP2;
- openSUSE Linux 12.1;
- openSUSE Linux 12.2;
- Debian GNU/Linux 6.0.5;
- Ubuntu 10.04 LTS;
- Ubuntu 12.04 LTS.
- Características:

▪ Deve prover as seguintes proteções:
Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
▪ Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir
- tarefas);
- Gerenciamento de Backup: Criação de cópias dos objetos
- infectados em um reservatório de backup antes da tentativa de
- desinfectar ou remover tal objeto, sendo assim possível a
- restauração de objetos que contenham informações importantes;
- Gerenciamento de Quarentena: Quarentena de objetos suspeitos e
- corrompidos, salvando tais arquivos em uma pasta de quarentena;
- Verificação por agendamento: procura de arquivos infectados e
- suspeitos (incluindo arquivos em escopos especificados); análise de
- arquivos; desinfecção ou remoção de objetos infectados.

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

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

  - Servidores Windows
    - Plataforma 32-bits:
    - Microsoft Windows Server 2003 Standard / Enterprise (SP2);
    - Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
    - Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
    - Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
  - Plataforma 64-bits:
    - Microsoft Windows Server 2003 Standard / Enterprise (SP2);
    - Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
    - Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
    - Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
    - Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
    - Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
    - Microsoft Windows Storage Server 2008 R2;
    - Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
    - Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
    - Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
    - Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
    - Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Microsoft Windows Storage Server 2012 (Todas edições);
- Microsoft Windows Storage Server 2012 R2 (Todas edições);
- Microsoft Windows Hyper-V Server 2012;
- Microsoft Windows Hyper-V Server 2012 R2.

- Características:
  - Deve prover as seguintes proteções:
    - Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou
    - modificado;
    - Auto-proteção contra-ataques aos serviços/processos do antivírus;
    - Firewall com IDS;
    - Controle de vulnerabilidades do Windows e dos aplicativos
    - instalados;

- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
  - Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir
  - tarefas);
  - Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
  - Leitura de configurações;
  - Modificação de configurações;
  - Gerenciamento de Backup e Quarentena;
  - Visualização de relatórios;
  - Gerenciamento de relatórios;
  - Gerenciamento de chaves de licença;
  - Gerenciamento de permissões (adicionar/excluir permissões
  - acima);
- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

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

- 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;
- Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
- Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
- Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- Capacidade de verificar objetos usando heurística;
- Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- Capacidade de agendar uma pausa na verificação;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;

- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção:
  - Restaurar o objeto para uso;
- Caso negativo de desinfecção:

▪ Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
▪ Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
▪ Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
▪ Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
▪ Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

○ Servidores Linux

Compatibilidade:

Plataforma 32-bits:
▪ Red Hat Enterprise Linux Server 5.x;
▪ Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
▪ CentOS 6.x (6.0 - 6.6);
▪ SUSE® Linux Enterprise Server 11 SP3;
▪ Ubuntu Server 12.04 LTS;
▪ Ubuntu Server 14.04 LTS;
▪ Ubuntu Server 14.10;
▪ Oracle Linux 6.5;
▪ Debian GNU/Linux 7.5, 7.6, 7.7;
▪ openSUSE 13.1.
▪ Plataforma 64-bits:
▪ Red Hat Enterprise Linux Server 5.x;
▪ Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
▪ Red Hat Enterprise Linux Server 7;
▪ CentOS-6.x (6.0 - 6.6);
▪ CentOS-7.0;
▪ SUSE Linux Enterprise Server 11 SP3;
▪ SUSE Linux Enterprise Server 12;
▪ Novell Open Enterprise Server 11 SP1;
▪ Novell Open Enterprise Server 11 SP2;
▪ Ubuntu Server 12.04 LTS;
▪ Ubuntu Server 14.04 LTS;
▪ Ubuntu Server 14.10;

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

- Oracle Linux 6.5;
- Oracle Linux 7.0;
- Debian GNU/Linux 7.5, 7.6, 7.7;
- openSUSE® 13.1.

○ Características:

Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado).
- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
  - Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir
  - tarefas);
  - Gerenciamento de Backup: Criação de cópias dos objetos
  - infectados em um reservatório de backup antes da tentativa de
  - desinfectar ou remover tal objeto, sendo assim possível a
  - restauração de objetos que contenham informações importantes;
  - Gerenciamento de Quarentena: Quarentena de objetos suspeitos e
  - corrompidos, salvando tais arquivos em uma pasta de quarentena;
  - Verificação por agendamento: procura de arquivos infectados e
  - suspeitos (incluindo arquivos em escopos especificados); análise de
  - arquivos; desinfecção ou remoção de objetos infectados;
- Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

NETWORK
SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA
DA INFORMAÇÃO LTDA
RUA CAPITÃO MELO, Nº 3373
JOAQUIM TÁVORA - CEP 60.120-220
FORTALEZA CEARÁ

Alarico Isaías de Sousa Guimarães
CPF: 620.143.313-91
Representante Legal

NETWORK SECURE
CNPJ: 05.250.796/0001-54

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT

Poderosos controles de endpoints granulares combinados com segurança e gerenciamento proativos de dados e dispositivos móveis

Controles de aplicativos, da Web e de dispositivos, incluindo listas brancas dinâmicas suportadas pelo exclusivo laboratório interno da Kaspersky, adicionam uma nova dimensão para aprofundar a segurança de endpoints. Dispositivos móveis pertencentes à empresas e funcionários (BYOD) também são protegidos, e as plataformas são unificadas para gerenciamento juntamente com todos os endpoints protegidos através do console do Kaspersky Security Center. A proteção de servidores de arquivos garante que infecções não se disseminem para os endpoints protegidos por meio dos dados armazenados.

CONTROLES DE ENDPOINTS

Controle de Aplicativos com as Listras Brancas Dinâmicas — que usam as reputações de arquivos em tempo real entregues pela Kaspersky Security Network, os administradores de TI podem permitir, bloquear ou controlar aplicativos, incluindo a operação de um cenário de listas brancas de 'Negação Padrão' em um ambiente real ou de teste. O Controle de privilégios de aplicativos e a Verificação de vulnerabilidades monitoram aplicativos e restringem aqueles que operam de forma suspeita.

Controle da Web — políticas de navegação podem ser criadas com base em categorias predefinidas ou personalizáveis, garantindo supervisão abrangente e eficiência administrativa.

Controle de dispositivos — políticas de dados granulares que controlam a conexão de armazenamento removível e outros dispositivos periféricos podem ser definidas, programadas e aplicadas usando-se máscaras para implementação simultânea de diversos dispositivos.

SEGURANÇA DE SERVIDORES DE ARQUIVOS

Gerenciados juntamente com segurança de endpoints através do Kaspersky Security Center.

SEGURANÇA MÓVEL:

Poderosa segurança para dispositivos móveis — tecnologias avançadas, proativas e assistidas em nuvem combinam-se para entregar proteção em multicamadas de endpoints móveis em tempo real.

Componentes de proteção da Web, de antispam e de antiphishing aumentam ainda mais a segurança do dispositivo.

Antirroubo remoto — Bloqueio, Limpeza, Localização, Verificação do Chip, Alarme, Retrato e Limpeza total ou seletiva, todos impedem o acesso não autorizado a dados corporativos caso um dispositivo móvel seja perdido ou roubado. A habilitação do administrador e do usuário final, juntamente com o suporte do Google Cloud Management, oferece rápida ativação, se necessário.

Gerenciamento de aplicativos móveis (Mobile Application Management - MAM) — controla o limite do usuário ao executar aplicativos de listas brancas, impedindo a implementação de software indesejado ou desconhecido. '**Empacotamento de aplicativos**'isola dados corporativos em dispositivos pertencentes aos funcionários. Criptografia adicional ou "Limpeza seletiva" podem ser remotamente aplicadas.

Gerenciamento de dispositivos móveis (Mobile Device Management — MDM) — uma interface unificada para dispositivos **Microsoft® Exchange ActiveSync** e **iOS MDM** com implementação de políticas OTA (Over The Air, por conexão sem fio). **Samsung KNOX** com base em dispositivos Android™ também é compatível.

Portal de autoatendimento — permite o auto registro na rede de dispositivos aprovados de propriedade dos funcionários com instalação automática de todos os certificados e chaves necessários e a ativação de emergência por usuários / proprietários de recursos antirroubo, reduzindo a carga de trabalho administrativa de TI.

O Kaspersky Endpoint Security for Business - SELECT também inclui todos os componentes do nível CORE.

Kaspersky® Endpoint Security for Business

Select

Ready for GDPR

Kaspersky Endpoint Security for Business Select provides HuMachine™-based protection for a wide range of platforms – including Linux servers and endpoints. It delivers multi-layered security that detects suspicious behavior and blocks threats, including ransomware. Cloud-enabled controls reduce your exposure to attacks – and mobile management features help you to protect data on mobile devices.

The protection and management capabilities you need

Kaspersky Lab has built powerful enterprise-class features into the progressive tiers of our offerings. We've made sure that the technology is uncomplicated and flexible enough for any-sized business to use.

Which tier is right for you?

- **SELECT**
- ADVANCED
- TOTAL

Multiple protection layers for

- Windows, Linux and Mac
- Windows and Linux servers
- Android and other mobile devices
- Removable storage

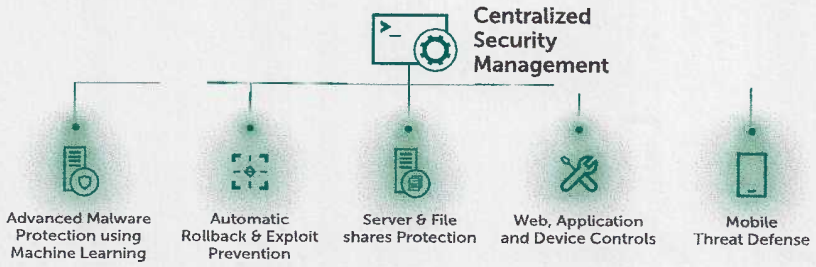
Unparalleled security against

- Software exploits
- Ransomware
- Mobile malware
- Advanced threats
- Fileless threats
- PowerShell & script-based attacks
- Web threats

Features included

- Anti-Malware next level
- Vulnerability Assessment
- Security Policy Adviser
- AI-based learning
- AMSI support new
- Encrypted traffic scanning new
- Process isolation
- Exploit Prevention and Rollback
- Firewall and OS firewall management
- Cloud-assisted protection
- Integrated EDR agent
- SIEM integration via Syslog new
- Application Control
- Web and Device Controls
- Server and containers protection next level
- Windows Linux subsystem support new
- Mobile Threat Defense next level
- Reporting

See our webpages for details here.



Next Generation protection and control for every endpoint

One management console

From the 'single pane of glass' management console, administrators can view and manage the entire security landscape and apply your chosen security policies to every endpoint in your business. This helps deploy security rapidly and with minimum interruption or fuss, using a wide range of preconfigured scenarios.

Agile, adaptive security

The product is designed to work within any IT environment. It employs a full stack of proven and Next Gen technologies an to prevent detected attacks; built-in sensors and integration with Endpoint Detection and Response (EDR) enable the capture of large volumes of data to discover even the most obscure, sophisticated cyberattacks.

Customer satisfaction assured

Our strong focus on R&D means that our products deliver the security you need. Decision-makers like you consistently express outstanding levels of satisfaction with the results, as regularly confirmed in independent surveys and reports.

Key features

Core features

Exploit Prevention
Prevents malware executing and exploiting software, delivering an extra layer of protection against unknown, zero-day threats.

Behavioral Detection and Automatic Rollback
Identifies and protects against advanced threats, including ransomware, fileless attacks and admin account takeovers. Behavior Detection blocks attacks, while Automatic Rollback reverses any changes already made.

Protection against encryption for shared folders
A unique anti-cryptor mechanism can block the encryption of files on shared resources conducted by a malicious process running on another machine on the same network.

Network Threat Protection
Malware using a buffer-overrun attack can modify a process already running in the memory and in this way execute malicious code. Network Threat Protection identifies network attacks and stops them in their tracks.

Web console
To improve fault-tolerance you can deploy our web console to centrally manage both physical and virtual machines, not only in Amazon but also in Microsoft Azure cloud environments.

Mobile security features

Innovative anti-malware technologies
Combined ML-based, proactive and cloud-assisted detection result in real-time protection. A Web Protection, on-demand and scheduled scans increase the security.

Deployment Over the Air (OTA) provisioning
Delivers the ability to pre-configure and deploy applications centrally using SMS, email and PC.

Remote anti-theft tools
SIM-Watch, Remote Lock, Wipe and Find - all prevent unauthorized access to corporate data if a mobile device is lost or stolen.

Application Control for mobile devices
Application Control protects data on installed software and enables administrators to enforce the installation and usage of specific applications.

Cloud-enabled endpoint controls

Application Control
Reduces your exposure to attack, giving total control over what software can run when on PCs, powered by Dynamic Whitelisting from our in-house laboratory. Default Allow and Default Deny scenarios are supported.

Dynamic whitelisting
For a better applications categorization, Application Control uses a Dynamic Whitelisting Database developed by Kaspersky Lab, based on systemizing knowledge of legitimate software.

Device Control
This feature allows users to set, schedule and enforce data policies that control removable storage and other peripheral devices – connected to a USB or any other bus type.

Host Intrusion Prevention (HIPS)
Regulates access to sensitive data and recording devices by using our local and cloud (Kaspersky Security Network) reputation databases, without affecting the performance of authorized applications.

Support and Professional Services

Professional help is available whenever you need it. Operating in more than 200 countries, from 34 offices worldwide, we have you covered 24/7/365. Take advantage of our Premium Support packages (MSA), or call on our Professional Services to ensure that you derive maximum benefit and ROI from your Kaspersky Lab security installation.

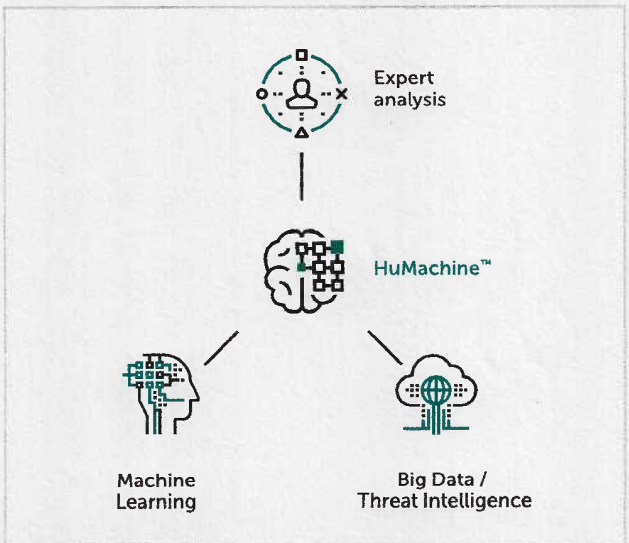
See for yourself

Experience True Cybersecurity for yourself! Visit this page **to trial the full version** of Kaspersky Endpoint Security for Business.

Kaspersky Lab
Find a partner near you: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
IT Security News: **business.kaspersky.com/**
Our unique approach: **www.kaspersky.com/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com



NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

AO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS (TJAM)
COMISSÃO PERMANENTE DE LICITAÇÃO (CPL)

REF.: PREGÃO ELETRÔNICO/SRP Nº. 026/2019-TJAM

ANEXO I – Declaração conjunta de cumprimento das condições de habilitação e de inexistência de impedimento legal para licitar ou contratar com a Administração Pública

A **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, inscrito(a) no CNPJ n°. **05.250.796/0001-54**, por intermédio de seu representante legal o(a) Sr.(a) **JOSE MURILO CIRINO NOGUEIRA JUNIOR**, portador(a) da Carteira de Identidade nº **99010123694** e do CPF nº **648.711.503-72**, **DECLARA**:

1) que está ciente e concorda com as condições contidas no edital e seus anexos, e que cumpre plenamente os requisitos de habilitação definidos no edital;

2) que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

3) que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal.

Fortaleza, 25 de Julho de 2019.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
RUA CAPITÃO MELO, Nº 3373
JOAQUIM TÁVORA - CEP: 60.120-220
FORTALEZA – CEARÁ

Jose Murilo Cirino Nogueira Junior
CPF: 648.711.503-72
Representante Legal

NETWORK SECURE
CNPJ: 05.250.796/0001-54

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

AO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS (TJAM)
COMISSÃO PERMANENTE DE LICITAÇÃO (CPL)

REF.: PREGÃO ELETRÔNICO/SRP Nº. 026/2019-TJAM

ANEXO II – Declaração de elaboração independente de proposta

JOSE MURILO CIRINO NOGUEIRA JUNIOR, inscrito no CPF sob nº **648.711.503-72** e portador da Cédula de Identidade de nº **99010123694**, brasileiro, casado residente e domiciliado na Av. Coronel Miguel Dias, 1010 - Torre A, Apto 1301 Água Fria - Fortaleza/CE - CEP: 60.810-160, como representante devidamente constituído da **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, inscrita sob o CNPJ: **05.250.796/0001-54**, situada na Rua Capitão Melo, 3373 – CEP: 60120-220 – Fortaleza/CE doravante denominada NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, em atendimento ao disposto no edital do Pregão Eletrônico/SRP nº. 026/2019, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta anexa foi elaborada de maneira independente pela NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico/SRP nº. 026/2019, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico/SRP nº. 026/2019, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico/SRP nº. 026/2019 quanto a participar ou não da referida licitação;

d) que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a ou discutido com qualquer outro participante

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

potencial ou de fato do Pregão Eletrônico/SRP nº. 026/2019 antes da adjudicação do objeto da referida licitação;

e) que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do Tribunal de Justiça do Amazonas antes da abertura oficial das propostas; e

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Fortaleza, 25 de Julho de 2019.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
RUA CAPITÃO MELO, Nº 3373
JOAQUIM TÁVORA - CEP: 60.120-220
FORTALEZA CEARÁ

Jose Murilo Cirino Nogueira Junior
CPF: 648.711.503-72
Representante Legal

NETWORK SECURE
CNPJ: 05.250.796/0001-54

NETWORK SECURE
MAIS PROTEÇÃO A CADA INFORMAÇÃO.

AO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS (TJAM)
COMISSÃO PERMANENTE DE LICITAÇÃO (CPL)

REF.: PREGÃO ELETRÔNICO/SRP Nº. 026/2019-TJAM

DECLARAÇÃO DE EMPRESA DE PEQUENO PORTE

A **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, inscrita no CNPJ nº **05.250.796/0001-54,** por intermédio de seu representante legal o(a) Sr(a) **JOSE MURILO CIRINO NOGUEIRA JUNIOR**, portador(a) da Carteira de Identidade nº **99010123694** e CPF nº: **648.711.503-72**, DECLARA, sob as sanções administrativas cabíveis e sob as penas da lei, ser:

( ) Microempresa

(X) Empresa de Pequeno Porte

( ) Indicar/Detalhar a existência de restrição da documentação exigida para fins de habilitação (art.30, §4º do Decreto nº 13.735 de 18 de junho de 2016.

Nos termos da legislação vigente, não possuindo nenhum dos impedimentos previstos no § 4º do artigo 3º da Lei Complementar nº 123/06.

Fortaleza, 25 de Julho de 2019.

05.250.796/0001-54
NETWORK SECURE SEGURANÇA
DA INFORMAÇÃO LTDA
RUA CAPITÃO MELO, Nº 3373
JOAQUIM TÁVORA - CEP 60.120-220
FORTALEZA — CEARÁ

Jose Murilo Cirino Nogueira Junior
CPF: 648.711.503-72
Representante Legal

NETWORK SECURE
CNPJ: 05.250.796/0001-54

Av. Queiroz Filho, 1.700 - Torre A
São Paulo SP
Conjunto 803

Tel: (11) 4302 4225
CEP: 05319 000
www.kaspersky.com

KASPERSKY lab

São Paulo, de 11 Junho de 2019

Prezados(as) Senhores(as)

A Kaspersky Lab Soluções Seguras Brasil Ltda., com sede em São Paulo-SP, declara que a empresa: **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, inscrita no CNPJ sob n° 05.250.796/0001-54, é uma revenda certificada e credenciada, membro Platinum do Programa de Parceria da Kaspersky, tendo profissionais certificados para a prestação de serviços de implantação, instalação, configuração e prestação de suporte técnico das soluções e para ministrarem treinamento referente às soluções.

Por motivos internos referente às políticas de treinamento e atualização do programa de canais da Kaspersky Lab, esta declaração tem validade até 31 de Dezembro de 2019.

Com a intenção de gerar confiança e estabelecer um relacionamento duradouro e de sucesso com sua respeitada instituição, coloco-me à sua inteira disposição para quaisquer esclarecimentos ou comentários.

Atenciosamente,

Roberto Rebouças
Diretor Geral Brasil

Kaspersky Lab S. S. Brasil Ltda
CNPJ: 11.139.530/0001-31

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza - Ce.
26 JUN. 2019

SELO DE AUTENTICIDADE 03
AUTENTICAÇÃO Nº IA 018237 KYVO

3º OFÍCIO DE NOTAS -TABELIONATO PERGENTINO MAIA
Av. Padre Antonio Tomás, 920 - Aldeota - Fortaleza-CE
Tel: (85) 3304-9444 - CEP: 60140-160 - CNPJ:06.572.994/0001-05

Roberto Fiuza Maia
Notário

Rodrigo de Paula Pessoa Maia
Bernardo de Paula Pessoa Maia
Andréa Pamplona Maia
Janaina Carvalho Gois
Substitutos

Livro: **0488**

Folha: **081**

Prot.:**083547**

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
1º Traslado
ABR. 2019
TABELIÃO - ESC. AUTORIZADO - ESC. AUTORIZADO - ESC. SUBSTITUTA - ESC. AUTORIZADO - ESC. AUTORIZADO

PROCURAÇÃO BASTANTE que faz e assina, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.,** na forma abaixo:

Saibam quantos este público instrumento virem que, aos 5 (cinco) dias do mês de fevereiro do ano de 2019 (dois mil e dezenove), nesta cidade de Fortaleza, Capital do Estado do Ceará, República Federativa do Brasil, na Rua Capitão Melo, nº 3373, Bairro Joaquim Távora, onde eu, Sabrina Carvalho Gois, escrevente autorizada, vim em diligência, estava o sócio administrador, adiante qualificado, da ora outorgante **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.,** pessoa jurídica de direito privado, com sede nesta Capital, na Rua Capitão Melo, nº 3373, Bairro Joaquim Távora, inscrita no CNPJ sob o nº 05.250.796/0001-54, neste ato representada por seu sócio administrador JOSE MURILO CIRINO NOGUEIRA JUNIOR, brasileiro, casado, empresário, residente e domiciliado nesta Capital, na Av. Coronel Miguel Dias, nº 1010, Aptº 1301, Torre A, Bairro Água Fria, portador da CNH nº 1226678851-DETRAN-CE, registro nº 00809571455, onde consta a cédula de identidade nº 99010123694-SSP-CE, inscrito no CPF sob o nº 648.711.503-72, o presente reconhecido por mim, pela verificação dos documentos supra exibidos em seus originais, de cuja(s) identidade(s) e capacidade jurídica dou fé. Então pela outorgante, me foi dito, que nomeava e constituía seu bastante procurador, **ALARICO ISAIAS DE SOUSA GUIMARÃES,** brasileiro, casado, provedor de soluções, residente e domiciliado nesta Capital, na Av. Paisagística, nº 06, Apt 407, Bloco 01, Bairro Itaperi, portador da CNH nº 1407122265-DETRAN-CE, registro nº 03035138190, onde consta a cédula de identidade nº 96002206506-SSPDS-CE, inscrito no CPF sob o nº 620.143.313-91, a quem confere poderes amplos e ilimitados para praticar todos os atos relativos à contrato em geral, responder a repartições públicas e privadas, licitação, podendo formular ofertas escritas e verbais, negociar preços, assinar documentos de habilitação, atas e instrumentos de compromisso, interpor recursos e renunciar o direito de propô-los, retirar login e senha, preenchendo e assinando todas as formalidades legais para viabilidade do mesmo, praticar todos os demais atos pertinentes ao certame em nome da empresa outorgante, assistir a abertura de propostas, fazer impugnações, reclamações, protestos e recursos, assinar propostas, atas, documentos necessários, fazer novas propostas, rebaixos, descontos, receber em devolução documentos pertencentes à outorgante, assinar contratos, acordar, discordar, desistir de recursos, juntar e retirar documentos, prestar esclarecimentos, informações, assinar requerimentos e petições, podendo tudo requerer e assinar para o bom e fiel cumprimento do presente mandato, o que será dado por bom, firme e valioso e preencher todas as formalidades legais, **sendo vedado o substabelecimento. O PRESENTE INSTRUMENTO TEM VÁLIDADE DE 24 (VINTE E QUATRO) MESES A CONTAR DESTA DATA. (FEITO SOB MINUTA). O(s) nome(s) e dados do(s) procurador(es) e os elementos relativos ao objeto do presente instrumento foram fornecidos e conferidos pelo(s) outorgante(s), que por eles se responsabiliza(m).** E como assim o disse, do que dou fé,

lavrei este instrumento, que lido e achado conforme, aceita e assina. Eu, (a.) Sabrina Carvalho Gois, escrevente autorizada, a lavrei. Eu, Rodrigo de Paula Pessoa Maia, escrevente substituto, a subscrevo. (a.a.) Rodrigo de Paula Pessoa Maia. **JOSE MURILO CIRINO NOGUEIRA JUNIOR**. Está conforme o original. Dou fé. Selo nº AD470739, AE247747. Trasladada em seguida. VÁLIDO SOMENTE COM SELO DE AUTENTICIDADE.

CARTÓRIO PERGENTINO MAIA
Fabiola da Penha Freire
Escrevente Autorizada
Fortaleza - Ceará

Subscrevo e assino

Em testemunho (X) da verdade.

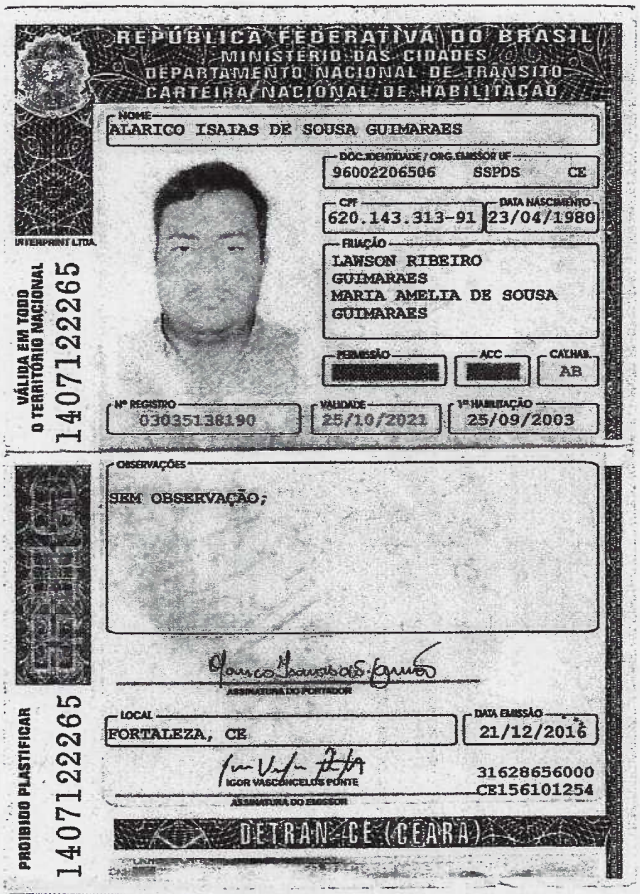
TRIBUNAL DE JUSTIÇA
PROVIMENTO 08/2014

EMOLUMENTOS: R$ 36,05
FERMOJU: R$ R$ 4,22
SELO: R$ R$ 5,91
ISS: R$ 1,80
FAADEP: R$ 1,80
FRMMP: R$ R$ 1,80

06
NOTARIAL II
Procurações e Escrituras sem Valor Declarado
Nº AD 470739
KLMT

01
REGISTRAL
Distribuição
Nº AE 247747
HTUW

Certifico que a presente cópia fotográfica é reprodução fiel do original. Dou fé
Fortaleza - Ce.
18 ABR. 2019
BERTO PINZA MAIA - TABELIÃO



REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DAS CIDADES
DEPARTAMENTO NACIONAL DE TRÂNSITO
CARTEIRA NACIONAL DE HABILITAÇÃO

NOME
ALARICO ISAIAS DE SOUSA GUIMARAES

DOC. IDENTIDADE / ORG. EMISSOR UF
96002206506 SSPDS CE

CPF
620.143.313-91

DATA NASCIMENTO
23/04/1980

FILIAÇÃO
LAWSON RIBEIRO GUIMARAES
MARIA AMELIA DE SOUSA GUIMARAES

PERMISSÃO

ACC

CAT.HAB.
AB

Nº REGISTRO
03035138190

VALIDADE
25/10/2021

1ª HABILITAÇÃO
25/09/2003

OBSERVAÇÕES
SEM OBSERVAÇÃO;

ASSINATURA DO PORTADOR

LOCAL
FORTALEZA, CE

DATA EMISSÃO
21/12/2016

IGOR VASCONCELOS PONTE
ASSINATURA DO EMISSOR

31628656000
CE156101254

DETRAN CE (CEARA)

UNIFINGERPRINT LTDA.

VÁLIDA EM TODO O TERRITÓRIO NACIONAL

1407122265

PROIBIDO PLASTIFICAR

1407122265

SELO DE AUTENTICIDADE
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
AUTENTICAÇÃO
Nº HZ 287187 VNWG

03

Certifico que a presente cópia fotostática é a reprodução fiel do original. Dou fé.
Fortaleza - CE.
22 MAIO 2019

ROBERTO FIUZA MAIA - TABELIÃO
MARCIO GOULART DE AQUINO - ESC. AUTORIZADO
CLAUDIA CARNEIRO DA SILVA - ESC. AUTORIZADA
CONCEIÇÃO DE MARIA CORREIA MAIA - ESC. SUBSTITUTA
MARIA MARLY MOTA RIBEIRO - ESC. AUTORIZADA