CONTRATO PARA FORNECIMENTO DA RENOVAÇÃO DE ASSINATURA DE 2.500 (DUAS MIL E QUENHENTOS) LICENÇAS DE USO DE SOFTWARE ANTIVÍRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT BRAZILIAN, COM GARANTIA MÍNIMA DE 36(TRINTA E SEIS) MESES, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA E A EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.(PROCESSO ADMINISTRATIVO N.º 8500753-86.2018.8.06.0000).

CT N.º 04/2018

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**, com sede na Av. General Afonso Albuquerque Lima, s/n, Bairro Cambeba, em Fortaleza-CE, inscrito no CNPJ/MF sob o nº 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou CONTRATANTE, neste ato representado por seu Presidente, Desembargador Francisco Gladyson Pontes e por sua Secretária de Tecnologia da Informação, Dra. Denise Maria Norões Olsen, e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, com sede na Rua Capitão Melo, nº 3373, Bairro Joaquim Távora, em Fortaleza/CE, inscrita no CNPJ/MF sob o nº 05.250.796/0001-54, neste ato representada por seu Diretor, José Murilo Cirino Nogueira Júnior, portador da cédula de identidade nº 99010123694-SSP-CE e inscrito no CPF/MF nº 648.711.503-72, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei nº 10.520/2002 e pela Lei n.º 8.666/93, e suas alterações posteriores.

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da Licitação realizada sob a modalidade Pregão Eletrônico nº 31/2016, devidamente homologada pelo Presidente do Tribunal de Justiça do Estado do Ceará, tudo de conformidade com as disposições da Lei Federal nº 10.520/2002 e a Lei Federal nº 8.666, de 21 de junho de 1993, e suas alterações, na Ata de Registro de Preços nº 05/2017, e em conformidade com o Processo Administrativo nº 8500753-86.2018.8.06.0000.

CLÁUSULA SEGUNDA – DO OBJETO

O Objeto deste Instrumento consiste no **fornecimento da renovação de assinatura de 2.500 (duas mil e quinhentas) licenças de uso de software antivírus *Kaspersky Endpoint Security for Business - Select Brazilian***, conforme especificações contidas no Edital do Pregão Eletrônico nº 31/2016, bem como no(s) seu(s) Anexo(s), todos parte(s) integrante(s) deste Contrato.

CONFERIDO

PARÁGRAFO ÚNICO – DOCUMENTAÇÃO COMPLEMENTAR

A prestação do objeto obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Instrumento, no que não o contrarie.

CLÁUSULA TERCEIRA – DA DESCRIÇÃO DA SOLUÇÃO

ITEM	DESCRIÇÃO	UNID. MEDIDA	QTD	VLAOR UNITÁRIO	VALOR TOTAL
1	Renovação de licenças Kaspersky Endpoint Security for Business - Select Brazilian com 36 meses de garantia. **Part Number: KL4863KAYTD**	UNIDADE	2500	R$ 65,00	R$ 162.500,00
			TOTAL GLOBAL	**R$ 162.500,00**	

I - Considerações Gerais

a. Os bens/serviços deverão atender, no mínimo, às especificações descritas no ANEXO I – **Especificações Técnicas.**

II - Requisitos da Solução

a. Requisitos de Manutenção

a.1. Da Garantia e Suporte Técnico

a.1.1. A garantia dos produtos e suporte técnico remoto deverão ser fornecidos durante a vigência do contrato sem quaisquer custos adicionais ao TJCE;

a.1.2. A garantia dos produtos deverá ser fornecida pelo fabricante do Software **Kaspersky Endpoint Security for Business - Select Brazilian**, que é a atual solução de antivírus do TJCE;

a.1.3. O prazo de vigência da garantia dos produtos oferecidos será no mínimo de 36 (trinta e seis) meses, contados a partir da emissão do respectivo termo de recebimento definitivo;

a.1.4. Durante o período de garantia dos produtos, deverão ser fornecidos gratuitamente: correções, novas versões, releases ou atualizações mais recentes comercialmente disponíveis dos produtos e suporte técnico remoto;

a.1.5. O suporte técnico remoto deverá ser prestado diretamente pela CONTRATADA e deverá contemplar(no mínimo): atendimento telefônico para solução de problemas de funcionamento/configuração do software antivírus adquirido;

a.1.5.1. O tempo de início de atendimento telefônico, será no máximo de 01(uma) hora após a abertura do chamado técnico;

a.1.6. O atendimento remoto será prestado no regime 8x5 (oito horas por dia cinco dias por semana em dias úteis e no horário comercial);

a.1.7. O número de solicitações de suporte por telefone será ilimitado;

a.1.8. Forma de acesso do CONTRATANTE à CONTRATADA: por telefone e/ou por meio eletrônico, via web ou por e-mail;

a1.9. Forma de resposta da CONTRATADA ao CONTRATANTE: por telefone e/ou por meio eletrônico, via web ou por e-mail;

a.1.10. Os chamados para atendimento telefônico deverão ser abertos e registrados diretamente com a CONTRATADA e gerenciados pela mesma através de atendimento telefônico, web e/ou por e-mail, fornecendo neste momento o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos.

CONFERIDO

CLÁUSULA QUARTA – DAS OBRIGAÇÕES

São obrigações das partes neste Contrato:

I - DO CONTRATANTE:

a) Efetuar os pagamentos devidos à CONTRATADA, nas formas estabelecidas neste contrato;
b) Comunicar à CONTRATADA qualquer anormalidade ocorrida na execução do objeto, diligenciando para que eventuais irregularidades ou falhas sejam plenamente corrigidas;
c) Apurar a qualidade dos serviços contratados, determinando o que for necessário à regularização das faltas ou defeitos observados, aferindo as sanções cabíveis;
d) Receber provisória e definitivamente o produto ofertado nas formas definidas neste Contrato;
e) Notificar, por escrito, à CONTRATADA da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e ampla defesa.

II - DA CONTRATADA:

a) Fornecer ao TJCE os produtos/serviços, objeto deste Contrato, de acordo com as especificações técnicas (**Anexo I**) e condições constantes no instrumento convocatório e seus anexos, no prazo determinado;
a.1. Eventual atraso na entrega do objeto deste Contrato deverá ser devidamente justificado, devendo a Administração analisar essa justificativa;
b) Comunicar ao CONTRATANTE qualquer anormalidade que interfira no bom andamento do contrato;
c) Arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado ao CONTRATANTE e a terceiros, por sua culpa, ou em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção do contrato, exceto quando isto ocorrer por exigência do CONTRATANTE, ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 24 (vinte e quatro) horas após a sua ocorrência;
d) Efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente Contrato, bem como, observar e respeitar as Legislações Federal, Estadual e Municipal, relativas ao objeto do contrato;
e) Emitir notas fiscais/faturas de acordo com a Legislação, contendo descrição completa dos serviços;
f) Manter durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste Contrato;
g) Em até 02 (dois) dias após a emissão do TRD (Termo de Recebimento Definitivo), a CONTRATADA deverá apresentar documentação cuja origem seja exclusivamente do fabricante dos softwares que permita identificar claramente o início e o fim do período de garantia das licenças renovadas e/ou adquiridas conforme o Edital de Pregão Eletrônico e seus anexos. Serão aceitos para comprovação do período de garantia as informações obtidas na console de gerenciamento do software, sítio do fabricante na Internet ou declaração do fabricante;
h) Comprovar, durante toda a execução do contrato, a regularidade do FGTS, INSS, débitos trabalhistas, Fisco Federal, Estadual e Municipal;
i) A CONTRATADA deverá tratar como "confidenciais" quaisquer informações, a que tenha acesso para execução do objeto, não podendo revelá-las ou facilitar sua disponibilização a terceiros. A obrigação permanecerá válida durante o período de vigência contratual e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA;
i.1. As obrigações e conhecimentos sobre os requisitos de segurança serão ratificados por CONTRATADA e CONTRATANTE em documentos posteriores, quando da contratação, nos

CONFERIDO
NTS
30

termos de compromisso e de ciência – ANEXO IV e ANEXO V respectivamente.

CLÁUSULA QUINTA – FORMA DE ACOMPANHAMENTO DO CONTRATO

ID	Evento	Forma de Acompanhamento
1	Atesto da entrega das licenças de renovação e/ou aquisição do antivírus *Kaspersky Endpoint Security for Business - Select Brazilian*	O CONTRATANTE verificará a entrega das licenças e a sua validade, após a entrega da solução conforme descrito na Cláusula Nona, para posteriormente emitir o termo de recebimento definitivo, caso o produto ofertado esteja conforme as especificações exigidas neste Contrato.

CLÁUSULA SEXTA – PAPEIS E RESPONSABILIDADES

ID	Papel	Entidade	Responsabilidade
1	Fiscal Técnico	Diretor(a) da Divisão de Suporte Técnico	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os critérios de aceitação definidos em contrato; Identificação de não conformidade com os termos contratuais; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato); Comunicar por escrito, ao gestor do contrato, qualquer falta cometida pela empresa CONTRATADA, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar à aplicação de sanção ou à rescisão contratual; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato; Realizar pessoalmente a medição dos serviços contratados; Recusar serviço ou fornecimento irregular ou em desacordo com condições previstas em edital, na proposta da CONTRATADA e no contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados; Averiguar se é o contratado quem executa o contrato e certificar-se de que não existe cessão ou subcontratação fora das hipóteses legais;

CONFERIDO

			Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Atestar a efetiva realização do objeto contratado para fins de pagamento das faturas correspondentes.
2	Fiscal Requisitante do Contrato	Chefe do Serviço de Segurança da Informação	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os critérios de aceitação definidos em contrato, junto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Verificação da manutenção da necessidade, economicidade e oportunidade da contratação; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato), em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços, em conjunto com o Fiscal Técnico; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Comunicar por escrito, ao gestor do contrato, qualquer falta cometida pela empresa CONTRATADA, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão

CONFERIDO

			levar a aplicação de sanção ou à rescisão contratual, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato, em conjunto com o Fiscal Técnico.
3	Fiscal Administrativo	Diretor (a) da Divisão de Gestão Administrativa de TI	Certificar-se do correto cálculo e recolhimento das obrigações trabalhistas, previdenciárias e tributárias decorrentes do contrato; Efetuar o controle da vigência, realizando comunicado ao fiscal técnico em tempo hábil, uma vez que este deverá controlar os prazos de execução, necessidades de prorrogações ou nova contratação, ficando o fiscal administrativo responsável pelo controle da época de reajustamento dos preços contratados, tomando as providências cabíveis em tempo hábil junto à Divisão Central de Contratos e Convênios do TJCE, quando necessário; Verificar se a empresa CONTRATADA cumpriu com a garantia prevista no contrato.
4	Gestor do Contrato	Secretário(a) de Tecnologia da Informação	Manter registro próprio, atualizado, das ocorrências relacionadas à execução do contrato; Acompanhar o cumprimento do cronograma de execução e dos prazos previstos; Determinar à CONTRATADA a regularização das falhas ou defeitos observados, assinalando prazo para correção; Relatar, por escrito, à autoridade competente do órgão responsável, a inobservância de cláusulas contratuais ou quaisquer ocorrências que possam trazer dificuldades, atrasos, defeitos e prejuízos à execução da avença, em especial os que ensejarem a aplicação de penalidades; Comunicar à autoridade competente do órgão responsável, apresentando as devidas justificativas, a eventual necessidade de acréscimos ou supressões de serviços, materiais ou equipamentos, identificadas no curso das atividades de fiscalização; Solicitar à CONTRATADA a substituição de empregado ou preposto da CONTRATADA e aprovar, previamente, mediante termo juntado ao processo, a substituição de iniciativa da CONTRATADA, quando assim exigir o contrato; Receber, definitivamente, por meio de ateste na nota fiscal/fatura ou documento equivalente, devidamente discriminado, obras, serviços e materiais; Acompanhar o prazo de vigência do contrato e manifestar-se, quando provocado pela Administração, sobre os aspectos de oportunidade, conveniência, razoabilidade e economicidade administra-

CONFERIDO

			tiva de se realizar alteração, prorrogação ou rescisão do contrato, anexando, quando for o caso, documentação comprobatória.

CLÁUSULA SÉTIMA – METODOLOGIA DE AVALIAÇÃO DA QUALIDADE

Etapa/Fase/Item	Método de Avaliação
Durante o prazo de vigência do contrato	Os serviços deverão ser avaliados com o monitoramento dos chamados técnicos abertos pela CONTRATANTE e a verificação da qualidade do atendimento e cumprimento do NMSE(Nível Mínimo de Serviço Exigido).

CLÁUSULA OITAVA – NÍVEL MÍNIMO DE SERVIÇO EXIGIDO

ID	Etapa/Fase/Item	Indicador	Valor Mínimo Aceitável
1	Da Entrega das Licenças	Dias	Máximo de 30 dias corridos contados a partir do recebimento da Ordem de Fornecimento de Bens (OFB) pela CONTRATADA.
2	Período de Garantia e Suporte Técnico Remoto ao Software Antivírus	Meses	No mínimo 36 meses após a emissão do respectivo termo de recebimento definitivo.
3	Regime de Atendimento do Suporte ao Software Antivírus	Horas/Dias da semana	8x5 (8 horas por dia cinco dias por semana em dias úteis e no horário comercial), para atendimento remoto.
4	Prazo para início de atendimento telefônico(remoto)	Horas	No máximo 01(uma) hora após abertura do chamado

CLÁUSULA NONA – PRAZOS E CONDIÇÕES

O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento, nos endereços, prazos e horários previstos nos incisos seguintes:

I - O prazo de entrega da renovação/aquisição de licenças de antivírus *Kaspersky Endpoint Security for Business - Select Brazilian* será de no máximo 30 (trinta) dias corridos, contados a partir do recebimento da Ordem de Fornecimento de Bens (OFB) pela CONTRATADA. A entrega dar-se-á através do envio por e-mail à diretoria do Departamento de Infraestrutura de TI e/ou à diretoria da Divisão de Suporte Técnico do TJCE, do(s) arquivo(s) contendo a(s) chave(s) das licenças de renovação e/ou aquisição adquiridas, comprovada conforme **alínea "g", inciso II da Cláusula Quarta**;

II - O Tribunal de Justiça do Estado do Ceará receberá provisoriamente (Termo de Recebimento Provisório - ANEXO II) o produto ofertado no ato da entrega, conforme citado na **alínea "g", inciso II da Cláusula Quarta**, e definitivamente (Termo de Recebimento Definitivo – ANEXO III) em um prazo não superior a 10 (dez) dias corridos, contados a partir da data de assinatura do Termo de Recebimento Provisório, verificando a conformidade do produto ofertado quanto às exigências do ANEXO I – Especificações Técnicas e o que foi proposto pela

CONFERIDO

CONTRATADA;

III - Na hipótese de desaprovação do produto ofertado, a CONTRATADA deverá substituí-lo no prazo máximo de 15(quinze) dias corridos, a contar da data do recebimento da comunicação do ocorrido através de ofício pelo Tribunal de Justiça do Estado do Ceará;

IV - A concessão do prazo estabelecido para substituição não obsta a aplicação das sanções administrativas previstas no contrato.

CLÁUSULA DÉCIMA – ACEITE, ALTERAÇÃO E RESCISÃO

I - Aceite

a. O aceite dos serviços será realizado conforme descrito na Cláusula Nona.

II - Alteração

a. Para quaisquer alterações que se fizerem necessárias, o TJCE elaborará um Termo de Aditivo a ser assinado pelas partes;

b. A CONTRATADA deverá aceitar, nas mesmas condições propostas, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial do contrato.

III - Cancelamento

a. Ficará o Contrato rescindido, mediante formalização, assegurado o contraditório e a ampla defesa, nos seguintes casos:

a.1. Atraso injustificado na execução dos serviços contratados;

a.2. Paralisação dos serviços sem justa causa ou prévia autorização da Administração;

a.3. Subcontratação total ou parcial do Objeto deste Contrato, associação da CONTRATADA com outrem, cessão ou transferência total ou parcial, bem como da fusão, cisão ou incorporação que afetem a boa execução do Contrato;

a.4. Desatendimento das determinações da autoridade designada para acompanhar e fiscalizar a execução do Contrato, assim como a de seus superiores;

a.5. Cometimento reiterado de falhas na execução do Contrato;

a.6. Decretação de falência ou insolvência civil;

a.7. Dissolução da empresa;

a.8. Alteração ou modificação da finalidade ou da estrutura da Empresa que prejudiquem a execução do Contrato;

a.9. Ocorrência de caso fortuito ou força maior regularmente comprovados, impeditivos da execução do Contrato;

a.10. RESCISÃO, nos casos previstos no art. 78 da Lei nº 8.666/93;

b. Poderá, ainda, ser rescindido o Contrato pelo CONTRATANTE, a qualquer tempo, mediante simples aviso à outra parte, com antecedência mínima de 30(trinta) dias.

CLÁUSULA DÉCIMA PRIMEIRA – PROPRIEDADE, SIGILO, RESTRIÇÕES

O direito de posse e propriedade de todos os artefatos e produtos elaborados pela Contratada em decorrência do contrato é do Tribunal de Justiça do Estado do Ceará, sendo vedada sua cessão, locação ou venda a terceiros.

I - Condições de manutenção de sigilo conforme alínea "i", inciso II da Cláusula Quarta.

CONFERIDO

CLÁUSULA DÉCIMA SEGUNDA – MECANISMOS FORMAIS DE COMUNICAÇÃO

ID	Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
1	Abertura de chamados remotos	Contratante	Contratada	A abertura de chamados será realizada através de contato telefônico, via site na web ou e-mail.	Sempre que necessário
2	Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Telefone, E-mail ou Presencial.	Sempre que necessário
3	Comunicações oficiais	Contratada/ Contratante	Contratante/ Contratada	Ofício por correspondência	Sempre que necessário

CLÁUSULA DÉCIMA TERCEIRA – DAS SANÇÕES APLICÁVEIS

No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o CONTRATANTE, as sanções administrativas aplicadas à CONTRATADA serão:

I - Advertência;

II - Suspensão temporária de participar de licitações e impedimento de contratar com a Administração Pública, por prazo não superior a 2 (dois) anos;

III - Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

IV - Multa de:

a. 0,20% (zero vírgula vinte por cento) por hora, sobre o valor contratual das licenças, por não atender aos prazos de início dos serviços de atendimento telefônico, limitado a 10% (dez por cento);

b. 0,26% (zero vírgula vinte e seis por cento), por dia de atraso, sobre os valores das licenças não entregues dentro do prazo de entrega, até o percentual de 8% (oito por cento);

b.1. No caso de atraso injustificado na entrega das licenças superior a 30 (trinta) dias, aplica-se, adicionalmente multa de 2% (dois por cento) sobre os valores dos itens não entregues dentro do prazo de entrega;

c. 10% (dez por cento), sobre o valor total do contrato, no caso de inexecução total da obrigação, sem prejuízo das demais consequências oriundas da rescisão unilateral da avença;

V - A multa a que se alude aos itens anteriores não impede que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas na Lei nº 8.666/93 e Lei nº 10.520/2002;

VI - As sanções acima descritas poderão ser aplicadas de forma distinta ou cumulativa;

VII - Ao TJCE será assegurado, após regular processo administrativo, utilizar a garantia para permitir a compensação da multa aplicada. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente.

CLÁUSULA DÉCIMA QUARTA – DO PREÇO

O CONTRATANTE pagará à CONTRATADA o valor global de **R$ 162.500,00 (cento e sessenta e dois mil e quinhentos reais)**, em conformidade com o descrito na tabela abaixo:

ITEM	DESCRIÇÃO	UNID.	QTD	VLAOR	VALOR

CONFERIDO

		MEDIDA		UNITÁRIO	TOTAL
1	Renovação de licenças Kaspersky Endpoint Security for Business - Select Brazilian com 36 meses de garantia. **Part Number: KL4863KAYTD**	UNIDADE	2.500	R$ 65,00	R$ 162.500,00
			TOTAL GLOBAL	**R$ 162.500,00**	

CLÁUSULA DÉCIMA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

Os recursos financeiros correrão por conta do Fundo Especial de Reaparelhamento e Modernização do Judiciário - FERMOJU, tendo como Fonte os recursos diretamente arrecadados, na seguinte dotação orçamentária:

04200021.02.126.036.23020.1500000.449039.27000.1.20
04200021.02.126.036.23021.1500000.449039.27000.1.20

CLÁUSULA DÉCIMA SEXTA – VIGÊNCIA CONTRATUAL E PRAZO DE EXECUÇÃO DOS SERVIÇOS

A vigência do contrato inicia na data de sua assinatura e vigorará:

I - Para o fornecimento das licenças de antivírus Kaspersky Endpoint Security for Business - Select Brazilian, por até 40(quarenta) dias contados a partir do recebimento da ordem de fornecimento de bens (OFB) pela CONTRATADA; e

II - Para a prestação dos serviços de garantia, por 36(trinta e seis) meses contados a partir da data respectivo termo de recebimento definitivo das licenças renovadas e/ou novas licenças adquiridas.

CLÁUSULA DÉCIMA SÉTIMA – DAS CONDIÇÕES DE PAGAMENTO

O pagamento será realizado através de depósito bancário, preferencialmente, nas agências do BANCO BRADESCO S/A, em até 30(trinta) dias após o recebimento definitivo dos bens/serviços adquiridos, mediante apresentação da fatura/nota fiscal atestada pelo setor competente deste Tribunal e mediante a apresentação de certidões negativas de débitos federal, estadual, municipal, previdenciário, trabalhistas e FGTS.

I - Constatada a situação de irregularidade do fornecedor contratado, deve-se providenciar a sua advertência, por escrito, no sentido de que, no prazo de 05 (cinco) dias úteis, o fornecedor regularize sua situação ou, no mesmo prazo, apresente sua defesa;

II - O prazo do inciso anterior poderá ser prorrogado uma vez, por igual período, a critério da Administração;

III - Não havendo regularização ou sendo a defesa considerada improcedente, a Administração deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do fornecedor, bem como quanto à existência de pagamento a ser efetuado pela Administração, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

IV - Persistindo a irregularidade, a Administração deverá adotar as medidas necessárias à rescisão dos contratos em execução, nos autos dos processos administrativos correspondentes, assegurada à Contratada a ampla defesa;

V - Havendo a efetiva prestação de serviços ou o fornecimento dos bens, os pagamentos serão realizados normalmente, até que se decida pela rescisão contratual, caso o fornecedor não regularize sua situação;

VI - As faturas/notas fiscais deverão ser emitidas em nome do Fundo Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ nº. 41.655.846/0001-47;

CONFERIDO

VII - O Tribunal de Justiça do Estado do Ceará reserva-se o direito de recusar o pagamento, caso o objeto não esteja em conformidade com as condições estabelecidas em contrato;

VIII - Caso existam penalidades a serem aplicadas, a CONTRATADA será notificada, sendo o prazo do atesto da respectiva fatura ou nota fiscal interrompido até a entrega das justificativas pela CONTRATADA;

IX - Nas notas fiscais referentes aos serviços descritos neste documento, deverão estar discriminados os valores dos tributos: Imposto sobre Serviços – ISS, PIS e COFINS. A CONTRATADA também deverá durante todo o período contratual manter suas documentações fiscais atualizadas.

CLÁUSULA DÉCIMA OITAVA – DA GARANTIA CONTRATUAL

Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a CONTRATADA prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

a) Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;

b) Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;

c) Seguro garantia;

d) Fiança bancária;

I - Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;

II - Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a Contratada deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias, contados da data em que for notificada;

III - A não apresentação da garantia até a assinatura contratual ou sua apresentação em desacordo com o prazo fixado significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;

IV - No caso de rescisão do contrato, a garantia se presta a cobrir prejuízos comprovados;

V - A garantia ofertada deverá cobrir multas aplicadas, bem como obrigações trabalhistas e previdenciárias, não deverá ser proporcional ao tempo de vigência do contrato, garantindo sua totalidade durante todo o período de vigência. Não será aceita cláusula que preveja a realização do contrato por terceiros, bem como cláusula que preveja a subrogação da seguradora nos créditos da segurada. Deve, também, ser concedido pela seguradora, prazo mínimo de 30 (trinta) dias para comunicação pelo TJCE das falhas cometidas pela segurada.

CLÁUSULA DÉCIMA NONA – DA LEGISLAÇÃO APLICÁVEL

Este contrato rege-se pela Lei nº 10.520/2002 e Lei nº 8.666/93, alterada pelas Leis nº 9.648/1998, nº 9.854/1999, legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

CLÁUSULA VIGÉSIMA – DO FORO

Fica eleito o foro de Fortaleza (CE), para dirimir quaisquer dúvidas oriundas do presente Contrato, caso não possam ser resolvidos por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

CONFERIDO

E, por estarem justos e acertados, firmam o presente em 02 (duas) vias de igual teor e forma, na presença da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça Eletrônico.

Fortaleza, 08 de FEVEREIRO de 2018.

DES. FRANCISCO GLADYSON PONTES
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ

DRA. DENISE MARIA NORÕES OLSEN
SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO DO TJCE

SR. JOSÉ MURILO CIRINO NOGUEIRA JÚNIOR
REP. LEGAL DA EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

Testemunhas: _____ _____

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

ESTADO DO CEARÁ PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA	ESPECIFICAÇÕES TÉCNICAS	Código: Versão:

Abaixo, apresentamos a descrição dos *part numbers* das licenças dos softwares antivírus: KL4863KAYTD, KL4863KAYTP e KL4313KAYTH e suas respectivas características técnicas mínimas necessárias para a contratação.

Produto	Part Number
Kaspersky Endpoint Security for Business – Select - Renovação	KL4863KAYTD
Kaspersky Endpoint Security for Business – Select – Aquisição	KL4863KAYTP
Kaspersky Security for Mail Server - Renovação	KL4313KAYTH
Kaspersky Security for Mail Server - Aquisição	

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2003 ou superior (Todas edições);

1.1.2. Microsoft Windows Server 2003 x64 ou superior (Todas edições);

1.1.3. Microsoft Windows Server 2008 (Todas edições);

1.1.4. Microsoft Windows Server 2008 Core (Todas edições);

1.1.5. Microsoft Windows Server 2008 x64 SP1 (Todas edições);

1.1.6. Microsoft Windows Server 2008 R2 (Todas edições);

1.1.7. Microsoft Windows Server 2008 R2 Core (Todas edições);

1.1.8. Microsoft Windows Server 2012 (Todas edições);

1.1.9. Microsoft Windows Server 2012 R2 (Todas edições);

1.1.10. Microsoft Windows XP Professional SP2 e superior;

1.1.11. Microsoft Windows XP Professional x64 e superior;

1.1.12. Microsoft Windows Vista SP1;

1.1.13. Microsoft Windows Vista x64 SP1;

1.1.14. Microsoft Windows 7;

1.1.15. Microsoft Windows 7 x64;

CONFERIDO

1.1.16. Microsoft Windows 8;

1.1.17. Microsoft Windows 8 x64.

1.2. Deve suportar as seguintes plataformas virtuais:

1.2.1. VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5;

1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

1.2.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;

1.2.4. Microsoft VirtualPC 6.0.156.0;

1.2.5. Parallels Desktop 7 e superior;

1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);

1.2.7. Citrix XenServer 6.1, 6.2;

1.3. Características:

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

1.3.2. Console deve ser baseada no modelo cliente/servidor;

1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.3.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.3.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;

1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;

1.3.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

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

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

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

CONFERIDO

1.3.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

1.3.13. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;

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

1.3.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

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

1.3.17. Capacidade de gerenciar smartphones e tablets (Windows Phone , Android e iOS) protegidos pela solução antivírus;

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

1.3.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.3.20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.3.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

1.3.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado através dos seguintes parâmetros:

Nome do computador;

Nome do domínio;

Range de IP;

Sistema Operacional Máquina virtual.

1.3.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.3.25. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

1.3.26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.3.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

CONFERIDO

1.3.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.3.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

1.3.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.3.31. Deve fornecer as seguintes informações dos computadores:

1.3.31.1. Se o antivírus está instalado;

1.3.31.2. Se o antivírus está iniciado;

1.3.31.3. Se o antivírus está atualizado;

1.3.31.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

1.3.31.5. Minutos/horas desde a última atualização de vacinas;

1.3.31.6. Data e horário da última verificação executada na máquina;

1.3.31.7. Versão do antivírus instalado na máquina;

1.3.31.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.3.31.9. Data e horário de quando a máquina foi ligada;

1.3.31.10. Quantidade de vírus encontrados (contador) na máquina;

1.3.31.11. Nome do computador;

1.3.31.12. Domínio ou grupo de trabalho do computador;

1.3.31.13. Data e horário da última atualização de vacinas;

1.3.31.14. Sistema operacional com Service Pack;

1.3.31.15. Quantidade de processadores;

1.3.31.16. Quantidade de memória RAM;

1.3.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

1.3.31.18. Endereço IP;

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

1.3.31.20. Atualizações do Windows Updates instaladas;

CONFERIDO

1.3.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

1.3.31.22. Vulnerabilidades de aplicativos instalados na máquina;

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

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

1.3.33.1. Mudança de gateway;

1.3.33.2. Mudança de subnet DNS;

1.3.33.3. Mudança de domínio;

1.3.33.4. Mudança de servidor DHCP;

1.3.33.5. Mudança de servidor DNS;

1.3.33.6. Mudança de servidor WINS;

1.3.33.7. Aparecimento de nova subnet;

1.3.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.3.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.3.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.3.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.3.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.3.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

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

1.3.41. Capacidade de gerar traps SNMP para monitoramento de eventos;

1.3.42. Capacidade de enviar emails para contas específicas em caso de algum evento;

CONFERIDO

1.3.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

1.3.44. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.3.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);

1.3.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

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

1.3.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.49. 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.

1.3.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.51. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

1.3.52. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.3.53. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows XP Professional SP3 e superior;

2.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2;

2.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;

2.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate;

2.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

2.1.6. Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior;

2.1.7. Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior;

2.1.8. Microsoft Windows 8 Professional/Enterprise;

2.1.9. Microsoft Windows 8 Professional/Enterprise x64;

2.1.10. Microsoft Windows 8.1 Enterprise x86 / 64;

2.1.11. Microsoft Windows 8.1 Pro x86 /64;

CONFERIDO NTI

2.1.12. Microsoft Windows 10 Enterprise x86 / 64;

2.1.13. Microsoft Windows 10 Pro x86 / 64.

2.2. Características:

2.2.1. Deve prover as seguintes proteções:

2.2.1.1. Antivírus de Arquivos residente (antispyware, antitrojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

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

2.2.1.3. Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos);

2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);

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

2.2.1.6. Firewall com IDS;

2.2.1.7. Auto proteção (contra ataques aos serviços/processos do antivírus);

2.2.1.8. Controle de dispositivos externos;

2.2.1.9. Controle de acesso a sites por categoria;

2.2.1.10. Controle de acesso a sites por horário;

2.2.1.11. Controle de acesso a sites por usuários;

2.2.1.12. Controle de execução de aplicativos;

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

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

2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa);

2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

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

2.2.6. 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;

CONFERIDO
NTS

2.2.7. 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;

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

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

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

2.2.11. Capacidade de verificar somente arquivos novos e alterados;

2.2.12. Capacidade de verificar objetos usando heurística;

2.2.13. Capacidade de agendar uma pausa na verificação;

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

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

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

2.2.16.1. Perguntar o que fazer, ou;

2.2.16.2. Bloquear acesso ao objeto;

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

2.2.16.2.2. Caso positivo de desinfecção:

2.2.16.2.2.1. Restaurar o objeto para uso;

2.2.16.2.3. Caso negativo de desinfecção:

2.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré estabelecida pelo administrador);

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

2.2.18. Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

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

2.2.20. Capacidade de verificar links inseridos em emails contra phishings;

2.2.21. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;

2.2.22. Capacidade de verificação de corpo e anexos de emails usando heurística;

2.2.23. O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:

2.2.23.1. Perguntar o que fazer, ou;

CONFERIDO

2.2.23.2. Bloquear o email;

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

2.2.23.2.2. Caso positivo de desinfecção:

2.2.23.2.2.1. Restaurar o email para o usuário;

2.2.23.2.3. Caso negativo de desinfecção:

2.2.23.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré estabelecida pelo administrador);

2.2.24. Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

2.2.25. Possibilidade de verificar somente emails recebidos ou recebidos e enviados.

2.2.26. Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

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

2.2.28. Deve ter suporte total ao protocolo IPv6;

2.2.29. Capacidade de alterar as portas monitoradas pelos módulos de Web e Email;

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

2.2.30.1. Perguntar o que fazer, ou;

2.2.30.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.30.3. Permitir acesso ao objeto;

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

2.2.31.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.2.31.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

2.2.33. 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;

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

CONFERIDO NTS

2.2.35. 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;

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

2.2.37. Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;

2.2.38. 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;

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

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

2.2.39.2. 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;

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

2.2.40.1. Discos de armazenamento locais;

2.2.40.2. Armazenamento removível;

2.2.40.3. Impressoras;

2.2.40.4. CD/DVD;

2.2.40.5. Drives de disquete;

2.2.40.6. Modems;

2.2.40.7. Dispositivos de fita;

2.2.40.8. Dispositivos multifuncionais;

2.2.40.9. Leitores de smart card;

2.2.40.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

2.2.40.11. Wi-Fi;

2.2.40.12. Adaptadores de rede externos;

2.2.40.13. Dispositivos MP3 ou smartphones;

2.2.40.14. Dispositivos Bluetooth;

CONFERIDO

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

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

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

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

2.2.45. 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;

2.2.46. 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);

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

2.2.48. 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;

2.2.49. 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 a web;

2.2.50. 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 a web.

3. Estações de trabalho Linux

3.1. Compatibilidade:

3.1.1. Plataforma 32-bits:

3.1.1.1. Canaima 3;

3.1.1.2. Red Flag Desktop 6.0 SP2;

3.1.1.3. Red Hat Enterprise Linux 5.8 Desktop;

3.1.1.4. Red Hat Enterprise Linux 6.2 Desktop;

3.1.1.5. Fedora 16;

3.1.1.6. CentOS-6.2;

3.1.1.7. SUSE Linux Enterprise Desktop 10 SP4;

CONFERIDO

3.1.1.8. SUSE Linux Enterprise Desktop 11 SP2;

3.1.1.9. openSUSE Linux 12.1;

3.1.1.10. openSUSE Linux 12.2;

3.1.1.11. Debian GNU/Linux 6.0.5;

3.1.1.12. Mandriva Linux 2011;

3.1.1.13. Ubuntu 10.04 LTS;

3.1.1.14. Ubuntu 12.04 LTS;

3.1.2. Plataforma 64-bits:

3.1.2.1. Canaima 3;

3.1.2.2. Red Flag Desktop 6.0 SP2;

3.1.2.3. Red Hat Enterprise Linux 5.8;

3.1.2.4. Red Hat Enterprise Linux 6.2 Desktop;

3.1.2.5. Fedora 16;

3.1.2.6. CentOS-6.2;

3.1.2.7. SUSE Linux Enterprise Desktop 10 SP4;

3.1.2.8. SUSE Linux Enterprise Desktop 11 SP2;

3.1.2.9. openSUSE Linux 12.1;

3.1.2.10. openSUSE Linux 12.2;

3.1.2.11. Debian GNU/Linux 6.0.5;

3.1.2.12. Ubuntu 10.04 LTS;

3.1.2.13. Ubuntu 12.04 LTS.

3.2. Características:

3.2.1. Deve prover as seguintes proteções:

3.2.1.1. Antivírus de arquivos residente (antispyware, antitrojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

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

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

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

3.2.2.2. 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;

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

CONFERIDO

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

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

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

3.2.5. 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 tomá-la a partir da extensão do arquivo;

3.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

4. Servidores Windows

4.1. Compatibilidade:

4.1.1. Microsoft Windows Small Business Server 2011 Essentials/Standard x64;

4.1.2. Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64;

4.1.3. Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64;

4.1.4. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1; x86/x64;

4.1.5. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64;

4.1.6. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1;

4.1.7. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1;

4.1.8. Microsoft Windows Server 2012 Foundation/Essentials/Standard x64;

4.1.9. Microsoft Windows Hyper-V Server 2008 R2 SP1;

4.1.10. Microsoft Terminal baseado em Windows Server 2003;

4.1.11. Microsoft Terminal baseado em Windows Server 2008;

4.1.12. Microsoft Terminal baseado em Windows Server 2008 R2;

4.1.13. Citrix Presentation Server 4.0 e 4.5;

4.1.14. Citrix XenApp 4.5, 5.0 e 6.0.

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

CONFERIDO

4.2.1.1. Antivírus de Arquivos residente (antispyware, antitrojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.1.2. Auto proteção contra ataques aos serviços/processos do antivírus

4.2.1.3. Firewall com IDS;

4.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados

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

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

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

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

4.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)

4.2.4.3. Leitura de configurações;

4.2.4.4. Modificação de configurações;

4.2.4.5. Gerenciamento de Backup e Quarentena;

4.2.4.6. Visualização de relatórios;

4.2.4.7. Gerenciamento de relatórios;

4.2.4.8. Gerenciamento de chaves de licença;

4.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

4.2.5.2. 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;

4.2.6. 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;

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

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

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

CONFERIDO

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

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

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

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

4.2.14. 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;

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

4.2.16. 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 tomá-la a partir da extensão do arquivo;

4.2.17. Capacidade de verificar somente arquivos novos e alterados;

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

4.2.19. Capacidade de verificar objetos usando heurística;

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

4.2.21. Capacidade de agendar uma pausa na verificação;

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

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

4.2.23.1. Perguntar o que fazer, ou;

4.2.23.2. Bloquear acesso ao objeto;

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

4.2.23.2.2. Caso positivo de desinfecção:

4.2.23.2.2.1. Restaurar o objeto para uso;

4.2.23.2.3. Caso negativo de desinfecção:

4.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré estabelecida pelo administrador);

CONFERIDO

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

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

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

4.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5. Servidores Linux

5.1. Compatibilidade:

5.1.1. Plataforma 32-bits:

5.1.1.1. Canaima 3;

5.1.1.2. Asianux Server 3 SP4;

5.1.1.3. Asianux Server 4 SP1;

5.1.1.4. Red Hat Enterprise Linux 6.2 Server;

5.1.1.5. Red Hat Enterprise Linux 5.8 Server

5.1.1.6. Fedora 16;

5.1.1.7. CentOS-6.2;

5.1.1.8. SUSE Linux Enterprise Server 11 SP2;

5.1.1.9. Novell Open Enterprise Server 11;

5.1.1.10. openSUSE Linux 12.1;

5.1.1.11. openSUSE Linux 12.2;

5.1.1.12. Mandriva Enterprise Server 5.2;

5.1.1.13. Ubuntu Server 10.04.2 LTS;

5.1.1.14. Ubuntu Server 12.04 LTS;

5.1.1.15. Debian GNU/Linux 6.0.5;

5.1.1.16. FreeB.SD 8.3;

5.1.1.17. FreeBSD 9.

5.1.2. Plataforma 64-bits:

5.1.2.1. Canaima 3;

5.1.2.2. Asianux Server 3 SP4;

5.1.2.3. Asianux Server 4 SP1;

5.1.2.4. Red Hat Enterprise Linux 6.2 Server;

5.1.2.5. Red Hat Enterprise Linux 5.8 Server;

5.1.2.6. Fedora 16;

CONFERIDO

5.1.2.7. CentOS-6.2;
5.1.2.8. SUSE Linux Enterprise Server 11 SP2;
5.1.2.9. Novell Open Enterprise Server 11;
5.1.2.10. openSUSE Linux 12.1;
5.1.2.11. openSUSE Linux 12.2;
5.1.2.12. Mandriva Enterprise Server 5.2;
5.1.2.13. Ubuntu Server 10.04.2 LTS;
5.1.2.14. Ubuntu Server 12.04 LTS;
5.1.2.15. Debian GNU/Linux 6.0.5;
5.1.2.16. FreeBSD 8.3;
5.1.2.17. FreeBSD 9.

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

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

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

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

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

5.2.2.2. 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;

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

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

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

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

5.2.5. 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 tomá-la a partir da extensão do arquivo;

CONFERIDO

5.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

6. Smartphones e tablets

6.1. Compatibilidade:

6.1.1. Apple iOS 7.0 – 9.2;

6.1.2. Windows Phone 8.1;

6.1.3. Android OS 2.3 – 5.1;

6.2. Características:

6.2.1. Deve prover as seguintes proteções:

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

6.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

6.2.1.1.2. Arquivos abertos no smartphone;

6.2.1.1.3. Programas instalados usando a interface do smartphone;

6.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

6.2.2. Deverá isolar em área de quarentena os arquivos infectados;

6.2.3. Deverá atualizar as bases de vacinas de modo agendado;

6.2.4. Deverá bloquear spams de SMS através de black lists;

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

6.2.6. Capacidade de desativar por política:

Wi-fi;

Câmera;

Bluetooth.

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

CONFERIDO

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

6.2.9. Deverá ter firewall pessoal;

6.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente (Mugshot);

6.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

6.2.12. Capacidade de enviar comandos remotamente de:

Localizar;

Bloquear.

6.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;

6.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;

6.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;

6.2.16. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

6.2.17. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

6.2.18. Capacidade de configurar White e blacklist de aplicativos;

6.2.19. Capacidade de localizar o dispositivo quando necessário;

6.2.20. Permitir atualização das definições quando estiver em "roaming";

6.2.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

6.2.22. Capacidade de enviar URL de instalação por e-mail;

6.2.23. Capacidade de fazer a instalação através de um link QRCode;

6.2.24. Capacidade de executar as seguintes ações caso a desinfecção falhe:

Deletar, ignorar, quarentenar, perguntar ao usuário.

7. Gerenciamento de dispositivos móveis (MDM)

7.1. Compatibilidade:

7.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync;

7.1.1.1. Apple iOS;

7.1.1.2. Windows Phone;

7.1.1.3. Android.

7.1.2. Dispositivos com suporte ao Apple Push Notification (APNs) servisse;

7.1.2.1. Apple iOS 3.0 ou superior;

7.2. Características:

7.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

7.2.2. Capacidade de ajustar as configurações de:

7.2.2.1. Sincronização de e-mail;

CONFERIDO
NTIS

7.2.2.2. Uso de aplicativos;

7.2.2.3. Senha do usuário;

7.2.2.4. Criptografia de dados;

7.2.2.5. Conexão de mídia removível;

7.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

7.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;

7.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

7.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

8. Servidores de e-mail Windows

8.1. Compatibilidade:

8.1.1. Microsoft Small Business Server 2008 Standard;

8.1.2. Microsoft Small Business Server 2008 Premium;

8.1.3. Microsoft Essential Business Server 2008 Standard;

8.1.4. Microsoft Essential Business Server 2008 Premium;

8.1.5. Microsoft Windows Server 2008 x64 R2 Enterprise Edition;

8.1.6. Microsoft Windows Server 2008 x64 R2 Standard Edition;

8.1.7. Microsoft Windows Server 2008 x64 Enterprise Edition SP1;

8.1.8. Microsoft Windows Server 2008 x64 Enterprise Edition SP2;

8.1.9. Microsoft Windows Server 2008 x64 Standard Edition SP1;

8.1.10. Microsoft Windows Server 2008 x64 Standard Edition SP2;

8.1.11. Microsoft Windows Server 2003 x64 R2 Enterprise Edition SP2;

8.1.12. Microsoft Windows Server 2003 x64 R2 Standard Edition SP2;

8.1.13. Microsoft Windows Server 2003 x64 Enterprise Edition SP2;

8.1.14. Microsoft Windows Server 2003 x64 Standard Edition SP2 ;

8.1.15. Microsoft Exchange Server 2003 Standard Edition;

8.1.16. Microsoft Exchange Server 2003 Enterprise Edition;

8.1.17. Microsoft Exchange Server 2007 SP1 x64;

8.1.18. Microsoft Exchange Server 2007 SP2 x64;

8.1.19. Microsoft Exchange Server 2007 SP3 x64;

8.1.20. Microsoft Exchange Server 2010;

8.1.21. Microsoft Exchange Server 2010 SP1.

8.2. Características:

8.2.1. Deve utilizar as tecnologias VSAPI 2.0, 2.5 e 2.6;

8.2.2. Capacidade de iniciar várias cópias do processo de antivírus;

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

CONFERIDO

8.2.4. Capacidade de verificar pastas públicas, e-mails enviados, recebidos e armazenados contra vírus, spywares, adwares, worms, trojans e riskwares;

8.2.5. Capacidade de verificar pastas públicas e e-mails armazenados de forma agendada, utilizando as últimas vacinas e heurística;

8.2.6. O antivírus, ao encontrar um objeto infectado, deve:

8.2.6.1. Desinfectar o objeto, notificando o recipiente, destinatário e administradores, ou

8.2.6.2. Excluir o objeto, substituindo-o por uma notificação;

8.2.6.3. Bloquear acesso ao objeto;

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

8.2.6.3.2. Caso positivo de desinfecção:

8.2.6.3.2.1. Restaurar o objeto para uso;

8.2.6.3.3. Caso negativo de desinfecção:

8.2.6.3.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré estabelecida pelo administrador);

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

8.2.8. Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada;

8.2.9. Capacidade de gravar logs de atividade de vírus nos eventos do sistema e nos logs internos da aplicação;

8.2.10. Capacidade de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação.

9. Servidores de e-mail Linux

9.1. Compatibilidade:

9.1.1. Sistemas 32-bit:

9.1.1.1. Red Hat Enterprise Linux Server 5.2 Server;

9.1.1.2. Fedora 9;

9.1.1.3. SUSE Linux Enterprise Server 10 SP2;

9.1.1.4. openSUSE Linux 11.0;

9.1.1.5. Debian GNU/Linux 4.0 (r4);

9.1.1.6. Mandriva Corporate Server 4.0;

9.1.1.7. Ubuntu 8.04.1 Server Edition;

9.1.1.8. FreeBSD 6.3, 7.0.

9.1.2. Sistemas 64-bit:

9.1.2.1. Fedora 9;

9.1.2.2. Red Hat Enterprise Linux Server 5.2 Server;

9.1.2.3. SUSE Linux Enterprise Server 10 SP2;

9.1.2.4. penSUSE Linux 11.0;

CONFERIDO

9.1.2.5. Debian 6.0.2.

9.1.3. MTA:

9.1.3.1. Sendmail 8.12.x ou superior;

9.1.3.2. Qmail 1.03;

9.1.3.3. Postfix 2.x;

9.1.3.4. Exim 4.x;

9.2. Características:

9.2.1. Capacidade de verificar o tráfego SMTP do servidor contra malware em todos os elementos do e-mail: cabeçalho, corpo e anexo;

9.2.2. Capacidade de notificar o administrador, o remetente e o destinatário caso um arquivo malicioso seja encontrado no e-mail;

9.2.3. Capacidade de quarentenar objetos maliciosos;

9.2.4. Capacidade de salvar backup dos objetos antes de tentativa de desinfecção;

9.2.5. Capacidade de fazer varredura no sistema de arquivos do servidor;

9.2.6. Capacidade de filtrar anexos por nome ou tipo de arquivo;

9.2.7. Capacidade de criar grupos de usuários para aplicar regras de verificação de e-mails;

9.2.8. Deve permitir gerenciamento via console WEB;

9.2.9. Deve ser atualizado de maneira automática via internet ou por servidores locais, com frequência horária.

CONFERIDO

ANEXO II – TERMO DE RECEBIMENTO PROVISÓRIO

ESTADO DO CEARÁ PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA	**TERMO DE RECEBIMENTO PROVISÓRIO - TRP**	**Código:** **Versão:**

1. IDENTIFICAÇÃO

Contrato Nº		**N. da OS/OFB**	
Objeto			
Contratante			
Contratada		**CNPJ**	

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 34, inciso I, da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 11/09/2014, que os serviços (ou bens), relacionados na OS identificada, foram recebidos nesta data e serão objetos de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até (DD) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

2. APROVAÇÃO

Fiscal Técnico	Preposto
(Nome) - (Matricula)	(Nome) - (Qualificação)

Fortaleza, (DD de MMMM de AAAA)

CONFERIDO

ANEXO III – TERMO DE RECEBIMENTO DEFINITIVO

ESTADO DO CEARÁ PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA	**TERMO DE RECEBIMENTO DEFINITIVO - TRD**	Código: Versão:

1. IDENTIFICAÇÃO

Contrato Nº		**N. da OS/OFB**	
Objeto			
Gestor do Contrato			
Fiscal Requisitante do Contrato			

Por este instrumento, os servidores acima identificados atestam, para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 11/09/2014, que o(s) serviço(s) ou bem(ns) integrante(s) da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Termo de Referência/Projeto Básico do Contrato supracitado.

2. APROVAÇÃO

Fiscal Requisitante	Gestor do Contrato
(Nome) – (Qualificação)	(Nome) - (Matrícula)

Fortaleza, (DD de MMMM de AAAA)

Ciente,

Preposto
(Nome) – (Qualificação)

Fortaleza, (DD de MMMM de AAAA)

CONFERIDO

ANEXO IV – TERMO DE COMPROMISSO

AQSETIN2016002 – Aquisição e Renovação das Licenças de Antivírus

CONDIÇÕES DO TERMO

O (NOME DO ÓRGÃO), sediado em (ENDEREÇO), CNPJ n.° (CNPJ), doravante denominado CONTRATANTE, e, de outro lado, a (NOME DA EMPRESA), sediada em (ENDEREÇO), CNPJ n.° (CNPJ), doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.° DD/AAAA doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Primeira – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I - Informação: é o conjunto de dados organizados de acordo com procedimentos executados por

CONFERIDO

meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II - Informação Pública ou Ostensiva: é aquela cujo acesso é irrestrito, obtida por meio de divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III - Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV - Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V - Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

CONFERIDO NTIS

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

CONFERIDO

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou

CONFERIDO

recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da eqüidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOs e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

CONFERIDO

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessária a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da (CIDADE DA CONTRATANTE), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

De Acordo

<Ao final, assinam um representante do contratante e da contratada, preenchendo-se a data de aprovação do artefato>

Contratante (Nome do Contratante) (Matrícula)	Contratada (Nome da Contratada) (Qualificação)
Testemunha 1 (Nome) (Qualificação)	Testemunha 2 (Nome) (Qualificação)

Fortaleza, (DD de MMMM de AAAA)

CONFERIDO

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ANEXO V – TERMO DE CIÊNCIA

AQSETIN2016002 – Aquisição e Renovação das Licenças de Antivírus

• FINALIDADE

1. Este documento tem como finalidade obter comprometimento formal dos empregados da contratada diretamente envolvidos nos projeto sobre o conhecimento da declaração e manutenção de sigilo e das normas de segurança vigentes na instituição.

• EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO.

Contrato Nº:		
Objeto:		
Gestor do Contrato	**Matrícula:**	
Contratante:		
Contratada:	**CNPJ**	
Preposto da Contratada:	**CPF**	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

• CIÊNCIA E APROVAÇÃO

(Nome) – (Matrícula) Preposto da Contratada	(Nome) – (Matrícula) Funcionário	(Nome) – (Matrícula) Funcionário
(Nome) – (Matrícula) Funcionário	(Nome) – (Matrícula) Funcionário	(Nome) – (Matrícula) Funcionário

Fortaleza, (DD de MMMM de AAAA)

CONFERIDO

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

Roberto Fiuza Maia
Notário

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

Livro: **0384**

Folha: 092

1º Traslado

Prot.: **063517**

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

Saibam quantos este público instrumento virem que, aos 26 (vinte e seis) dias do mês de outubro do ano de 2015 (dois mil e quinze), nesta cidade de Fortaleza, Capital do Estado do Ceará, República Federativa do Brasil, neste Cartório, na Avenida Padre Antônio Tomás, nº 920, Aldeota, compareceu perante mim, Conceição de Maria Correia Maia, escrevente substituta, como outorgante, **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.,** pessoa jurídica de direito privado, com sede nesta Capital, na Rua Capitão Melo, nº 3373, 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 Rua Zuca Accioly, nº 633, aptº 202, Bloco G, Manoel Dias Branco, portador da cédula de identidade nº 99010123694-SSP-CE e da CNH nº 00809571455-DETRAN-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, do que dou fé. Então pela outorgante, me foi dito, representada como está, que nomeava e constituía sua bastante procuradora, **FRANCISCA ANDREA CAMINHA CIRINO,** brasileira, casada, diretora financeira, residente e domiciliada nesta Capital, na Rua Zuca Accioly, nº 633, aptº 202, bloco G, Manoel Dias Branco, portadora da cédula de identidade nº 2001002296402-SSPDS-CE, inscrita no CPF sob o nº 824.533.063-91, a quem confere poderes amplos e ilimitados para representá-la, pagando e recebendo contas, comprando e vendendo mercadorias relativas ao seu comércio, promovendo cobranças amigáveis e judiciais, dando recibos e quitações; admitir e demitir empregados, fixar-lhes os respectivos salários, assinar contratos de trabalhos e carteiras profissionais; abrir, movimentar e encerrar contas bancárias em nome da outorgante, em quaisquer estabelecimentos bancários, oficiais ou particulares, inclusive **BANCO DO BRASIL S/A, CEF-CAIXA ECONÔMICA FEDERAL, BANCO DO NORDESTE DO BRASIL S/A** e **BANCO BRADESCO S/A**, podendo, para tanto, assinar propostas ou contrato de abertura de contas de depósito com as cláusulas e condições que convencionar, emitir, assinar e endossar cheques, receber cheques devolvidos, fazer depósitos e retiradas, passar recibos, dar e receber quitação, verificar saldos bancários, requerer e receber talonários de cheques, solicitar extratos bancários, autorizar débitos e transferências de numerários, por meio de carta ou qualquer outro meio, endossar e assinar duplicatas e descontá-las, bem como ordem de pagamento, requerer e receber cartão magnético, cadastrar e alterar senhas, passar recibos, dar e receber quitação; representá-la nas repartições públicas Federais, Estaduais, Municipais e Autárquicas, sociedades de economia mista e entidades paraestatais, inclusive na **JUSTIÇA DO TRABALHO, INSS, RECEITA FEDERAL DO BRASIL, JUNTA COMERCIAL, MINISTÉRIO DO TRABALHO E EMPREGO, SECRETARIA DA FAZENDA, SEBRAE** e onde mais necessário se fizer, assinando e requerendo o que for necessário, formular documentos, protestar títulos e notas promissórias, autorizar débitos, transferências e pagamentos por meio de cartas, autorizar e conceder alteração nos vencimentos e valores de todos os títulos comerciais, negociando nos bancos, produzir provas e justificações, assinar e receber correspondências, passar recibos, receber, dar quitação, participar de concorrências públicas e/ou particulares, participar de carta convite, tomadas de preços, licitações, pregões presenciais e eletrônicos, apresentar e retirar documentos, assinar e requerer tudo que for necessário, assinando contratos de qualquer natureza, aceitando, estabelecendo cláusulas e condições; contrair empréstimo bancário em nome da outorgante, em