# TERMO DE REFERÊNCIA

## Aquisição de soluções em segurança da informação

### 1. OBJETO DA CONTRATAÇÃO

**Registro de preços** para eventual contratação de empresa(s) especializada(s) no fornecimento dos seguintes produtos e serviços:

| Lote | Bem/Serviço |
|---|---|
| 1 | 1000 (hum mil) licenças de solução de proteção para endpoints e antispam, com garantia de funcionamento pelo período de 24 (vinte e quatro) meses, após o período inicial de garantia de 12 (doze meses), totalizando 36 (trinta e seis) meses de suporte ininterrupto, incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, contemplando os serviços de implantação, configuração, garantia de atualização contínua e repasse de conhecimento (capacitação) de toda a solução. |
| 2 | Aquisição de 1 cluster de firewall baseado em appliance (mínimo de dois dispositivos) e 1 cluster em servidores intel (2 licenças – atualmente instalado em servidor Dell R720), incluindo software de gerência, instalação, configuração, operação assistida de 200 horas, atualização de novas versões, suporte técnico, capacitação e garantia por 24 (vinte e quatro) meses após a garantia inicial de 12 (doze) meses, totalizando 36 (trinta e seis) meses de suporte ininterrupto. |

Os requisitos técnicos completos estão descritos no ANEXO I deste termo de referência.

### 2. JUSTIFICAVA DA CONTRATAÇÃO

2.1. É inquestionável a relevância dos serviços de TI para o bom desempenho das atividades da TERRACAP. A eventual indisponibilidade desses serviços causa impactos severos aos trabalhos, sejam eles finalísticos ou de apoio, podendo até mesmo impedir ou dificultar as ações institucionais. Com isso, vem a necessidade de se manter cada vez mais atualizado contra pragas virtuais tais como, ataques do dia zero, ameaças desconhecidas, ameaças avançadas persistentes, ransomwares, entre outras.

2.2. A TERRACAP possui atualmente em seu parque 750 estações de trabalho ativas, 90 servidores Windows e 74 servidores Linux somando um total de 914 equipamentos que necessitam de proteção contra infecção de códigos maliciosos.

2.3. Diante da importância de manter o parque computacional da TERRACAP protegido contra ameaças virtuais, faz-se necessária aquisição de licenças de solução de antivirus/antimalware e antispam para atendimento aos requisitos mínimos de segurança da informação na empresa.

2.4. Atualmente existe implementada no parque da TERRACAP, a solução de segurança de firewall, filtro de conteúdo e IPS do fabricante Check Point. Com essa tecnologia, a TERRACAP não possui histórico de danos ou prejuízos ao ambiente computacional causados por invasões, vírus ou outro tipo de código malicioso. Uma grande preocupação Coordenação de Informática se refere ao fato do produto adotado ter chegado ao fim de seu contrato, gerando assim um grande aumento de vulnerabilidade em todo o parque instalado. Os danos causados por uma invasão aos sistemas ou mesmo indisponibilidade dos sistemas podem acarretar um amplo estrago na imagem da empresa.

2.5. **Seria impreterível a solução do problema, por intermédio da aquisição de novos**

**dispositivos do mesmo ou de outro fabricante, respeitando os descritivos técnicos descritos no ANEXO I deste instrumento.**

2.6. Outro fator é que a TERRACAP, com o passar do tempo, teve aumento da demanda pelos serviços de tecnologia da informação e a rede corporativa passou por um processo de adequação e expansão, resultando em aumento de capacidade de processamento, banda e de usuários.

2.7. Como consequência dessas expansões na infraestrutura de rede, torna-se necessário adequar a infraestrutura de segurança e proteção, de modo a garantir a qualidade do serviço diante da nova realidade, inclusive aumentando o parque de segurança da informação, com a aquisição de novas unidades de firewall a fim de assegurar o suporte necessário a um tráfego intenso e crescente da rede de dados da TERRACAP.

2.8. Deste modo, justificamos que caso a aquisição não aconteça poderá haver interrupção dos serviços e indisponibilidade nos acessos à internet. Sugerimos então o atendimento dessa demanda o mais breve possível.

2.9. As necessidades corporativas da TERRACAP a serem sanadas e suportadas pela aquisição do objeto desta contratação e seus objetivos estratégicos foram elencadas no Plano Diretor de Tecnologia da Informação, conforme a seguir:

Necessidade 6 – "Sustentação do serviço de TI"

Meta 9 – "Manter infraestrutura e serviços de suporte operacional"

2.10. **RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO**

a) Minimizar as ameaças virtuais ao ambiente computacional da TERRACAP, com capacidade de identificar ameaças complexas e avançadas de forma automática;

b) Proteger as estações de trabalho e servidores da rede corporativa contra agentes maliciosos;

c) Garantir a segurança da informação trafegada na rede corporativa;

d) Proteger os dados armazenados nas estações de trabalho dos colaboradores da TERRACAP;

e) Proteger a transferência de informações institucionais por meio eletrônico;

f) Melhoria do processo de resposta a incidentes, com a capacidade de análise e rastreabilidade a partir de uma gerência centralizada;

g) Ampliar a capacidade de proteção e análise de tráfego, assim como o nível geral de segurança do ambiente, em conformidade com as mudanças realizadas na infraestrutura de rede da TERRACAP.

h) Administração centralizada em cada contexto de solução, com integração entre os elementos de contexto diferentes e assegurando total compatibilidade com o ambiente existente de gerência de rede.

i) Capacidade de oferecer proteção aos novos segmentos e maior throughput da rede; Capacidade de analisar mais segmentos, e capturar dados em maiores taxas/throughput.

## 3. DESCRIÇÃO DA SOLUÇÃO DE TI

As contratações das soluções de segurança da informação foram subdivididas em 2 (dois) lotes distintos, a fim de assegurar a maior competitividade. São eles:

| LOTE | ITEM | DESCRIÇÃO | QTDE | PAGAMENTO |
|---|---|---|---|---|
| | 1 | Licenças de uso de solução contra Antispam com suporte e garantia por 36 meses. | 1000 | Por licença |
| | 2 | Licenças de uso de solução de AntiVirus e AntiMalware com | 1000 | Por licença |

| | | | | |
|---|---|---|---|---|
| **LOTE 1** | 2 | suporte e garantia por 36 (trinta e seis) meses. | 1000 | Por licença |
| | 3 | Serviço de Instalação e configuração (40 H/H). | 01 | Único |
| | 4 | Serviço de Capacitação para até 6 servidores e ouvintes (turma única). | 01 | Único |

Valor estimado das licenças e serviços do LOTE 1: **R$ 187.694,35 (cento e oitenta e sete mil seiscentos e noventa e quatro reais e trinta e cinco centavos)** pela aquisição da solução com suporte e atualização completa por 12 (doze meses) e extensão do período de suporte técnico por 24 (vinte e quatro) meses adicionais, totalizando 36 (trinta e seis) de serviço ininterrupto, respeitados os requisitos técnicos exigidos, adicionando instalação, configuração e capacitação.

| LOTE | ITEM | DESCRIÇÃO | QTDE | PAGAMENTO |
|---|---|---|---|---|
| **LOTE 2** | 1 | Aquisição de Solução de Segurança (TIPO 1 – Cluster de Firewall baseado em appliances) com suporte e garantia por 36 meses. | 1 | Por produto |
| | 2 | Aquisição de Solução de Segurança (TIPO 2 – Cluster de Firewall baseado em servidores intel da Terracap) com suporte e garantia por 36 meses. | 1 | Por produto |
| | 3 | Serviço de instalação e configuração (limitada a até 40 H/H) | 2 | Por serviço prestado |
| | 4 | Serviço de operação assistida (H/H) | 200 | Por serviço prestado |
| | 5 | Serviço de Capacitação para até 6 servidores e ouvintes (turma única) | 1 | Único |

Valor estimado dos produto e serviços do LOTE 2: **R$ 1.738,450,30 (um mil setecentos e trinta e oito reais e quarenta e cinco centavos e trinta centavos)** pela aquisição da solução com suporte e atualização completa por 12 (doze meses) e extensão do período de suporte técnico por 24 (vinte e quatro) meses adicionais, totalizando 36 (trinta e seis) de serviço ininterrupto, respeitados os requisitos técnicos exigidos, adicionando instalação, configuração e capacitação.

## 4. ESPECIFICAÇÃO TÉCNICA

4.1. A solução ofertada deverá atender a todos os itens discriminados neste termo de referência e seu anexo como solução de fornecimento.

4.2. O detalhamento da especificação técnica da solução está contido no Anexo I.

### 4.3. Instalação, Configuração e Capacitação Técnica

4.3.1. Os softwares e todos os seus elementos deverão ser entregues e instalados nas dependências da TERRACAP por técnico certificado pelo fabricante para este fim.

4.3.2. Os produtos do LOTE 1 deverão, obrigatoriamente, ser do mesmo fabricante para que não haja problemas de integração e monitoramento da solução, que utilizará, obrigatoriamente, o mesmo software de gerência a ser fornecido junto com a solução.

4.3.3. Os produtos do LOTE 2 deverão, obrigatoriamente, ser do mesmo fabricante para que não haja problemas de integração e monitoramento da solução, que utilizará, obrigatoriamente, o mesmo software de gerência a ser fornecido junto com a solução.

4.3.4. Os produtos do item 2 do Lote 2 deverão comprovar, sob pena de desclassificação, que possuem o servidor Dell R720 em sua HCL por intermédio de documento fornecido pelo fabricante.

4.3.5. A solução e todos os seus elementos deverão ser configurados e otimizados segundo as

melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade no ambiente computacional.

4.3.6. A CONTRATADA deverá providenciar a desinstalação automática de todas as cópias instaladas do software em estações e servidores e a instalação do novo software em um único processo.

4.3.7. Ao final da implantação da solução, é obrigatória apresentação de relatório contendo as informações de data e hora da realização das atividades de configuração, nome do responsável pela demanda, nome do responsável pelo atendimento, número de controle (protocolo) e descrição sucinta do serviço.

4.3.8. As atividades deverão ser apresentadas e detalhadas por meio de ordens de serviço, previamente ao início das atividades.

4.3.9. A CONTRATADA deverá prover repasse de conhecimento na solução aderida.

4.3.10. Os Cursos de capacitação, previstos nos LOTES 1 e 2, deverão ser ministrados em Brasília para a equipe técnica do CONTRATANTE para cada produto ou serviço ofertado.

4.3.11. Os Cursos de capacitação, previstos nos LOTES 1 e 2, deverão ser ministradas por representante tecnicamente certificado pelo fabricante nos componentes da solução ofertada.

4.3.12. Os Cursos deverão capacitar a equipe técnica do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais nas soluções ofertadas.

4.3.13. Nos cursos de capacitação, o material didático completo da solução deverá ser fornecido para cada aluno.

4.3.14. Todos integrantes das equipes capacitadas deverão receber certificados de conclusão.

4.3.15. Cada capacitação deverá ser na modalidade de turma fechada para o máximo de 6 (seis) participantes (entre servidores e ouvintes) e carga horária mínima de 30 (trinta) horas.

4.3.16. A solução ofertada nos LOTES 1 e 2 deverão atender a todos os itens discriminados neste termo de referência e seu anexo I como solução de fornecimento. Caso haja equipamentos a serem fornecidos, estes deverão ser novos, de primeiro uso.

4.4. **Garantia e Suporte**

4.4.1. A garantia da solução especificada deverá ser contada a partir da emissão do Termo de Recebimento Definitivo (TRD).

4.4.2. Os serviços de suporte técnico contemplam as atividades de assistência técnica para atendimento em caso de problemas na solução, esclarecimentos de dúvidas técnicas, bem como atualização de firmware e software.

4.4.3. O suporte técnico aos produtos fornecidos deverá contemplar serviços de atendimento a dúvidas técnicas, por via telefone ou e-mail, bem como serviços de suporte on-site, sem limites de chamados técnicos em qualquer modalidade, devendo o serviço estar disponível em horário comercial (8X5).

4.4.4. Durante o prazo de vigência da garantia, sem quaisquer ônus adicionais para o CONTRATANTE, a própria CONTRATADA, às suas expensas, por intermédio de sua matriz, filiais, escritórios ou representantes técnicos autorizados pelo fabricante, está obrigada a:

a) Prestar suporte telefônico e por Internet (disponibilidade de uma base de conhecimentos para pesquisa de problemas/dicas de utilização) para todos os componentes de software e hardware em horário comercial;

b) Corrigir defeitos de fabricação ou de projeto;

c) Fornecer, sem ônus adicionais, correções e novas versões disponíveis para todos os softwares, firmwares e drivers oferecidos;

4.4.5. A CONTRATADA deverá possibilitar, caso seja necessária, a abertura de chamado técnico diretamente no fabricante da solução.

4.4.6. A CONTRATADA deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de software, aplicação de correções (patches), diagnóstico,

avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

4.4.7. Os chamados serão classificados de acordo com a SEVERIDADE do problema, como segue:

a) SEVERIDADE ALTA: Aplicado quando há indisponibilidade do uso dos equipamentos/softwares;

b) SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos equipamentos/softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade; e

c) SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso dos equipamentos.

| Severidade | Atendimento | Solução definitiva |
|---|---|---|
| Alta | 2 (duas) horas | 4 (quatro) horas |
| Média | 4 (quatro) horas | 12 horas |
| Baixa | 12 (doze) horas | 24 (vinte e quatro) horas |

4.5. Para os chamados de severidade ALTA (paralização de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 02 (duas) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 4 (quatro) horas corridas a contar do início do atendimento.

4.6. Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 04 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

4.7. Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 12 (doze) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

4.8. Para os chamados de qualquer severidade, a critério da Terracap, poderá ser agendado o melhor horário para atendimento.

4.9. Caso o problema não possa ser resolvido por meio de manutenção corretiva, componentes defeituosos deverão ser substituídos por outros com as mesmas funcionalidades dentro do prazo de 48 (quarenta e oito) horas corridas, contadas a partir do registro da solicitação.

4.10. É inadmissível a substituição de peças ou componentes mecânicos ou eletrônicos de marcas ou modelos diferentes daqueles constantes da proposta vencedora.

4.11. O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia a Terracap quanto à efetiva solução do problema.

4.12. Qualquer chamado fechado, sem anuência da Terracap ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

4.13. A CONTRATADA manterá cadastro das pessoas indicadas pela Terracap que poderão efetuar abertura e autorizar o fechamento de chamados.

4.14. Ao término de atendimentos relacionados à assistência técnica da garantia, a CONTRATADA deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser assinado por técnico da TERRACAP.

4.15. A CONTRATADA deverá substituir, em até 24 (vinte e quatro) horas, o equipamento/componente já instalado por um novo, sem ônus para a TERRACAP, quando comprovados

defeitos de fabricação, do próprio ou de seus componentes, que comprometa o seu desempenho, nas seguintes hipóteses:

a) Caso ocorram 4 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

b) Caso a soma dos tempos de paralisação do equipamento/componente ultrapasse 40 (quarenta) horas, dentro de qualquer intervalo de 30 (trinta) dias.

4.15.1. O atendimento deve ser efetuado em língua portuguesa.

4.15.2. A CONTRATADA deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

a) Data e hora da abertura do chamado;

b) Data e hora do início do atendimento;

c) Responsável pelo atendimento da solicitação;

d) Motivo da ocorrência (indicação do defeito);

e) Status do chamado (aberto, em tratamento, fechado, etc.);

f) Data e hora do fechamento do chamado;

g) Solução adotada (resolução);

4.15.3. Os serviços cobertos pela garantia deverão ser prestados nas instalações da TERRACAP, em Brasília/DF.

4.15.4. Os serviços cobertos pela garantia deverão ser prestados pela empresa fabricante e/ou pela CONTRATADA.

4.15.5. Os serviços cobertos pela garantia deverão ser prestados por técnicos certificados pelo fabricante da solução.

## 5. DO REGISTRO DE PREÇO

5.1. O Decreto 7.892, de 23 de janeiro de 2013, que disciplina o Sistema de Registro de Preços, define as hipóteses especiais, porém não taxativas, sobre a admissão do Registro de Preços pela Administração Pública.

5.2. No caso da contratação pleiteada neste certame, o Registro de Preços é necessário uma vez que a contratação será realizada de forma parcelada, disciplinada pelo artigo 15 da Lei 8.666/93 e pelo Decreto 7.892/2013.

5.3. Após a adjudicação e a homologação do resultado da licitação pela autoridade competente, será efetuado o registro de preços mediante Ata de Registro de Preços, a ser firmada entre a(s) licitante(s) vencedora(s) e a TERRACAP, com efeito de compromisso de fornecimento para futura contratação.

5.4. O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, contados da sua assinatura e lançamento no sistema.

5.5. Alinhada à estratégia de implantação da TERRACAP e com o objetivo de fomentar a utilização do planejamento adequado para a realização das contratações públicas, a Ata de Registro de Preços, durante a sua vigência, **não poderá ser utilizada por qualquer órgão ou entidade da Administração, sendo esta de uso EXCLUSIVO da TERRACAP**.

5.6. Alterações nos produtos e serviços a serem fornecidos deverão ser comunicadas ao Gestor da Ata, designado pela TERRACAP e, obrigatoriamente, serão submetidos à nova homologação. Os novos produtos e serviços deverão possuir características técnicas idênticas ou superiores ao ofertado pela proposta da empresa beneficiária do registro de preços.

## 6. DEVERES E RESPONSABILIDADES DA CONTRATANTE

6.1. Nomear Gestor do contrato para acompanhar e fiscalizar a execução do contrato;

6.2. Encaminhar formalmente demandas, preferencialmente por meio de Ordem de Serviço,

de acordo com os critérios estabelecidos neste Termo de Referência;

6.3. Fiscalizar o perfeito cumprimento do objeto e das demais cláusulas do Edital e do Contrato;

6.4. Comunicar tempestivamente à CONTRATADA, por escrito, sobre as possíveis irregularidades observadas no decorrer da prestação dos serviços para a imediata adoção das providências para sanar os problemas eventualmente ocorridos;

6.5. Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o que estabelecem o Edital e o Contrato;

6.6. Atestar as notas fiscais/faturas desde que tenham sido entregues conforme estipulado no contrato, verificar os relatórios apresentados, encaminhar as notas fiscais e/ou faturas, devidamente atestadas, para pagamento;

6.7. Efetuar os pagamentos, no prazo e nas condições indicadas neste instrumento, dos serviços que estiverem de acordo com as especificações, comunicando à CONTRATADA quaisquer irregularidades ou problemas que possam inviabilizar os pagamentos;

6.8. Comunicar a CONTRATADA para que seja efetuada a substituição de empregado que, por qualquer motivo, não esteja correspondendo às expectativas;

6.9. Notificar a CONTRATADA, por escrito, sobre as imperfeições, falhas, e demais irregularidades constatadas na execução dos procedimentos previstos no presente Edital e no Contrato, a fim de serem tomadas as providências cabíveis para correção do que for notificado;

6.10. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

6.11. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitados pelo preposto da CONTRATADA;

## 7. DEVERES E RESPONSABILIDADES DA CONTRATADA

7.1. Prestar e cumprir integralmente todos os serviços que forem demandados relacionados no Termo de Referência;

7.2. Responsabilizar-se pelo perfeito cumprimento do objeto do contrato, arcar com os eventuais prejuízos causados à TERRACAP ou a terceiros, provocados por ineficiência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução dos serviços, respondendo integralmente pelo ônus decorrente de sua culpa ou dolo na entrega dos serviços, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pela TERRACAP;

7.3. Comunicar à TERRACAP, por escrito, quaisquer anormalidades, que ponham em risco o êxito e o cumprimento dos prazos de execução dos serviços, propondo as ações corretivas necessárias;

7.4. Assumir todas as despesas e ônus relativos ao pessoal utilizado e a quaisquer outras derivadas ou conexas com o Contrato, ficando ainda, para todos os efeitos legais, inexistente qualquer vínculo empregatício entre seus colaboradores e/ou preposto e a TERRACAP;

7.5. Assumir toda a responsabilidade pelos encargos fiscais e comerciais resultantes do fornecimento do objeto do presente Termo de Referência;

7.6. Designar um Preposto, para exercer as seguintes atribuições: receber serviços, aceitar os serviços demandados, participar de reuniões, entregar produtos, assinar documentos, apresentar relatórios de progresso e de níveis de serviço e pré-faturas e efetuar quaisquer atividades relacionadas com a gestão do presente contrato. O preposto deverá se apresentar na sede da TERRACAP sempre que convocado;

7.7. Aceitar as determinações da TERRACAP, para a substituição dos colaboradores cuja atuação, permanência ou comportamento forem, a seu critério, considerados prejudiciais e inconvenientes à execução dos serviços;

7.8. Fornecer as devidas notas fiscais/faturas, nos termos da lei e cumprir todas as obrigações fiscais decorrentes da execução do Contrato, responsabilizando-se por quaisquer infrações fiscais daí advindas, desde que a infração fiscal tenha resultado de obrigação da CONTRATADA;

7.9. Manter todas as condições de habilitação jurídica, fiscal, trabalhista e qualificação técnica, que ensejaram a sua contratação, devidamente atualizadas, durante toda a vigência do

contrato, sob pena de retenção dos valores, até sua regularização, sem ônus para a TERRACAP, bem como a aplicação das demais penalidades;

7.10. Manter o devido sigilo sobre as informações e dados, contidos em quaisquer mídias e documentos, que seus empregados ou prepostos vierem a obter em função dos serviços prestados à TERRACAP, respondendo pelos danos que possam provocar pelo descumprimento;

7.11. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitados pelos agentes designados pela TERRACAP.

7.12. A CONTRATADA disponibilizará, sem ônus para CONTRATANTE, plantão em horário comercial. Caso seja necessário atendimento fora do horário comercial, este será, via telefone, para atendimento de demandas emergenciais.

## 8. MODELO DE EXECUÇÃO DOS CONTRATOS

8.1. As licenças e produtos deverão ser entregues pela contratada, livre de quaisquer taxas, impostos, fretes e outros encargos.

8.2. O Recebimento Definitivo se dará após a instalação, configuração e verificação da conformidade com as Especificações do presente Edital, por servidor da TERRACAP devidamente autorizado.

### 8.3. Prazos e Condições

8.3.1. O prazo de vigência deste contrato é de **36 (trinta e seis) meses**, contado da data da sua publicação.

8.3.2. O prazo para entrega e instalação da solução deverá ocorrer em até 30 (trinta) dias úteis a partir da emissão, pelo CONTRATANTE, da ordem de serviço, posterior à assinatura do contrato.

8.3.3. Entende-se que tais serviços deverão contemplar a instalação das licenças demandadas pela CONTRATANTE, configuração, testes e entrega de documentação, prestados nas dependências da TERRACAP visando colocar os produtos em operação, devidamente instalados e configurados e com transferência de conhecimentos para a Equipe Técnica da TERRACAP.

8.3.4. A garantia será de 36 (trinta e seis) meses após o recebimento definitivo.

8.3.5. Os prazos são contados excluindo-se o dia do começo e incluindo-se o do vencimento.

### 8.4. Horários e Locais de Entrega

8.4.1. O funcionamento da TERRACAP se dá em horário comercial de 07:00 às 19:00 horas, de segunda a sexta-feira, exceto feriados. Desta forma, os produtos deverão ser entregues nas dependências da TERRACAP preferencialmente neste horário.

### 8.5. Mecanismos de Comunicação

8.5.1. Todos os serviços serão prestados sob demanda mediante emissão do documento de Ordem de Serviço ou Fornecimento de Bens pelo Gestor do Contrato.

8.5.2. O documento deverá conter obrigatoriamente as seguintes informações:

a) Número da OS/FB

b) Nome do projeto/contrato

c) Data do registro da demanda

d) Nome da contratada

e) A definição e a especificação dos bens a serem fornecidos

f) A quantidade de bens a serem fornecidos

g) Cronograma estimado de execução

h) Assinatura de representante da CONTRATADA

i) Data de aprovação e assinatura do gestor do contrato e do responsável pela

área demandante da TERRACAP

8.6. **Pagamento**

8.6.1. O pagamento será efetuado à CONTRATADA, após o aceite definitivo do documento de Ordem de Serviço ou Fornecimento de Bens ou serviços. As Notas Fiscais/Faturas deverão conter seu endereço, seu CNPJ, o número do contrato, o número do banco, da agência e da conta corrente da empresa e a descrição clara do objeto da contratação;

8.6.2. A Nota Fiscal/Fatura deverá ser entregue acompanhada dos seguintes documentos:

a) Cópias de todos os Documentos de Fornecimento de Bens concluídos no período.

b) Termo de Recebimento Definitivo assinado.

8.6.3. Os pagamentos serão efetuados, em moeda corrente, de acordo com prazo estabelecimento em norma interna da TERRACAP a contar da data de atesto da Nota Fiscal /Fatura, com emissão de Ordem Bancária para crédito em conta corrente da CONTRATADA, conforme disposto no artigo 40 inciso XIV alínea "a'" da Lei nº. 8.666/93, se comprovada a regularidade da empresa, mediante apresentação das certidões exigidas no edital de licitação;

8.6.4. No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão estes restituídos à CONTRATADA para as correções solicitadas, não respondendo a TERRACAP por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

8.7. **Garantia Financeira**

8.7.1. Como garantia das obrigações assumidas, a CONTRATADA prestará a garantia no valor correspondente a 5% (cinco por cento) do valor total do Contrato.

8.8. **Propriedade e Sigilo das Informações**

8.8.1. A CONTRATADA não poderá repassar a terceiros, em nenhuma hipótese, qualquer informação da TERRACAP que possa expor sua segurança da informação e atingir suas áreas de negócio.

## 9. MODELO DE GESTÃO DO CONTRATO

9.1. **Fiscalização**

9.1.1. A Fiscalização dos serviços será acompanhada pelo Gestor do Contrato especialmente designado pela TERRACAP, o qual deverá conferir os produtos entregues pela CONTRATADA e atestar a prestação dos serviços, quando executados satisfatoriamente, para fins de pagamento nos termos do art. 67, da Lei no. 8.666/93.

9.1.2. O Gestor do Contrato poderá recusar qualquer produto que esteja em desacordo com as especificações técnicas, e as constantes do Projeto Básico, podendo determinar prazo para a correção de possíveis falhas ou substituições de produtos em desconformidade com o solicitado;

9.1.3. Eventuais irregularidades de caráter urgente deverão ser comunicadas, por escrito, ao Gestor de Contrato com os esclarecimentos julgados necessários a serem apreciados pelo servidor designado;

9.1.4. As decisões e providências sugeridas pela empresa ou julgadas imprescindíveis, que ultrapassarem a competência do fiscal designado pela TERRACAP, deverão ser encaminhadas à autoridade superior, para a adoção das medidas cabíveis;

9.1.5. Ao Gestor do Contrato fica assegurado o direito de exigir o cumprimento de todos os itens constantes do Termo de Referência, da proposta da CONTRATADA e das cláusulas contrato.

9.2. **Sanções Aplicáveis**

9.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretarem prejuízos significativos para a CONTRATANTE.

9.2.2. Moratória diária de 0,2% (dois décimos por cento), sobre o valor do Contrato em caso de atraso na execução do objeto, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia, e a critério da TERRACAP, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

9.2.3. Moratória diária de 0,3% (três décimos por cento), sobre o valor do contrato, em caso de atraso na execução do objeto, por período superior ao previsto no item 9.2.2 limitado a 30 (trinta) dias subsequentes. Após o trigésimo primeiro dia, e a critério da TERRACAP, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

9.2.4. Compensatória de até 5% (cinco por cento) sobre o valor do Contrato, em caso de atraso na execução do objeto, por período superior ao previsto no item 9.2.3, ou de inexecução parcial da obrigação assumida.

9.2.5. Compensatória de até 10% (dez por cento) sobre o valor do Contrato, em caso de inexecução total da obrigação assumida.

9.2.6. Compensatória de até 10% (dez por cento) sobre o valor do Contrato, em caso de não cumprimento da garantia de atualização de versão do objeto ao longo do período de vigência do Contrato.

9.2.7. No caso de ocorrência concomitante das multas previstas nos itens anteriores 9.2.2 e 9.2.3, o percentual aplicado não poderá ultrapassar a 7,5% (sete e meio por cento).

9.2.8. As sanções, quando couberem, serão aplicadas pela autoridade administrativa, assegurada a ampla defesa e podendo dar-se cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo.

9.2.9. A suspensão temporária de atividade e de impedimento de contratar com a Administração serão aplicadas mediante procedimento administrativo, assegurada a ampla defesa, sempre que a CONTRATADA reincidir na prática de infrações de maior gravidade à Administração.

9.2.10. As sanções supracitadas poderão ser aplicadas à CONTRATADA por período de até 2 (dois) anos.

## 10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

### 10.1. Qualificação Técnica

10.1.1. Conforme previsto na Lei 8.666/93, no art. 43 § 3°, os Atestados de Capacidade Técnica apresentados poderão, à critério da TERRACAP, serem objetos de diligência.

10.1.2. As exigências para habilitação, relativa à qualificação técnica do **LOTE 1** são as descritas a seguir:

a) A LICITANTE VENCEDORA deverá fornecer declaração comprometendo-se a prestar garantia total de 36 (trinta e seis) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

b) A LICITANTE VENCEDORA deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução englobando a instalação e configuração de cada solução de segurança a ser fornecida.

c) Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato.

d) A proposta deverá indicar em qual página e item da documentação apresentada está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I deste Termo de Referência; e também os atestados de capacidade. A proposta deverá incluir todos os catálogos ou prospectos do fabricante, preferencialmente em língua portuguesa (Brasil), correspondente aos produtos ofertados, com descrição detalhada de cada item.

10.1.3. As exigências para habilitação, relativa à qualificação técnica do **LOTE 2** são as descritas a seguir:

a) A LICITANTE VENCEDORA deverá fornecer declaração comprometendo-se a prestar garantia total de 36 (trinta e seis) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

b) A LICITANTE VENCEDORA deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução englobando a instalação e configuração de cada solução de segurança a ser fornecida.

c) A LICITANTE VENCEDORA deverá comprovar que os produtos do item 2 do Lote 2 possuem o servidor Dell R720 em sua HCL por intermédio de documento fornecido pelo fabricante.

d) Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato.

e) A proposta deverá indicar em qual página e item da documentação apresentada está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I deste Termo de Referência; e também os atestados de capacidade. A proposta deverá incluir todos os catálogos ou prospectos do fabricante, preferencialmente em língua portuguesa (Brasil), correspondente aos produtos ofertados, com descrição detalhada de cada item.

10.2. **Critérios de Seleção**

10.2.1. A licitação será realizada na modalidade de Pregão Eletrônico, com julgamento pelo critério de "Menor Preço por Lote", atendidas as especificações e características descritas neste Termo de Referência.

10.2.2. Exige-se que os produtos/serviços ofertados no LOTE 1 seja do mesmo fabricante. Esta medida visa garantir a total integração da plataforma.

10.2.3. Exige-se que os produtos/serviços ofertados no LOTE 2 seja do mesmo fabricante. Esta medida visa garantir a total integração da plataforma.

## 11. PROVA DE CONCEITO

11.1. Poderá ser solicitada, a critério exclusivo da TERRACAP, prova de conceito da solução à empresa classificada, antes da adjudicação, com o objetivo de realizar testes de comprovação de atendimento às especificações e requisitos exigidos nas Especificações Técnicas deste Termo de Referência caso a documentação entregue pela LICITANTE seja considerada insuficiente para comprovar o atendimento a todos.

11.2. O ônus de realização da prova de conceito caberá exclusivamente ao proponente da solução. A Terracap, fornecerá apenas, o ambiente físico, pontos elétricos e lógicos para a realização dos testes.

## 12. VISTORIA

12.1. As licitantes poderão realizar vistoria no ambiente físico e tecnológico da TERRACAP, representados por meio de pessoal devidamente credenciado.

12.2. A vistoria não é obrigatória e não será fornecido atestado de vistoria.

12.3. A vistoria será acompanhada por um profissional designado pela CODIN, devendo ser agendado previamente pelo telefone (61) 3342-2171.

## 13. ANEXOS

13.1. ANEXO - I Especificações Técnicas (documento SEI/GDF 5634315)

## 14. EQUIPE DE PLANEJAMENTO

| | |
|---|---|
| **Júlio Cezar S. Henriques** | Integrante Técnico |
| **Clayton Carneiro de França** | Integrante Requisitante |
| **Wellington Rodrigues Guimarães** | Integrante Administrativo |

| | |
|---|---|
| **Clayton Carneiro de França** | Coordenador de Informática |

## 15. APROVAÇÃO

| | |
|---|---|
| **Júlio Cesar de Azevedo Reis** | Presidente |

Documento assinado eletronicamente por **JÚLIO CEZAR SCHETTINI HENRIQUES - Matr.0002401-5**, **Chefe da Divisão de Suporte**, em 28/02/2018, às 12:53, conforme art. 6º, do Decreto n° 36.756, de 16 de Setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **WELLINGTON RODRIGUES GUIMARÃES - Matr.0002308-6**, **Assessor(a)**, em 28/02/2018, às 14:30, conforme art. 6º, do Decreto n° 36.756, de 16 de Setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **CLAYTON CARNEIRO DE FRANCA - Matr.0001689-6**, **Chefe da Coordenação de Informática**, em 28/02/2018, às 16:10, conforme art. 6º, do Decreto n° 36.756, de 16 de Setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **5558697** código CRC= **2C8A07BC**.

# ANEXO I.

# ESPECIFICAÇÃO TÉCNICA DAS SOLUÇÕES

## 1. LOTE 1

**A solução de segurança para a proteção contra Antispam e Anti-vírus/Anti-malware deverá ser de apenas 01 (um) fabricante.**

### 1.1. Proteção anti-malware

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

1.1.1.1. Windows Server 2003, 2008, 2008 R2 e 2012 (32/64-bit);

1.1.1.2. Windows 7 (x86/x64);

1.1.1.3. Windows 10

1.1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

1.1.3. Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;

1.1.4. Deve possuir capacidade nativa de integração com modulo de análise virtual para ameaças desconhecidas em sandbox do mesmo fabricante da solução ofertada

1.1.5. Deve possuir tecnologia de Machine Learning sendo capaz de detectar variantes de malwares desconhecidos por similaridade de código;

1.1.6. Deverá incluir módulo de monitoração de comportamento malicioso de aplicações de forma a bloqueá-las mesmo quando a assinatura não for reconhecida;

1.1.7. Deverá incluir regras específicas para detecção de ransonware;

1.1.8. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

1.1.9. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

1.1.9.1. Processos em execução em memória principal (RAM);

1.1.9.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

1.1.9.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

1.1.9.4. Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

1.1.10. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;

1.1.11. Deve possuir detecção heurística de vírus desconhecidos;

1.1.12. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

1.1.13. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

1.1.13.1. Em tempo real de arquivos acessados pelo usuário;

1.1.13.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

1.1.13.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

1.1.13.4. Por linha-de-comando, parametrizável, com opção de limpeza;

1.1.13.5. Automáticos do sistema com as seguintes opções:

1.1.13.6. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

1.1.13.7. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

1.1.13.8. Frequência: horária, diária, semanal e mensal;

1.1.13.9. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

1.1.14. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

1.1.15. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

1.1.16. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

1.1.17. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

1.1.18. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

1.1.19. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentenar a ameaça;

1.1.20. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

1.1.21. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

1.1.22. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

1.1.23. A solução de antivírus deverá ser capaz de submeter automaticamente arquivos suspeitos a uma solução de análise de ameaças direcionadas/desconhecidas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado da análise, no mínimo, as seguintes informações;

1.1.23.1. Processos de AutoStart;

1.1.23.2. Modificações de Arquivos de Sistema;

1.1.23.3. Serviços criados e modificados;

1.1.23.4. Atividade de Rede Suspeita;

1.1.23.5. Modificações de Registros;

1.1.24. A análise de ameaças direcionadas/desconhecidas locais deverá detectar objetos maliciosos que explorem vulnerabilidades específicas dos seguintes sistemas operacionais e aplicativos apresentando relatório detalhado da ameaça;

1.1.24.1. Microsoft Windows 7 em Português;

1.1.24.2. Microsoft Office: 2010 e 2013;

1.1.24.3. Adobe Reader: 9, X e XI;

1.1.24.4. Java;

1.1.24.5. Firefox;

1.1.24.6. Adobe Flash Player;

1.1.25. Funcionalidade de Atualização

1.1.25.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

1.1.26. Deve permitir atualização incremental da lista de definições de vírus;

1.1.27. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

1.1.28. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

1.1.29. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

1.1.30. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

1.1.31. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

1.1.32. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

## 1.2. Funcionalidade de administração

1.2.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

1.2.2. Deve possibilitar instalação "silenciosa";

1.2.3. Deve permitir o bloqueio por nome de arquivo;

1.2.4. Deve permitir o travamento de pastas/diretórios e de compartilhamentos;

1.2.5. Deve permitir o rastreamento e bloqueio de infecções;

1.2.6. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

1.2.7. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

1.2.8. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

1.2.9. Deve permitir a desinstalação através da console de gerenciamento da solução;

1.2.10. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

1.2.11. Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

1.2.12. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

1.2.13. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

1.2.14. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

1.2.15. Deve permitir a deleção dos arquivos quarentenados;

1.2.16. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

1.2.17. Deve permitir integração com Active Directory para acesso a console de administração;

1.2.18. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

1.2.19. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

1.2.20. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.2.21. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

1.2.22. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

1.2.23. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

1.2.24. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.2.25. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional

1.2.26. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

1.2.27. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

1.2.28. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

1.2.29. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

1.2.30. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

1.2.31. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

1.2.32. Deve permitir a criação de usuários locais de administração da console de anti-malware;

1.2.33. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

1.2.34. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

1.2.35. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

1.2.36. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

1.2.37. Deve permitir a gerência de domínios separados para usuários previamente definidos;

1.2.38. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

1.2.39. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

## 1.3. Funcionalidade de controle de dispositivos

1.3.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

1.3.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

1.3.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

1.3.4. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

1.3.5. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

## 1.4. Funcionalidade de autoproteção

1.4.1. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

1.4.2. Deve possuir no mecanismo de autoproteção as seguintes proteções:

1.4.3. Autenticação de comandos ipc;

1.4.4. Proteção e verificação dos arquivos de assinatura;

1.4.5. Proteção dos processos do agente de segurança;

1.4.6. Proteção das chaves de registro do agente de segurança;

1.4.7. Proteção do diretório de instalação do agente de segurança.

## 1.5. Proteção anti-malware para estações Linux

1.5.1. Deverá suportar, no mínimo, as seguintes Distribuições:

1.5.1.1. Debian 8.0 ou superior;

1.5.1.2. Oracle Linux 5.0 ou superior

1.5.2. O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante

1.5.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados

1.5.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

1.5.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits, e outros;

1.5.6. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;

1.5.7. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

1.5.8. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

1.5.9. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

1.5.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

1.5.11. As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil;

## 1.6. Proteção anti-malware para estações Mac OS X

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

1.6.1.1. Mac os x 10.6.8 (snow leopard) e 10.7 (lion) em processadores 32 e 64 bits;

1.6.1.2. Mac os x Server 10.6.8 e 10.7 em processadores 32 e 64 bits;

1.6.1.3. Mac os x 10.8 (mountain lion) em processadores 64 bits;

1.6.2. Suporte ao apple remote desktop para instalação remota da solução;

1.6.3. Gerenciamento integrado à console de gerência central da solução

1.6.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

1.6.5. Permitir a verificação das ameaças da maneira manual e agendada;

1.6.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

1.6.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

## 1.7. Funcionalidade de HIPS – Host IPS e Host Firewall

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

1.7.1.1. Windows Server 2003, 2008, 2008 R2 e 2012 (32/64-bit);

1.7.1.2. Windows 7 (x86/x64);

1.7.1.3. Windows 10.

1.7.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

1.7.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

1.7.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

1.7.5. Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída

1.7.6. A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

1.7.7. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows 7 ou superior, por meio de regras de host ips;

1.7.8. Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

1.7.9. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

1.7.10. Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

1.7.11. Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

1.7.12. Deve permitir a criação de políticas de segurança personalizadas;

1.7.13. Deve permitir limitar o número de conexões simultâneas no sistema operacional

1.7.14. Deve permitir a emissão de alertas via smtp e snmp;

1.7.15. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

1.7.16. Deve permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

1.7.17. Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

1.7.18. Deve permitir a criação de regras de firewall pelos seguintes frame types: Ip, ipv4, ipv6, arp, revarp.

1.7.19. Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code;

1.7.20. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

1.7.21. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

1.7.22. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

1.7.23. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

1.7.24. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

1.7.25. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

## 1.8. Controle de aplicações

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

1.8.1.1. Windows Server 2003, 2008, 2008 R2 e 2012 (32/64-bit);

1.8.1.2. Windows 7 (x86/x64);

1.8.1.3. Windows 10;

1.8.2. Deve permitir a criação de políticas de segurança personalizadas;

1.8.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

1.8.3.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

1.8.3.2. Range de endereços IPS;

1.8.3.3. Sistema operacional;

1.8.3.4. Grupos de máquinas espelhados do Active Directory;

1.8.3.5. Usuários ou grupos do Active Directory;

1.8.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

1.8.5. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

1.8.5.1. Nenhum;

1.8.5.2. Somente bloqueios;

1.8.5.3. Somente regras específicas;

1.8.5.4. Todas as aplicações executadas;

1.8.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs;

1.8.7. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;

1.8.8. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

1.8.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

1.8.10. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;

1.8.11. As políticas de segurança devem permitir o controle através de regras de aplicação;

1.8.12. As regras de controle de aplicação devem permitir as seguintes ações:

1.8.12.1. Permissão de execução;

1.8.12.2. Bloqueio de execução;

1.8.12.3. Bloqueio de novas instalações;

1.8.13. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

1.8.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

1.8.14.1. Assinatura sha-1 do executável;

1.8.14.2. Atributos do certificado utilizado para assinatura digital do executável;

1.8.14.3. Caminho lógico do executável;

1.8.14.4. Base de assinaturas de certificados digitais válidos e seguros;

1.8.15. As regras de controle de aplicação devem possuir categorias de aplicações;

1.8.16. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

1.8.17. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

1.8.18. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

1.8.19. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

## 1.9. Proteção contra vazamento de informações – DLP

1.9.1. O Controle de Dispositivo assegura a proteção dos dados pessoais ao restringir o acesso do usuário a dispositivos instalados no computador ou conectados a este, incluindo:

1.9.1.1. Dispositivos de armazenamento de dados (discos rígidos, unidades removíveis, unidades de fita, unidades de CD/DVD)

1.9.1.2. Ferramentas de armazenamento de dados (modens, placas de rede externas)

1.9.1.3. Dispositivos desenvolvidos para conversão de dados de impressão (impressoras)

1.9.1.4. Barramentos de conexão (também referidos simplesmente como "barramentos"), referindo a interfaces para conexão de dispositivos a computadores (como USB, FireWire e Infravermelho)

1.9.2. Abaixo, resumo de funcionalidades:

1.9.2.1. 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.

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

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

1.9.2.4. Capacidade de configurar novos dispositivos específicos por Class ID/Hardware ID

## 1.10. Criptografia

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

1.10.1.1. Windows Server 2003, 2008, 2008 R2 e 2012 (32/64-bit);

1.10.1.2. Windows 7 (x86/x64);

1.10.1.3. Windows 10.

1.10.2. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;

1.10.3. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

1.10.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

1.10.5. Deve possuir suporte ao algoritmo de criptografia aes-256;

1.10.6. Deve possuir a capacidade de exceções para criptografia automática;

1.10.7. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

1.10.8. Deve possuir certificação FIPS 140-2;

1.10.9. Deve possuir funcionalidade de criptografia por software ou hardware;

1.10.10. Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

1.10.11. Deve possuir compatibilidade de autenticação por múltiplos fatores;

1.10.12. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

1.10.13. Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

1.10.14. Deve possuir políticas por usuários, grupos e dispositivos;

1.10.15. Deve possuir desbloquear um disco com no mínimo os seguintes métodos: Sequência de cores; Autenticação com ad; Single sign-on com ad; Senha pré-definida; Número pin e Smart card;

1.10.16. Deve possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

1.10.17. Deve possuir mecanismos de criptografia transparentes para o usuário;

1.10.18. Deve possuir mecanismos para wipe (limpeza) remoto;

1.10.19. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

1.10.20. Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

1.10.21. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

1.10.22. Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

1.10.23. O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

1.10.24. O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

1.10.25. O ambiente de autenticação pré-inicialização deve permitir a mudança do leiaute do teclado;

1.10.26. O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

1.10.27. O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

1.10.28. Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (mbr – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades da solução de criptografia e visualizar, testar e modificar as configurações de rede;

1.10.29. O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser

controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

1.10.30. Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

1.10.31. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

1.10.31.1. Microsoft bitlocker;

1.10.31.2. Apple filevault;

1.10.32. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

1.10.33. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

1.10.34. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

1.10.35. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

1.10.36. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho e quando a estação é inicializada;

1.10.37. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

1.10.38. Deve possibilitar que cada política tenha uma chave de criptografia única;

1.10.39. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

1.10.39.1. Chave do usuário: somente o usuário tem acesso aos arquivos;

1.10.39.2. Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

1.10.39.3. Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

1.10.40. Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

1.10.41. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

1.10.42. Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

1.10.43. Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

1.10.44. Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

1.10.45. Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

1.10.46. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

1.10.47. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

1.10.48. Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

1.10.49. Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

1.10.50. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

1.10.51. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

1.10.52. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

1.10.53. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

1.10.54. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

## 1.11. Proteção a smartphones e tablets

1.11.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais: IOS, Android, Windows mobile e Windows phone;

1.11.2. As funcionalidades estarão disponíveis de acordo com cada plataforma;

1.11.3. Deve permitir o provisionamento de configurações de: Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

1.11.4. Deve possuir proteção de anti-malware;

1.11.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

1.11.6. Deve possuir capacidade de detecção de spam proveniente de SMS;

1.11.7. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

1.11.8. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

1.11.9. Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

1.11.10. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

1.11.11. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

1.11.12. Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

1.11.13. Controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; e Bloqueio por tentativas inválidas;

1.11.14. Controle de acesso à seguintes funções e status dos dispositivos móveis: Bluetooth; Câmera; Cartões de memória; Wlan/wifi; Aceitar TLS não confiável; Instalação de aplicativos; Sincronia automática enquanto em modo roaming; Dados de diagnostico; Itunes quando houver; Imessage; Remoção de aplicativos; Browser / Navegadores internet incluindo Safari; Javascript; Popups; Aceitação de cookies; Captura de tela; Siri quando houver; Discagem por voz; Youtube; Abertura de documentos de aplicativos gerenciados em aplicativos terceiros; GPS;

Microsoft Activesync; MMS/SMS; Porta infravermelha; Alto-falante; Armazenamento USB; 3g/4g e Ancoragem (tethering)

## 1.12. Anti-spam (Appliance de gateway de e-mail- Lote 01 item 01)

1.12.1. Permitir balanceamento de carga (Load Balance) para o mesmo domínio;

1.12.2. Possui gerenciamento de configurações de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente;

1.12.3. Permitir o Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

1.12.4. Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

1.12.5. Possuir a detecção de SPAMs utilizando tecnologia heurística,

1.12.6. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;

1.12.7. Permitir a criação de White e Black Lists para detecção de SPAMs;

1.12.8. Possuir proteção contra Phishings;

1.12.9. Possuir proteção inteligente contra-ataques de Engenharia Social.

1.12.10. Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

1.12.11. Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados ( Exploits) e Ataque de dia-zero (Zero-Day);

1.12.12. Possuir reputação de links que estejam dentro do corpo das mensagens;

1.12.13. Possuir níveis de sensibilidade no bloqueio de mensagens com links de má reputação;

1.12.14. Possuir White List para a checagem de reputação em URL's dentro de mensagens;

1.12.15. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

1.12.16. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

1.12.17. Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

1.12.18. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

1.12.19. Proteção contra Spywares, Dialers, Adwares, e Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

1.12.20. Bloqueio de malware empacotado (packed malware) de forma heurística;

1.12.21. Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (, ), [, ] e assim por diante;

1.12.22. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

1.12.23. Permitir criar filtros definidos pelo tamanho de mensagem;

1.12.24. Possuir proteção contra Graymail;

1.12.25. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

1.12.26. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

1.12.27. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;

1.12.28. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

1.12.29. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

1.12.30. Permitir criar regras distintas para mensagens que entram e saem do ambiente;

1.12.31. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

1.12.32. Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;

1.12.33. Permitir limitar o número de destinatários por mensagem;

1.12.34. Possui regra específica para anexos protegidos por senha

1.12.35. Possuir módulo de Data Loss Prevention (DLP), prevenido ações de vazamento de informações, com regras baseadas em: Palavras chaves; Expressões regulares e Extensões de arquivos.

1.12.36. Possuir verificação de mensagens criptográficas de cliente que suporte os seguintes cipher suítes: AES128-SHA; DHE-RSA-AES128-SHA; AES256-SHA; ADH-RC4-MD5; RC4-SHA; RC4-MD5;DHE-DSS-AES128-SHA e IDEA-CBC-SHA;

1.12.37. Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

1.12.38. Permitir a configuração individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);

1.12.39. Possibilidade de exceções ao bloqueio por reputação com base em pais range de ip ou ip

1.12.40. Configurar nível de sensibilidade da reputação de Ips em até quatro níveis

1.12.41. Permitir configurar o código de erro para mensagens rejeitadas;

1.12.42. Possuir configuração personalizada para cada tipo de ataque: SPAM, Vírus, Dicionário e Mensagens de Retorno (Bounced Mails);

1.12.43. Permitir personalizar os filtros baseado em: Tempo; Total de mensagens; Porcentagem de mensagens e Ação a ser tomada;

1.12.44. Prevenir contra-ataques de SPAM e de Malwares, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

1.12.45. Prevenir contra ataques DHA (Directory Harvest Attack);

1.12.46. Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas;

1.12.47. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

1.12.48. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

1.12.49. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

1.12.50. Permitir inserção de carimbo no assunto da mensagem;

1.12.51. Permitir a inserção de um header customizado (X-header);

1.12.52. Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;

1.12.53. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

1.12.54. Permitir a inserção de texto no corpo da mensagem;

1.12.55. Permitir customizar a mensagem que será inserida no corpo das mensagens;

1.12.56. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

1.12.57. Permitir inserir variáveis nas notificações, onde informem no mínimo os seguintes dados: Remetente; Destinatário; Assunto; Data; Nome do arquivo detectado; Nome do vírus detectado; Tamanho total da mensagem e seus anexos; Tamanho total do anexo; Número de anexos detectados pela regra; Ação tomada pela ferramenta e Nome da quarentena para onde a mensagem foi enviada;

1.12.58. Permitir configurar ações para mensagens fora do padrão (mensagens malformadas);

1.12.59. Permitir ação personalizada para mensagens com anexos protegidos por senha;

1.12.60. Permitir quarentenar mensagens de SPAM;

1.12.61. Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

1.12.62. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

1.12.63. Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

1.12.64. Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

1.12.65. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

1.12.66. Permitir exclusão automática das mensagens em quarentena;

1.12.67. Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo; Microsoft Active Directory e OpenLDAP.

1.12.68. Permitir o gerenciamento via console web HTTPS suportando no mínimo os navegadores Internet Explorer e Firefox;

1.12.69. A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento;

1.12.70. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

1.12.71. Realizar atualização de vacinas de forma incremental

1.12.72. Realizar atualização da versão do software. A atualização deve permitir conexão através de serviço Proxy;

1.12.73. Possibilidade de configurar o “greeting” SMTP;

1.12.74. Permitir o controle de relay baseado no domínio e/ou endereço IP;

1.12.75. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

1.12.76. Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;

1.12.77. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio;

1.12.78. Permitir a definição de timeout de conexão SMTP

1.12.79. Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único.

1.12.80. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

1.12.81. A solução deve ofertar possibilidade de ter domínio mascarado;

1.12.82. Possuir autenticação via TLS (Transport Layer Security);

1.12.83. Possuir mecanismo de alerta especifico para ataques do tipo Command & Control (C&C).

1.12.84. A solução deve apresentar relatórios criados através de console web;

1.12.85. A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

1.12.86. A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

1.12.87. A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

1.12.88. Possuir integração no mínimo com os seguintes serviços de diretório: LDAP (Microsoft Active Directory, OpenLDAP e Lotus Domino)

1.12.89. A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

1.12.90. A solução deve possibilitar trafego via Secure SMTP;

1.12.91. A solução deve permitir reindexação da base de dados de forma agendada;

1.12.92. É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;

1.12.93. A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;

1.12.94. A solução deve ser oferecida em formato de software appliance;

1.12.95. A solução deve ser gerenciada totalmente por sua console Web, além de possuir interface CLI intuitiva com gerenciamento dedica a solução;

1.12.96. A solução precisa ser compatível com a plataforma de virtualização VmWare ESXi 5.0/5.5

## 1.13. Gerenciamento

1.13.1. A solução deverá ser fornecida em forma de licenças de 01 (um) ou mais softwares e suportar sua instalação em servidor na plataforma Windows 2003 Server ou superior, seja o servidor físico ou virtual;

1.13.2. A solução deverá possuir uma ou mais consoles capazes de consolidar informações coletadas dos módulos de anti-malware, anti-spam, filtro web, proteção de servidores e inspeção avançada de tráfego de forma centralizada ou não;

1.13.3. A solução de gerência deverá ser acessada por console Web suportando no mínimo os browsers Internet Explorer e Firefox.

1.13.4. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS:

1.13.5. Deve possuir integração com Microsoft Active Directory;

1.13.6. Deverá suportar instalação integrada com base de dados MSSQL;

1.13.7. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP;

1.13.8. Deve gerenciar logs das atividades e eventos gerados pela solução;

1.13.9. Deve permitir a criação de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários

1.13.10. Implementar sincronização de hora através de protocolo NTP;

1.13.11. Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);

1.13.12. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados;

1.13.13. Implementar através da interface gráfica mecanismo para configuração de notificações dos alertas;

1.13.14. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução;

1.13.15. Implementar através da interface gráfica mecanismo de Dashboard onde seja possível a visualização das seguintes informações ou similares: Sumário de detecção e proteção, gráfico de top infecções, e gráfico do throughput de tráfego monitorado;

1.13.16. Deverá permitir a geração de relatórios e gráficos parametrizáveis nos formatos html, pdf, xml e csv;

1.13.17. Deve permitir criação de modelos de relatórios customizados;

1.13.18. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

1.13.19. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

1.13.20. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

1.13.21. Deve de permitir a criação de políticas de segurança personalizadas;

1.13.22. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

1.13.22.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

1.13.22.2. Range de endereços IPS;

1.13.22.3. Sistema operacional;

1.13.22.4. Agrupamento lógicos dos módulos.

1.13.23. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

1.13.24. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo configurável;

1.13.25. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações

1.13.26. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

# 1 LOTE 2

**A solução de segurança Firewall, deverá ser de apenas 01 (um) fabricante.**

**Pede-se a renovação de licença da solução de Gerenciamento e cluster intel constante na Account ID 0006735838 e a atualização tecnológica do item 1 do lote 2, também faz referência a account ID 0006735838. Caso a solução ofertada não seja do fabricante CHECKPOINT, este deverá ofertar produtos com as seguintes características:**

2.1 Dimensionamento (LOTE 2 / Item 1 )

2.1.1 Possuir 10 (dez) interfaces 10/100/1000Base-T;

2.1.2 Suportar interface 10/100/1000Base-T dedicada ao gerenciamento fora de banda;

2.1.3 Suportar a expansão para no mínimo 16 (dezesseis) interfaces 10/100/1000Base-T;

2.1.4 Suportar interface de 40 Gbps;

2.1.5 Possuir 01 (uma) Interface Console Serial;

2.1.6 Possuir 01 (uma) de Alimentação Bivolt 100-240 VAC;

2.1.7 Possuir sistema de arrefecimento interno;

2.1.8 Possuir armazenamento interno mínimo de 450 (Quatrocentos e Cinquenta) GBytes com sistema operacional e logs;

2.1.9 Suportar 20 (vinte) firewalls virtuais;

2.1.10 Ser fornecido com kit rack 19” necessário para instalação;

2.2 Performance (serão utilizadas como parâmetro de avaliação as RFC´s 3511 ou 2544)

2.2.1 22 (vinte e dois) Gbps de Throughput de Firewall com pacote de 1518 bytes;
2.2.2 150 (cento e cinquenta) Mil novas conexões por segundo;
2.2.3 03 (três) Milhões de conexões concorrentes;
2.2.4 03 (três) Gbps de Throughput de VPN com AES-128;
2.2.5 03 (três) Gbps de Throughput de IPS;

2.3 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Item 1)

2.3.1 Por funcionalidades de NG - Next Generation Threat Prevention, entende-se: controle granular de aplicações e URL, identificação de usuários, Antivirus e Antibot, IPS e Firewall.
2.3.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
2.3.3 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
2.3.4 O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
2.3.5 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
2.3.6 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
2.3.7 O Gateway de Segurança deve ser capaz de suportar as seguintes funcionalidades gerenciamento unificado de aplicações em uma única plataforma:
2.3.7.1 Stateful Inspection Firewall
2.3.7.2 Intrusion Prevention System
2.3.7.3 User Identity Acquisition
2.3.7.4 Application Control and URL filtering
2.3.7.5 AntiBot e AntiVirus
2.3.7.6 Threat Emulation (Sandboxing)
2.3.7.7 AntiSpam and Email Security
2.3.7.8 IPSec VPN
2.3.7.9 Data Loss Prevention
2.3.7.10 Mobile Access
2.3.7.11 Security Policy Management
2.3.7.12 Logging and Status
2.3.7.13 Event Correlation and Reporting
2.3.8 A solução deverá prover conscientização do usuário final de acordo com as políticas de segurança em tempo real;
2.3.9 A Solução deverá prover inspeção SSL:
2.3.10 A solução deverá suportar PFS (Perfect Forward Secrecy) e suítes ECDHE de criptografia;
2.3.11 A solução deverá possuir suporte para AES-NI, AES-GCM com a finalidade de aumentar o desempenho.

2.4 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Item 2)

2.4.1 Por funcionalidades de NG - Next Generation Threat Prevention, entende-se: controle granular de aplicações e URL, identificação de usuários, Antivirus e Antibot, IPS e Firewall.

2.4.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
2.4.3 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
2.4.4 O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
2.4.5 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
2.4.6 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
2.4.7 O Gateway de Segurança deve ser capaz de suportar as seguintes funcionalidades gerenciamento unificado de aplicações em uma única plataforma:
2.4.7.1 Stateful Inspection Firewall
2.4.7.2 Intrusion Prevention System
2.4.7.3 User Identity Acquisition
2.4.7.4 IPSec VPN
2.4.7.5 Security Policy Management
2.4.7.6 Logging and Status
2.4.7.7 Event Correlation and Reporting
2.4.8 A solução deverá prover conscientização do usuário final de acordo com as políticas de segurança em tempo real;
2.4.9 A Solução deverá prover inspeção SSL:
2.4.10 A solução deverá suportar PFS (Perfect Forward Secrecy) e suítes ECDHE de criptografia;
2.4.11 A solução deverá possuir suporte para AES-NI, AES-GCM com a finalidade de aumentar o desempenho.

2.5 CONTROLE DE POLÍTICAS DE FIREWALL DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Itens 1 e 2)

2.5.1 A solução deve incluir appliance do próprio fabricante ou servidores Open Server de outros fabricantes sendo eles listados em uma base de compatibilidade de hardware (HCL).
2.5.2 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado;
2.5.3 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;
2.5.4 Deve suportar atuação como cliente NTP (Network Time Protocol) nas versões 1, 2, 3 e 4;
2.5.5 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;
2.5.6 O hardware deve ser baseado em arquitetura aberta usando processadores Intel ou AMD a fim de manter flexibilidade e adaptação a novas ameaças sem impacto na performance;
2.5.7 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-

interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

2.5.8 A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;

2.5.9 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos;

2.5.10 A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança;

2.5.11 A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos, permitindo a pesquisa dos mesmos em todo o log orientado aos sentidos vertical, horizontal e transversal, sendo necessário apenas a informação da string de texto no campo de pesquisa para que seja feito o filtro dos eventos NGFW de forma agregada e multidisciplinar (trazendo a trilha das diversas funcionalidades relacionadas a esta pesquisa);

2.5.12 As regras deverão ser construídas utilizando objetos de rede baseadas no protocolo IP. Durante a criação da regra, tais objetos deverão ser associados automaticamente às suas interfaces de rede correspondentes, sem que haja necessidade de o administrador associar, na regra, qual é a interface de rede origem da conexão, nem a interface de rede destino da conexão. Não será aceito definição de interface com a variável “any”;

2.5.13 Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas.

2.5.14 Deverá possibilitar a implementação de balanceamento de links em modos de Ativo/Ativo ou Ativo/Passivo.

2.5.15 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.

2.5.16 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;

2.5.17 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS, certificados digitais e dispositivos biométricos

2.5.18 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;

2.5.19 Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades;

2.5.20 Implementar roteamento e encaminhamento baseado em políticas;

2.5.21 Deve implementar roteamento multicast (PIM-SM);

2.5.22 Possuir funcionalidade de DHCP Relay e DHCP Server;

2.5.23 Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras;

2.5.24 Possuir base de regras singular sem separação de regras orientadas a versão de endereço IP utilizada;

2.5.25 Prover a otimização administrativa e lógica quando referenciado há um mesmo host com as duas versões do endereço IP sem a multiplicação de objetos e regras;
2.5.26 Implementar sub-interfaces ethernet lógicas;
2.5.27 Deve suportar os seguintes tipos de NAT:
2.5.27.1 Nat dinâmico (Many-to-1);
2.5.27.2 Nat dinâmico (Many-to-Many);
2.5.27.3 Nat estático (1-to-1);
2.5.27.4 NAT estático (Many-to-Many);
2.5.27.5 Nat estático bidirecional 1-to-1;
2.5.27.6 NAT de Origem;
2.5.27.7 NAT de Destino;
2.5.28 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;
2.5.29 Deve implementar roteamento estático IPv4 e IPV6;
2.5.30 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4;
2.5.31 Deve implementar roteamento dinâmico (OSPFv3) para IPv6;
2.5.32 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing);
2.5.33 Deve suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;:
2.5.34 A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através de padrões de análise de protocolo tais como de Tipo de Protocolo ou Inspeção de SSH;
2.5.35 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
2.5.36 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
2.5.37 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos seguintes modos: camada 2 (l2) e camada 3 (l3);
2.5.38 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;
2.5.39 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações.
2.5.40 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QoS e protocolos de roteamento dinâmico devem operar durante a vigência do contrato, garantindo o suporte e atualizações de software com o fabricante.
2.5.41 Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);
2.5.42 Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo (s) outro (s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede;
2.5.43 Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;

2.5.44 Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações;
2.5.45 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS;
2.5.46 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;
2.5.47 Deve comprovar através de reports do NSS LABS score de 100% em: Stability & reliability"
2.5.48 Deve comprovar através de reports do NSS LABS score mínimo de 97% em:
• Security effectiveness";
2.5.49 Deve estar licenciado e habilitado para uso ilimitado de usuários e endereços de rede de acordo com as funcionalidades deste documento.
2.5.50 O módulo de Firewall oferecido deve ter passado nos testes da NSS Labs para produtos de Firewall com pelo menos 95% de efetividade. Sendo que o mesmo também deve ter 100% de efetividade nos testes de evasão e estar entre os recomendados do relatório;
2.5.51 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;
2.5.52 A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports";
2.5.53 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;
2.5.54 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;
2.5.55 Deverá suportar métodos de autenticação de usuário, cliente e sessão;
2.5.56 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente;
2.5.57 Habilidade de realizar upgrade via SCP ou https via interface WEB;
2.5.58 A solução deve suportar o minimo 20.000 entradas de ARP;
2.5.59 A solução de Firewall deve suportar no mínimo 5000 regras;
2.5.60 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando tiver mais de um administrador executando alterações simultaneamente;
2.5.61 A solução de segurança deve suportar no minimo 30.000 regras de Firewall;
2.5.62 A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços;
2.5.63 A solução deverá disponibilizar uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com zero-downtime;
2.5.64 A Solução ofertada deverá possuir uma única interface para gerenciamento de regras para IPv4 e IPv6.
2.5.65 A solução deverá possuir aceleração de regras de firewall implementado através de software para aumentar a performance da análise das regras de firewall.
2.5.66 A solução deverá possuir a configuração de processadores específicos para cada interface de rede para aumentar a performance da análise das regras de firewall.

2.5.67 Possuir funcionalidade de HTTP e HTTPS proxy.

2.6 CARACTERÍSTICAS DE ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Itens 1 e 2)

2.6.1 Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:
- 2.6.1.1.1 Em modo Transparente:
- 2.6.1.1.2 Em Layer 2;
- 2.6.1.1.3 Em Layer 3;

2.6.2 O HA deve sincronizar:
- 2.6.2.1.1 Todas as sessões;
- 2.6.2.1.2 Certificados de-criptografados;
- 2.6.2.1.3 Todas Associações de Segurança das VPNs;
- 2.6.2.1.4 Todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS;

2.6.3 O HA (modo de Alta-Disponibilidade) deve possibilitar tracking de IP.

2.6.4 Monitoração de falha de link.

2.6.5 Para melhor desempenho ou em caso de crescimento da rede, a solução deve suportar mais de dois membros no cluster de NG Firewall ou NGTP;

2.6.6 A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

2.6.7 Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante;

2.7 CARACTERÍSTICAS DE VPN DA SOLUÇÃO DE SEGURANÇA(LOTE 2 – Itens 1 e 2)

2.7.1 A solução deve suportar CA Interna e CA Externa de terceiros;

2.7.2 A solução pode incluir appliance do proprio fabricante ou servidores de outros fabricantes para atendimento a este item, sendo eles listados em uma base de compatibilidade de hardware. Sendo possivel utilizar solução de terceiro para compor o projeto solicitado;

2.7.3 Solução deve suportar 3DES e AES-256 de criptografia para IKE Fase I e "Suite-B-MCG-128" “Suite-B-GCM-256" para a fase II;

2.7.4 Solução deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 e Grupo 20;

2.7.5 Solução deve suportar a integridade dos dados com MD5, SHA1, SHA-256, SHA-384 e AES-XCBC;

2.7.6 Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

2.7.7 A Solução deve suportar clientless SSL VPN para acesso remoto;

2.7.8 Solução deve suportar VPNs baseadas em redes e VPNs através de rotas com suporte a protocolos de roteamento dinâmico;

2.7.9 Solução deve incluir a capacidade de estabelecer VPNs com gateways de IPs públicos dinâmicos;

2.7.10 Solução deve incluir compressão IP para client-to-site e VPN site-to-site;

2.7.11 Suportar IPSec VPN:

2.7.12 Criptografia DES, 3DES, AES128, AES256, AES-GCM-128 e AES-GCM-256;

2.7.13 Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
2.7.14 Diffie-Hellman Group 1, Group 2 e Group 5, Group 14, Group 19, Group 20;
2.7.15 Algoritmo Internet Key Exchange (IKE) versões I e II;
2.7.16 AES 128 ou 192 e 256 (Advanced Encryption Standard).

2.8 CARACTERÍSTICAS DE CONTROLE DE APLICAÇÕES WEB 2.0 DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Itens 1)

2.8.1 A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB 2.0;

2.8.2 A solução deve ser capaz de identificar qualquer tipo de aplicação Web 2.0 em até camada 7 independente de porta e protocolo;

2.8.3 Possuir um reconhecimento de pelo menos 6500 aplicações diferentes, incluindo categorização para tráfego relacionado a aplicações peer-to-peer, redes sociais, acesso remoto, update de software, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

2.8.4 Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, social widgets com controle granular para usuários ou grupos de usuários;

2.8.5 A solução deverá prover controle de segurança granular de ao menos 250.000 Web 2.0 widgets;

2.8.6 A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

2.8.7 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund);

2.8.8 Deve possibilitar não apenas o bloqueio das aplicações, mas também de portas e protocolos. Deve ainda distinguir protocolos de aplicações, por exemplo o protocolo GRE não deve ser tratado como aplicação na política.

2.8.9 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle,

active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

2.8.10 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;

2.8.11 Solução deve ser capaz de criar regras com várias categorias.

2.8.12 Deve possibilitar a permissão ou bloqueio de aplicações por pelos menos os seguintes critérios:

2.8.13 Aplicação da Web;

2.8.14 Categorias;

2.8.15 Nível de risco;

2.8.16 IP/Range de IP's/Redes;

2.8.17 Usuários do AD/LDAP;

2.8.18 Diferentes grupos de usuários;

2.8.19 Aplicações que sejam passiveis a técnicas de evasão por malwares e uso excessivo de banda como (ultrasurf, torrent, dropbox e file sharing);

2.8.20 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

2.8.21 Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e gerência;

2.8.22 Devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

2.8.23 Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas localmente, ou, através de ticket direto com o fabricante.

2.8.24 Deve possibilitar a customização, por regra, da tela de interação com o usuário, permitindo: informar, questionar e limitar a banda de acesso;

2.8.25 Deve permitir diferentes "telas" de interação com o usuário para dispositivos móveis;

2.8.26 Deve possibilitar a diferenciação e controle granular específico das aplicações: Gmail, Gmail Enterprise, Gmail-Drive, Gmail-file-transfer, Gmail-file-transfer-download, Gmail-file-transfer-upload, Inbox-by-Gmail, Gmail-chat, Gmail-video-chat, Gmail-Voice-Chat, Gmail-Voice-Video-Chat, Gmail-call-phone, Viber, Viber-file-transfer, Viber-Voice-Call, Viber-Voice-message, WhatsApp-Messenger, WhatsApp-Messenger-file-transfer, WhatsApp-Messenger-Web, WhatsApp-Messenger-Voice-Call;

2.8.27 Deve permitir o bloqueio de aplicações Proxies: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield

2.8.28 Deve permitir o bloqueio de aplicações: AirVPN, ClickTools, G-Cloud-Backup, Hide.Me, Intacct, JumboMail, JumboMail-Download, JumboMail-

Upload, JumboMail-Share, Nearby, PubNub, Sfax, Zapier, pCloud, skyZIP, AeroFS, Rocket-League, Tresorit, okta, Alexa, HubSpot, PingOne e VPN-Shield;

2.8.29 Deve possibilitar a integração da solução com base do Active Directory, Ldap, Radius ou base local para criação de políticas. Possibilitando a criação de regras utilizando:

2.8.30 Usuários;

2.8.31 Grupo de usuários;

2.8.32 Máquinas (estações de trabalho);

2.8.33 Endereço IP;

2.8.34 Endereço de Rede;

2.8.35 Combinação das opções acima;

2.8.36 A solução deve suportar a criação de mais de 500 regras de controle de aplicações no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso não permitido pelo orgão;

2.8.37 Possuir controle granular para quais funcionalidades de proteção, endereços IPs será executada a inspeção e de-criptografia de SSL tanto para tráfego de entrada (Inbound) e Saída (Outbound).

2.8.38 A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem para um período de tempo específico;

2.8.39 Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

2.8.40 Deve possibilitar a customização por regra utilizando as seguintes ações de controle:

2.8.40.1 Permitir;

2.8.40.2 Bloquear;

2.8.40.3 Monitorar;

2.8.40.4 Informar o usuário;

2.8.41 O mecanismo de Controle de aplicação deve apresentar contagem de utilização de regra de acordo com a utilização;

2.8.42 A solução deverá possuir uma interface de fácil utilização para buscas de Aplicações;

2.8.43 A solução deverá categorizar por Fator de Risco aplicações;

2.8.44 A solução deverá receber atualizações via internet para sua base;

2.8.45 A solução de ser capaz de identificar qualquer tipo de aplicação Web em até camada 7 independente de porta e protocolo;

2.8.46 A solução deverá possuir um mecanismo para informar ou perguntar ao usuário em tempo real com a finalidade de educá-los ou confirmar ações baseadas na política de acesso;

2.8.47 A solução deverá permitir a criação de exceções baseadas em objetos de rede;

2.8.48 A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;

2.8.49 A funcionalidade de Aplicação e filtros deverá possuir relatório de utilização.

2.9 CARACTERÍSTICAS DE IDENTIFICAÇÃO DE USUÁRIO COMUNS DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Itens 1 e 2)

2.9.1 Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP e Radius;

2.9.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.9.3 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.9.4 Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

2.9.5 Deve possuir suporte a identificação de múltiplos usuários conectados com um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular;

2.9.6 A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

2.9.7 Deve suportar autenticação para Smartphone e tablet's;

2.9.8 Deve suportar autenticação Kerberos transparente para single sign on;

2.9.9 A solução deverá compartilhar e propagar a identificação de usuários com outros gateways de segurança do mesmo fabricante;

2.9.10 Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

2.9.11 A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

2.9.12 A solução de identificação de usuário deve suportar engine onde assume que um único usuário está conectado por computador;

2.9.13 A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

2.9.14 A solução deve integrar-se perfeitamente com serviços de diretório, IF-MAP e Radius;

2.9.15 A solução deve permitir a identificação de usuários através de proxy via "X-forward headers";

2.9.16 A solução deverá suportar grupos LDAP "nested";

2.10 CARACTERÍSTICAS DE PREVENÇÃO DE AMEAÇAS (IPS) DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Itens 1 e 2)

2.10.1 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall sem a necessidade de uso de quaisquer interfaces externas onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança;

2.10.2 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;

2.10.3 A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho sem degradar a performance do equipamento solicitado neste edital;
2.10.4 A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;
2.10.5 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;
2.10.6 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
2.10.7 Em cada proteção de segurança, deve estar incluso informações como: código CVE, tipo de impacto na ferramenta, severidade, e tipo de ação que a mesma irá executar;
2.10.8 A solução deve fazer captura de pacotes para proteções específicas;
2.10.9 Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força a bruta a scanning de portas CIFS, Port overflow, Non Compliant SSL, IKE aggressive Exchange;
2.10.10 Deve ser capaz de bloquear tráfego SSH enviados em outras portas.
2.10.11 A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;
2.10.12 A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;
2.10.13 As regras de exceção devem possuir: origem, destino e serviço;
2.10.14 A solução deve ser capaz de inspecionar tráfego HTTPS (inbound/Outbound);
2.10.15 Proteger o ambiente de ataque DoS;
2.10.16 Baseado nas melhores práticas de segurança e otimização de tempo operacional dos administradores, a solução de IPS integrada no appliance de segurança, deve possuir uma base de assinaturas de segurança superior a 5000 (cinco mil) snassinaturas;
2.10.17 A solução de IPS deve possuir funcionalidade de simulação ou detecção do tráfego processado para fins de troubleshooting;
2.10.18 Na própria interface de gerência, a solução de IPS deve possuir índices por período (hora, semana ou mês) onde aponta o nível de ação das assinaturas baseada pela sua severidade;
2.10.19 Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os appliances que estão sendo gerenciados informando no mínimo: Nome do Gateway, Endereços IP nas versões 4 e 6, Perfil Utilizado, Informação de status da funcionalidade de bypass e modo de operação (bloqueio ou detecção).
2.10.20 Para melhor administração da solução, a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;
2.10.21 A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção) das assinaturas recentemente baixadas

via atualização sem alterar o padrão operacional do IPS previamente configurado;

2.10.22 O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de mail, Web e DNS, onde as mesmas poderão ser assinaladas no momento da criação do objeto de rede na solução;

2.10.23 Deverá possibilitar a inclusão de novas assinaturas e customização no formato SNORT;

2.10.24 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

2.10.25 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

2.10.26 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP;

2.10.27 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

2.10.28 A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados

2.10.29 Permitir: o redirecionamento do tráfego bloqueado via IPS para outras URL`s, demonstração do código de erro e definição da mensagem de bloqueio;

2.10.30 Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

2.10.31 A solução deve permitir a pré-configuração de no mínimo 15 perfis de proteção de IPS que podem ser utilizados a qualquer momento;

2.10.32 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo das opções granulares em: última hora, últimas 24 horas, última semana e último mês;

2.10.33 A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;

2.10.34 A solução deve permitir a configuração de políticas baseada em países, dispondo de pelo menos 220 países já cadastrados em sua base;

2.10.35 A solução deve possuir os seguintes esquemas de Update de assinaturas:

2.10.35.1 Update instantâneo, através de um click;

2.10.35.2 Update através de agendamento onde engloba horário, dias da semana ou dia do mês;

2.10.35.3 Update de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

2.10.36 A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP de entrada. Depois de importar esses certificados, a solução deve permitir o uso desses certificados na configuração de regra de IPS para Inspeção segura HTTP;

2.10.37 Dentro da engine de inspeção HTTPS, a solução deve permitir a criação de diferentes regras onde será especificado: origem, destino, tipo de serviço, ação e certificado que será atribuído por regra;

2.10.38 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

2.10.39 A solução deverá permitir a criação de perfil de proteção baseado em hosts internos ou servidores ou a combinação dos dois;
2.10.40 A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato;
2.10.41 A solução deverá possuir proteções para sistemas SCADA;
2.10.42 A solução deverá inspecionar o protocolo Citrix com a finalidade de comprovar que o tráfego é realmente o protocolo Citrix ICA;
2.10.43 Solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados;
2.10.44 Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

## 2.11 CARACTERÍSTICAS DE CONTROLE DE URL DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Item 1)

2.11.1 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado ao Firewall NG;
2.11.2 A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem de URL para um período de tempo específico;
2.11.3 Deve possuir as seguintes funcionalidades de filtro de URL:
2.11.3.1 Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
2.11.3.2 Deve ser possível a criação de políticas por Usuários e Grupos de Usuários cadastradas no AD, Ips, Redes e Grupos de Redes.
2.11.4 A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
2.11.5 O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;
2.11.6 Deverá ser possível questionar o usuário e obrigar o mesmo a justificar na própria página a necessidade do acesso, permitindo assim o registro em logs passíveis de auditoria;
2.11.7 A solução de Filtro de URL deverá ser totalmente integrada com a solução de Aplicações WEB 2.0 para melhor gerenciamento e controle Next Generation;
2.11.8 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund), sendo que para a opção de OUTBOUND não será necessário efetuar o MITM (Man In The Middle), ou seja, a solução deverá prover algum mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso de acordo com a política configurada;
2.11.9 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.11.10 A solução deve possuir engine de bloqueio de conteudo em sites de busca como (Google, Bing e Yahoo). Assim como o bloqueio de sites que estão em modo cashed;

2.11.11 Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

2.11.12 Deve possibilitar a customização por regra com as seguintes ações de controle:

2.11.12.1 Permitir;

2.11.12.2 Bloquear;

2.11.12.3 Monitorar;

2.11.12.4 Informar o usuário;

2.11.13 Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no appliance (Captive Portal);

2.11.14 Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.

2.11.15 Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs;

2.11.16 Deverá possuir pelo menos 60 categorias de URLs;

2.11.17 Deverá possibilitar a criação de Categorias de URLs customizadas;

2.11.18 Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

2.11.19 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categoriza ou categorizada incorretamente;

2.11.20 A solução deve suportar a criação de mais de mais de 500 regras de controle URL no mesmo dispositivo de de segurança, permitindo o controle granular de qualquer tipo de acesso não permitido pelo orgão;

2.11.21 Deve possibilitar a customização de pagina de bloqueio de interação com usuário;

2.11.22 Devem incluir informações das atividades dos usuários em seus logs;

2.11.23 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL.

## 2.12 CARACTERÍSTICAS DE ANTI-MALWARE (Antibot e Antivirus) DA SOLUÇÃO DE SEGURANÇA (LOTE 2 – Item 1)

2.12.1 Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança ou entregue em composição com outro fabricante desde que integrado à gerência centralizada de administração, monitoração e logs;

2.12.2 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

2.12.3 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

2.12.4 Implementar funcionalidade de detecção e bloqueio de callbacks;

2.12.5 A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;
2.12.6 A solução Antibot deve possuir mecanismo de detecção em multi-camadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação, assinaturas e análise de mensagens de email;
2.12.7 Implementar gerenciamento SNMP v1, v2 e v3;
2.12.8 Implementar atualização da base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização;
2.12.9 Implementar mecanismo de múltiplas fases para verificação de malware e/ou códigos maliciosos;
2.12.10 Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS ou Console do proprio fabricante;
2.12.11 Implementar importação de certificados digitais padrão X.509;
2.12.12 Implementar interface CLI segura através do protocolo SSH;
2.12.13 Implementar base de usuários local e consulta a base de usuários externa através dos protocolos TACACS+, RADIUS e LDAP;
2.12.14 Implementar sincronização de hora através de protocolo NTP;
2.12.15 Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);
2.12.16 Implementar gerenciamento centralizado das licenças de utilização da solução, incluindo adição e remoção de licenças;
2.12.17 A solução deve analisar e bloquear malware e/ou codigos maliciosos pelo menos nos seguintes tipos de arquivos: bat, com, exe, dll, vsd, reg, jar, txt, swf, cmd, mpg, jse, midi, mp3, hlp, php, png, TIF, WAV, ASF, HTM, COM, JPEG;
2.12.18 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP e CIFS;
2.12.19 A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou Rede, sendo possível escolher um Profile diferente para cada regra;
2.12.20 A solução de Anti-Virus deve permitir o bloqueio de download de arquivos que excedam o tamanho pré-defnido;
2.12.21 A solução de inspeção de vírus não deverá possuir limitação para o tamanho dos arquivos inspecionados (a limitação é baseada na quantidade de memória/Disco), sendo ela capaz de customizar o tamanho do arquivo inspecionado, assim como a ação caso o tamanho seja excedido;
2.12.22 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções, e gráfico da taxa de transferência de tráfego monitorado;
2.12.23 A solução deve permitir criar regras de exceção de acordo com a proteção a partir do log visualizado na interface gráfica da gerencia centralizada;
2.12.24 Implementar através da interface gráfica de administração, configuração de mecanismo de alerta onde seja possível configurar bloqueio/desbloqueio de uma comunicação do tipo callback;
2.12.25 A solução deve ser capaz de bloquear uma conexão até que a classificação da mesma seja completada.

2.12.26 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;
2.12.27 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
2.12.28 Implementar através da interface gráfica, pesquisa aos eventos já reconhecidos;
2.12.29 A solução deve permitir geração de relatórios, os quais devem apresentar via interface gráfica os seguintes informações no relatório:
2.12.29.1 - sumário executivo;
2.12.29.2 - relatório de servidores de callback;
2.12.29.3 - relatório de hosts infectados;
2.12.29.4 - Atividade de malware e detalhes dos Alertas.
2.12.30 A solução deve possuir na própria interface de gerência, gráfico contento informações em tempo real sobre as atividades recentes de malwares detectados na solução, sendo que essas informações deverão ser apresentadas em Mapa geografica por pais, através de IP ou URL e principais e-mails que foram scaneados;
2.12.31 Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;
2.12.32 A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do Fabricante;
2.12.33 A solução deve permitir a criação de White list baseado no MD5 do arquivo;
2.12.34 Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
2.12.35 Em caso de falha no mecanismo de inspeção do Anti-Virus, deve ser possível configurar se as conexões serão permitidas ou bloqueadas;
2.12.36 A solução de anti-bot e anti-virus, deve possuir recurso onde o administrador consiga criar as regras de política de segurança, permitindo salva las e posteriormente aplicar para entrar em modo detect/inspect.
2.12.37 Caso o administrador tenha realizado alteração na solução de anti-virus ou bot, essa funcionalidade deve possuir opção de aplicação de regra apenas nesta engine, sem interferir nas demais regras de outras funcionalidades de segurança. Assim evitando confronto com alteração de outras funcionalidades;
2.12.38 A solução deve ser capaz de procurar por ações de BOTs.
2.12.39 A solução deve suportar a detecção e prevenção de vírus Cryptors & ransmoware;
2.12.40 A solução deverá possuir mecanismo para proteger contra ataques de Spear phishing.
2.12.41 A solução deve ser capaz de proteger contra diversos ataquer DNS, como:
2.12.42 Analisar padrões de comunicação C&C e não apenas o servidor DNS destino
2.12.43 Funcionalidade DNS TRAP, que visa auxiliar na descoberta de hosts infectados que geram comunicação com C&C
2.12.44 Capacidade para detectar e Previnir ataque DNS tunneling
2.12.45 A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares
2.12.46 A solução deve ser capaz de previnir acesso a websites maliciosos
2.12.47 A solução deve ser capaz de realizar inspeção de tráfego SSL

2.12.48 A solução deverá receber atualizações de um serviço baseado em cloud.
2.12.49 A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.
2.12.50 A solução deverá ser capaz de inspecionar arquivos comprimidos.
2.12.51 A solução Antivirus deverá suportar a análise de links no corpo de emails.
2.12.52 A solução Antivirus deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS

**A solução de segurança ofertada deve possuir gerenciamento nativo através da plataforma de gerenciamento SMART (CPAP-SM504) existente na TERRACAP. Caso a solução ofertada não possua o gerenciamento nativo, deve ser contemplada como parte integrante da solução, uma plataforma de gerenciamento composta por 01 (um) ou mais softwares/appliances com as seguintes funcionalidades:**

## 2.13 CONSOLE DE GERÊNCIA E MONITORAÇÃO (LOTE 2 – Itens 1 e 2)

2.13.1 A solução de gerência deverá ser separada do Gateway de segurança onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto assim como logs e relatórios de forma unificada;
2.13.2 A solução de gerência deverá possibilitar sua instalação em ambiente virtualizado;
2.13.3 Deverão estar contempladas todas a licenças necessárias para gerenciamento de todas as soluções de segurança tipos 1, 2 e 3;
2.13.4 Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;
2.13.5 A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, WebGUI utilizando protocolo HTTPS, console e com possibilidade API aberta;
2.13.6 Caso haja a necessidade de instalação de algum software para a administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows ou Linux;
2.13.7 Implementar gerenciamento centralizado das licenças de utilização da solução, incluindo adição e remoção de licenças;
2.13.8 A solução de gerencia centralizada deverá ser composta por um unica console de gerenciamento, sem a necessidade de consoles adicionais para qualquer tipo de administração e analise de logs dos appliances e funcionalidades solicitadas neste edital;
2.13.9 Deve permitir a utilização de palavras chaves e cores para facilitar a identificação de regras na interface gráfica;
2.13.10 A solução deve proporcionar a opção de adicionar alta disponibilidade, utilizando um servidor ou appliance em standby que é automaticamente sincronizado com o servidor ou appliance primário;
2.13.11 Para melhor análise e administração do ambiente de segurança, a solução deve prover graficamente para cada regra, a informação da utilização da mesma através de “hit count”, com no mínimo as seguintes informações:

- Visualização do percentual de utilização em relação a outras regras;
- Informar a primeira e última vez que a regra foi utilizada, de acordo com a política estabelecida;

2.13.12 Deve incluir a capacidade de confiar em CAs externas com a opção de verificar o certificado de cada gateway externo através de, no mínimo, DN e IP;

2.13.13 A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

2.13.14 A gerência deve possuir console de Log onde deve ter a capacidade de visualizar os logs de segurança em tempo real permitindo ao administrador realizar as devidas análises para fins de troubleshooting;

2.13.15 A solução de gerência, deverá prover fácil administração na aplicação das políticas para os Gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, onde pode ser aplicada nos Gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho de configuração e aplicação de regra;

2.13.16 Deve possuir engine de visualização gráfica da topologia dos firewalls gerenciados, pela console centralizada;

2.13.17 Solução deve incluir o status de todos os túneis VPN, site-to-site e client-to-site sendo eles:

2.13.17.1Túneis permanentes e seu estado de conexão;

2.13.17.2Túneis;

2.13.18 A solução deverá prover informações gerais de cada gateway como volume de pacotes aceitos, conexões concorrentes, novas conexões e licenciamento informando o seu prazo de validade;

2.13.19 A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possivel a retenção temporaria local no appliance de segurança.

2.13.20 A solução de monitoração deverá ser capaz de possuir filtro onde consegue monitorar todos os usuários remotos logados;

2.13.21 A filtragem de logs deve ser intuitiva, ou seja, através do fornecimento de uma palavra chave, idêntico a pesquisa do Google, é disponibilizado a visualização dos logs filtrados atualizados com qualquer semelhança a palavra chave digitada;

2.13.22 Solução deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;

2.13.23 A solução dever ser capaz de criar filtro que permita a visualização de múltiplos logs como:

2.13.23.1.1 Top origem;

2.13.23.1.2 Top destino;

2.13.23.1.3 Principais acessos a determinados serviços;

2.13.23.1.4 Principais ações;

2.13.23.1.5 Principais funcionalidades de segurança utilizadas do Firewall;

2.13.23.1.6 Principais regras que foram utilizadas de acordo com o filtro criado;

2.13.23.1.7 Principais aplicações web utilizada de acordo com a funcionalidade de segurança disponível no Firewall;

2.13.24 Com o intuito de melhorar a rapidez na pesquisa de eventos e abrangência de período de busca do log, a solução ter a capacidade de possuir logs indexados;

2.13.25 Permitir o filtro de logs através da utilização de objetos populados na base de regras do NGFW ao invés de digitar o endereço IP do host;

2.13.26 Permitir pesquisa de logs através de informações do código de protocolo IP e porta de origem;
2.13.27 Deve prover filtros pré-definidos de eventos com maior importância;
2.13.28 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows;
2.13.29 A solução de gerência centralizada deverá possuir capacidade de analisar logs e eventos com intuito de mitigar qualquer anomalia no ambiente independente do appliance de segurança estar sob ataque ou elevado consumo de CPU e memória;
2.13.30 Deve manter um canal de comunicação seguro, com criptografia baseada em certificados, entre todos os componentes que fazem parte da solução de segurança, gerência, gateways, armazenamento de logs e emissão de relatórios;
2.13.31 Possuir autoridade certificadora interna para geração de certificados;
2.13.32 A solução de logs da gerência dever ter a capacidade de criar múltiplos filtros customizados, sendo possível salvar em favoritos para visualizar em um momento posterior ou através de uma rotina constante;
2.13.33 Permitir nas regras de Firewall, Controle de Aplicação e URL a ação excessão para host e serviço;
2.13.34 A solução deve ser capaz de criar regras de exceção para determinado tipo de proteção a partir do log apresentado na solução;
2.13.35 O gerenciamento deve permitir:
2.13.35.1 Criação e administração de políticas de Firewall, Controle de aplicação e IPS;
2.13.35.2 Criação e administração de políticas de Antivírus e Anti-Malware;
2.13.35.3 Criação e administração de políticas de Filtro de URL e prevenção contra ameaças avançadas;
2.13.35.4 Criação e administração de políticas de VPNs IPSec e SSL;
2.13.35.5 Monitoração de logs;
2.13.35.6 Ferramentas de investigação de logs;
2.13.35.7 Debugging;
2.13.35.8 Captura de pacotes;
2.13.35.9 Acesso concorrente de administradores;
2.13.36 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
2.13.37 Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
2.13.38 Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
2.13.39 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
2.13.40 Autenticação integrada à base de dados local ou servidor Radius;
2.13.41 Localização de em quais regras um endereço IP, Range de IP, subrede ou objetos estão sendo utilizados;
2.13.42 Deve atribuir sequencialmente um número a cada regra de Firewall, NAT e QoS;
2.13.43 Criação de regras que fiquem ativas em horário definido;
2.13.44 Criação de regras com data de expiração;

2.13.45 Backup das configurações e rollback de configuração para a última configuração salva;
2.13.46 Suportar Rollback de Sistema Operacional para a última versão local;
2.13.47 Habilidade de upgrade via SCP ou TFTP e interface de gerenciamento;
2.13.48 Validação de regras antes da aplicação;
2.13.49 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
2.13.50 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
2.13.51 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
2.13.52 Deve ser possível exportar os logs em CSV;
2.13.53 Rotação do log;
2.13.54 Exibição das seguintes informações, de forma histórica e em tempo real:
2.13.54.1 Situação do dispositivo e do cluster;
2.13.54.2 Principais aplicações;
2.13.54.3 Principais aplicações por risco;
2.13.54.4 Administradores autenticados na gerência da plataforma de segurança;
2.13.54.5 Número de sessões simultâneas;
2.13.54.6 Status das interfaces;
2.13.54.7 Uso de CPU;
2.13.55 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
2.13.56 Permitir a pesquisa na base de logs através de operadores boleanos e sintaxes "yesterday" e "today";
2.13.57 Gerar alertas automáticos via:
2.13.57.1 Email;
2.13.57.2 SNMP;
2.13.57.3 Syslog;
2.13.58 Deverá ser compatível com a solução de proteção de rede e permitir o gerenciamento centralizado de diversos equipamentos;
2.13.59 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
2.13.60 Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
2.13.61 O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível/homologado com/para VMware ESXi;
2.13.62 Deve consolidar logs de todos os dispositivos administrados;
2.13.63 Deve permitir exportar backup de configuração automaticamente via agendamento;
2.13.64 Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
2.13.65 Permitir que os logs de auditoria tenham identificação;
2.13.66 Permitir que todas as alterações em objetos gerem log de auditoria;
2.13.67 Permitir que todas as alterações das regras gerem log de auditoria;

2.13.68 Deve possuir mecanismo para identificar e informar aos administradores problemas de configuração de anti-spoofing;
2.13.69 Deve possuir mecanismo para checar e informar sobe uso de disco rígido, uso de memória, licenças, usuários e políticas da gerência centralizada;
2.13.70 A gerência centralizada deve prover no mínimo, em tempo real, a visualização estatística, gráfica linear e barras, das informações:
2.13.70.1 Visualização da quantidade de tráfego utilizado de aplicações e navegação;
2.13.70.2 Informações Gráficos;
2.13.70.3 Informações Estatísticas;
2.13.70.4 Interfaces mais utilizadas;
2.13.70.5 Serviços mais utilizados;
2.13.70.6 Destinos mais utilizados;
2.13.70.7 Volume de tráfego de entrada por regra;
2.13.70.8 Volume de tráfego de saída por regra;
2.13.70.9 Distribuição de pacotes em faixas de tamanho dos mesmos referenciado o volume e quantidade de pacotes por segundo;
2.13.70.10 Uso de CPU;
2.13.70.11 Número de conexões;
2.13.70.12 Taxa do número de pacotes por segundo aceitos;
2.13.70.13 Taxa do número de pacotes por segundo bloqueados;
2.13.70.14 Throughput;
2.13.70.15 Taxa de conexões por segundo;
2.13.70.16 Taxa de fragmentos processados por segundo;
2.13.70.17 Pico da taxa de pacotes por segundo decriptografados;
2.13.70.18 Taxa de pacotes por segundo decriptografados;
2.13.70.19 Pico da taxa de erros por segundo de decriptografia;
2.13.70.20 Taxa de erros por segundo de decriptografia;
2.13.70.21 Thoughput de decriptografia;
2.13.70.22 Pico da taxa de pacotes por segundo criptografados;
2.13.70.23 Taxa de pacotes por segundo criptografados;
2.13.70.24 Pico da taxa de erros por segundo de criptografia;
2.13.70.25 Taxa de erros por segundo de criptografia;
2.13.70.26 Thoughput de criptografia;

## 2.14 MÓDULO DE RELATÓRIOS E CORRELAÇÃO DE EVENTOS (LOTE 2 – Item 1)

2.14.1 Permitir a análise através de relatório da utilização de aplicações entre período histórico e presente;
2.14.2 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus, AntiMalware e Emulação), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
2.14.3 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e AntiMalware);
2.14.4 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, AntiMalware e Emulação), e URLs que passaram pela solução;
2.14.5 Gerar relatórios, contemplando no mínimo:
2.14.5.1.1 Resumo gráfico de aplicações utilizadas;
2.14.5.1.2 Principais aplicações por utilização de largura de banda;

2.14.5.1.3 Principais aplicações por taxa de transferência de bytes;
2.14.5.1.4 Principais hosts por número de ameaças identificadas;
2.14.6 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e AntiMalware), de rede vinculadas a este tráfego;
2.14.7 Deve permitir a criação de relatórios personalizados;
2.14.8 Disponibilizar relatório gráfico do percentual de eventos por CVE (Common Vulnerabilities and Exposures);
2.14.9 Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;
2.14.10 Deverá possuir mecanismo "Drill-Down" para navegação e análise dos logs em tempo real;
2.14.11 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
2.14.12 Deve incluir uma ferramenta do próprio fabricante ou solução de terceiros para correlacionar os eventos de segurança das funcionalidades adquiridas neste edital, sendo ele capaz de receber eventos de soluções de mercado;
2.14.13 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino;
2.14.14 Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos;
2.14.15 Disponibilizar recursos interativos de navegação nos eventos informados;
2.14.16 Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações: bloqueio da origem, envio de SNMP e envio de e-mail;
2.14.17 A solução deve exportar relatórios via HTML, CSV e MHT;
2.14.18 A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;
2.14.19 A solução deve permitir ao administrador atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador o foco sobre os eventos mais importantes;
2.14.20 A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:
2.14.20.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação;
2.14.20.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
2.14.20.3 Estatísticas com comparativo de período (hora, dia e mês);
2.14.21 Deve permitir a geração de relatórios com horários pré-definidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;
2.14.22 Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por país;
2.14.23 Deve permitir ao administrador o agrupamento de eventos baseado em quaisquer características, incluindo vários níveis de alinhamento;

2.14.24 A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
2.14.25 Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
2.14.26 Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes;
2.14.27 Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado;
2.14.28 Deve suportar a geração de relatório gráfico gerencial, provendo o consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos além do consumo interno dos usuários;
2.14.29 A solução dever ser capaz de criar ticket interno para maior mitigação de eventos, sendo possível editar comentários pelo administrador no momento da mitigação do evento;
2.14.30 Deve implementar, ou utilizar solução de terceiros, no mínimo, os seguintes tipos de correlação de eventos:
2.14.30.1 Compressão: Consiste em reduzir múltiplas ocorrências de um mesmo evento por um único evento, indicando quantas vezes o evento ocorreu durante o período de observação;
2.14.30.2 Filtragem: Consiste em suprimir um determinado evento, em função dos valores de um conjunto de parâmetros, previamente especificados;
2.14.30.3 Contagem: Capacidade de quantificar/contar a ocorrência de um mesmo evento;
2.14.30.4 Escalação: É a capacidade de um evento, através da análise de outros eventos ser considerado de maior importância ou severidade;

## 3 Serviço mensal de suporte técnico (Lotes 1 e 2);

3.1 A execução do serviço mensal de suporte técnico deverá ser realizada por profissional certificado pelo fabricante dos equipamentos, durante o período de licenciamento e garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o contrato e a garantia, podendo essa ser solicitada a qualquer momento;
3.2 O serviço de suporte técnico especializado da CONTRATADA deverá ser realizado em regime de 8x5, no idioma português, devendo a empresa possuir uma central de atendimento sem custos para a CONTRATANTE e atender aos chamados da equipe técnica nos prazos que se seguem:
3.2.1 Em no máximo 02 (duas) hora para suporte telefônico, após a abertura do chamado;
3.2.2 Em no máximo 04 (quatro) horas para suporte no local, após a solicitação de correção de problemas;
3.2.3 Início do atendimento: hora da abertura do chamado técnico;
3.2.4 Término do chamado: momento em que o(s) equipamento(s) torna-se operacional e com todas as funcionalidades disponíveis para uso, com ateste da Coordenação-Geral de Infraestrutura e Serviços da CONTRATANTE;

3.3 Durante o período de vigência do contrato, quando for o caso, todos os firmwares e softwares deverão ser atualizados a cada nova versão ou correção, sem nenhum custo adicional para a CONTRATANTE;

3.4 Fornecer atualizações de software recomendadas para manter o bom funcionamento da solução, sem ônus adicionais;

3.5 O serviço de suporte técnico poderá ser atendido através de contato telefônico, por e-mail ou nas dependências da CONTRATANTE, sendo este critério decidido pela equipe técnica da CONTRATANTE;

3.6 A CONTRATADA deverá possuir sistema de abertura de chamados para que a CONTRATENTE possa receber um identificador único para cada solicitação de atendimento e que tenha recursos (e-mail, página web, central telefônica ou etc.) que possa manter a equipe técnica da CONTRATANTE informada sobre o andamento de cada chamado, esteja ele aberto, em andamento ou fechado.