Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;

Capacidade de detecção keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;

Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;

Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Proativa com a base de reputação do fabricante;

Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

Possibilidade de agendar o escaneamento da detecção Proativa com periodicidade mínima por minuto e em todos os novos processos;

Possibilidade de agendar o escaneamento da detecção Proativa com periodicidade mínima por minuto e em todos os novos processos.

1.1.20. A Funcionalidade de Controle de Dispositivos e Aplicações deve possuir as seguintes carcterísticas:

Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

Controlar o uso de dispositivos com comunicação infra-vermelho, firewire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;

Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;

Gerenciamento integrado à console de gerência da solução;

Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;

Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

1.1.21. Os Relatórios e Monitoramentos possuir minimamente as seguintes funcionalidades:

Possuir, pelo menos, 25 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;

Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status (com vírus, desatualizada etc.);

Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

- As 10 máquinas com maior ocorrência de códigos maliciosos;
- Os 10 usuários com maior ocorrência de códigos maliciosos;
- Localização dos códigos maliciosos;
- Sumários das ações realizadas;
- Número de infecções detectadas diário, semanal e mensal;
- Códigos maliciosos detectados.

1.1.22. O Console Avançado de Distribuição e Relatórios deve possuir as seguintes características:

Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;

Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;

Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:

- CA;
- ESET;
- F-Secure;
- Kaspersky;
- McAfee;
- Sophos;
- Symantec;
- Trend Micro.

Permitir a remoção de outros softwares não desejados;

Criar tarefas de migração baseadas no resultado do inventário de antivírus;

Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;

Possibilidade de recuperar instalação em clientes em caso de falha;

Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;

Os seguintes cubos devem ser disponibilizados para criação de relatórios como:

- Alertas;
- Clientes;
- Políticas;
- Rastreamento.

Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança;

Exportar os relatórios criados nos formados xls, pdf e html.

1.1.23. As Funcionalidades de Controle de Acesso à Rede devem:

Possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

- Computador deve possuir antivírus, atualizados e ativo;
- Computador deve possuir firewall ativo;
- Computador deve possuir antispyware, atualizado e ativo;
- Computador deve possuir patches instalados, ativos e atualizados.

Deve ter a capacidade de iniciar à auto remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso a rede;

A auto remediação deve suportar download de programas e arquivos por links de HTTP, FTP e UNC;

Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação.

1.1.24. O Ponto de Reforço no Próprio Agente deve:

Ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não utilizam o agente (Máquinas não gerenciadas);

Ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não estiverem em conformidade com as políticas do controle de acesso a rede;

1.1.25. A Segurança de Mensageria deve:

Integrar a captura eficiente de spams com baixa taxa de categorização das mensagens como falsos positivos. Implementado como gateway de e-mails, deve proteger e-mails e mensagens instantâneas contra vírus, spams, phishing, botnets e outros e-mails indesejados. Deve incorporar recursos flexíveis para o gerenciamento de spams e atualizações automatizadas de filtros.

Deve possuir possibilidade de ser fornecido em modelo appliance;

Deve possuir possibilidade de ser fornecido em modelo virtual-appliance, compatível com VMWARE ESX e ESXi;

Sistema operacional da solução “pre-hardened”, com limitação dos serviços em uso;

Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do Órgão;

Deve ter capacidade de integração com servidor de criptografia, para criptografar mensagens e anexos;

Deve ter a capacidade de permitir ou não endereços de e-mail com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8-bit;

Deve ter a capacidade de rejeitar conexões que tentem serem abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS;

Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;

Deve ter a capacidade de implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual.

1.1.26. O Console de Gerência da Solução de Mensageria deve:

Permitir gerenciar mais de um servidor de gateway a partir da mesma console;

Permitir definir políticas individuais por servidor de gateway ou globais, a partir da mesma console;

Deve possuir capacidade de administrar de forma unificada, via interface Web (com criptografia), com diversos níveis de acesso (administração, relatórios, quarentena, apenas leitura);

Deve possuir possibilidade de acesso individual ao appliance via SSH, para execução de comandos via CLI (linha de comando);

Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS);

Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para especifica mensagem, sem necessidade de integração com produtos de terceiros ou “open source”;

Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior (item 0), em todos os appliances /equipamentos da solução ofertada;

Deve permitir realizar o rastreamento da mensagem, citada no item 0), utilizando caracteres double-byte para línguas estrangeiras;

Deve possuir funcionalidade de criação de Alias e Mascaramento de endereço;

Deve ser possível realizar notificação do administrador por email caso os filtros antispam não recebam atualizações por um determinado período de tempo;

Deve ser capaz de integração com LDAP Microsoft Active Directory 2003, Microsoft Active Directory 2008 ou superior para sincronização e autenticação;

Deve permitir a criação de políticas diferenciadas para tratamento de SPAM, Virus, Filtragem de Conteúdo e Controle de reputação (traffic shaping), de acordo com o destinatário da mensagem e reputação de origem;

Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento do usuários válidos e ações de Virus, Spam e Filtragem de Conteúdo diferenciadas por grupo do LDAP;

Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico, sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;

Deve possuir mecanismos de backup/restore da configuração existente na solução.

1.1.27. As Funcionalidades do AntiSpam devem:

Ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;

Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:

a. Apagar mensagem;

b. Enviar para Quarentena;

c. Encaminhar mensagem;

d. Encaminhar em BCC;

e. Gravar mensagem em disco;

f. Gravar em pasta de conformidade;

g. Modificar o assunto;

h. Adicionar informações ao cabeçalho;

i. Deferir a mensagem;

j. Rejecter a mensagem.

Deve ser capaz de quando a mensagem for gravada em pasta de conformidade, permitir definir ações distintas para as mensagens aprovadas e reprovadas;

Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;

Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);

Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);

Deve possuir centro especializado, 24x7, com monitoramento de mais de 2 milhões de mailboxes, para processamento de SPAMs recebidos e criação automática de novos filtros/assinaturas;

Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;

Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;

Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);

Deve ter a capacidade de reconhecimento de ameaças Dia-Zero, com assinatura de suspeitos de vírus;

Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:

- Assinaturas para corpo da mensagem e anexos;
- Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;
- Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramente do fornecedor da solução);
- Identificação de idiomas;
- Filtros de URLs;
- Filtros anti-phishing.

Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;

Deve permitir a criação de "compliance folders", para armazenagem de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo Administrador;

Deve possuir tecnologia para detecção de ataques de Spam, Vírus e Diretório (Usuários Inválidos);

Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;

Deve possuir a cada nível da detecção dos ataques, citados no item anterior (item 0), o controle do percentual de mensagens que serão recusadas;

Deve possuir a cada nível da detecção dos ataques, citados no item 0, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;

Deve possuir tecnologia para prevenção de ataques de “Bounce Messages”;

Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;

Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;

Deve possuir a capacidade para criação de regras baseada na detecção por “Wildcard”;

Deve possuir a capacidade para criação de regras baseada na detecção por expressões regulares;

Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);

Deve possuir capacidade de configurar criptografia TLS por domínio e por política;

Deve ter capacidade de detecção a pelo menos 10 idiomas (incluindo Português), permitindo o bloqueio de mensagens escritas nos idiomas não desejados;

Deve possuir capacidade de criar uma lista de IP´s confiáveis baseada no comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;

Deve possuir a capacidade de atualização automática periódica da lista de IP's confiáveis, citada no item anterior (item 0).

1.1.28. A Funcionalidades de Anti-malware deve minimamente:

Ter a capacidade de deleção total de mensagens enviadas por "Mass-Mailing Worms", com opção de ações diferenciadas por tráfego de entrada e saída;

Deve ter a capacidade de reconhecimento de Spywares e Adwares;

Deve possuir recurso para detecção dos ataques de duas escalas para Vírus e Diretório (LDAP), capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;

Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;

Deve possuir engine do antivírus comprovada por pelo menos 6 anos consecutivos de êxito nos testes realizados pelo instituto "Virus Bulletin" (www.virusbtn.com) - VB100 Award;

Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo.

1.1.29. A Quarentena da Solução de Mensageria deve minimamente:

Possuir uma Quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;

O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena (digest);

Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

Deve permitir que o usuário cadastre endereços de email em listas negras/listas brancas pessoais.

1.1.30. O Módulo de Simulação e Conscientização de Ataque Phishing deve minimamente:

A solução deve implementar módulo educacional de uso ilimitado durante o período de garantia para reconhecimento de ataques de Phishing, contemplando todos os usuários do Órgão, caso não exista este tipo de licenciamento deverão ser entregues no mínimo 250 possibilidades de utilização do módulo educacional para cada usuário do Órgão a serem utilizados a cada 12 meses de garantia contratada, não cumulativos entre um ano e outro de garantia;

A solução deve implementar módulo educacional contra ataques de Phishing desenhado especificamente para este fim, onde não serão aceitas simulações executadas a partir dos softwares que compõem a proteção do tráfego de e-mail do Órgão;

A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerado os recursos do Órgão para o envio dos e-mails de simulação;

A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos;

A solução deve implementar módulo educacional contra ataques de Phishing, todos no mesmo software, composto de no mínimo:

- Módulo de construção de e-mail para simulação do ataque de Phishing;
- Módulo de conscientização educacional de reconhecimento do ataque de Phishing;
- Módulo gráfico e de relatórios que permita avaliar se o usuário reportou à área de segurança o possível ataque de Phishing sofrido.

A solução educacional contra ataques de Phishing deve ser capaz de criar templates educacionais exclusivos para o Órgão, em português com a logo marca do Órgão;

A solução educacional contra ataques de Phishing deve ser capaz de criar templates educacionais exclusivos para o Órgão, de forma departamentalisada direcionada por setor do Órgão como por exemplo, área administrativa, área jurídica, área técnica de TI, área técnica administrativa, não se limitando somente à estas áreas, em português e com a logo marca do Órgão;

A solução educacional contra ataques de Phishing deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas ou externas;

A solução educacional contra ataques de Phishing deve ser capaz de durante a criação do e-mail template customizado para o Órgão, conter no mínimo as parametrizações abaixo:

a. Escolha de um anexo customizado pelo Órgão a ser anexado ao e-mail de simulação de ataque Phishing;

b. Seleção de usuário e de grupo de usuários que farão parte da simulação;

c. Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, específica por grupo a ser atingido;

d. Definição de assunto do e-mail de simulação do ataque Phishing;

e. Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing;

f. Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing;

g. A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:

- Nome do usuário;
- Sobrenome;
- Endereço de e-mail;
- Nome da empresa;
- Dia / Data / Hora / Ano;

A solução educacional contra ataques de Phishing deve ser capaz de criar relatórios executivos e mostrar de forma gráfica na console do produto no mínimo:

a. Verificação de quantas simulações foram enviadas para o Órgão;

b. Verificação de quantos usuários acessaram o e-mail de simulação de ataque Phishing;

c. Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque Phishing;

d. Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing;

e. Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;

f. Verificação de quantos usuários executaram o módulo de conscientização educacional Anti-Phishing;

g. Verificação da geo-localização dos usuários que sofreram a simulação do ataque de Phishing e foram capturados na simulação.

A solução educacional contra ataques de Phishing deve ser capaz de construir uma mensagem de conscientização direcionada para cada departamento informando que usuário foi pego em uma simulação de ataque Phishing, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque;

A solução educacional contra ataques de Phishing deve ser capaz de indicar a necessidade do usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização (item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários;

A solução educacional contra ataques de Phishing deve apresentar de forma gráfica o resultado geográfico de qual localidade o e-mail de simulação do ataque Phishing foi efetivo com usuários sendo atacados pela simulação;

A solução educacional contra ataques de Phishing deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização do Órgão.

1.1.31. A Segurança de Correio Eletrônico deve:

Fornecer proteção em tempo real para e-mails contra vírus, spams, spywares, phishing e outros ataques, enquanto aplica as políticas de conteúdo para o serviço de correio eletrônico.

Deve suportar ambientes de servidores Windows de 64 bits e Exchange virtualizados, com instalação fácil e administração simples.

1.1.32. A Arquitetura da Solução de Proteção a Correio Eletrônico deve minimamente:

Ser compatível com os sistemas operacionais Windows Server 2003 e Windows Server 2008, ambos em 32bits e 64bits;

Deve suportar Cluster Ativo/passivo da solução Exchange;

Deve ser compatível com Exchange Server 2003, 2007 e 2010;

Deve ser compatível com VSAPI versões 2.0, 2.5 e 2.6;

Deve ser compatível com ambientes virtuais Vmware e Hyper-V;

Deve permitir instalação remota.

1.1.33. O Console de Gerência da Solução de Proteção a Correio Eletrônico deve minimamente:

Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS) com as seguintes características:

- A console “Web-base” deve contemplar além do gerenciamento do próprio produto, no mínimo, o gerenciamento dos aplicativos de segurança a seguir:
- Software para segurança de estação de trabalho e servidores (“endpoint”);
- Software para filtro de antivírus e anti-span de E-Mail;
- Software para proteção de antivírus e anti-span das caixas postais;
- Software para proteção proativa;
- Software para filtro de fluxo WEB;
- Software de relatórios para segurança de estação de trabalho e servidores;
- Software para monitoração e proteção de dados confidenciais.

Deve possibilitar permissionamento de acesso a console, integrando-se com o Active Directory;

Deve ter a capacidade de gerência centralizada de vários servidores;

Deve ter possibilidade de agrupamento dos servidores de correio eletrônico para configuração de políticas semelhantes;

Deve ter capacidade de executar mudanças de configuração em tempo-real, sem necessidade de reiniciar a aplicação;

Deve permitir a instalação da console fora do servidor Exchange.

1.1.34. As Funcionalidades do Anti-Malware devem:

Ter a capacidade de verificação em tempo real de SMTP;

Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;

Deve ter a capacidade de verificação manual dos message stores;

Deve ter a capacidade de verificação agendada dos message stores;

Deve permitir verificar mailbox stores e public foldes;

Deve permitir definir a “idade mínima” das mensagens a serem verificadas;

Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:

- Tempo máximo de verificação;
- Número máximo de decomposição de arquivos compactados recursivamente;
- Tamanho máximo do arquivo descompactado;
- Número máximo de arquivos descompactados.

Deve ter mecanismo de detecção de mass-mailer worms;

Deve permitir, no mínimo, as seguintes ações para a detecção de malware:

- Reparar o anexo / corpo da mensagem;
- Quarentenar o anexo / corpo da mensage;
- Substituir a mensagem por um alerta;
- Apagar o anexo / corpo da mensagem;
- Apagar a mensagem inteira;
- Apenas alertar.

Deve ter capacidade de executar atualização de vacinas sem necessidade de reinício do serviço;

Deve ter mecanismos de detecção de epidemia baseados, no mínimo, em:

- Ocorrência do mesmo malware;
- Número total de malware;
- Ocorrência do mesmo assunto;
- Ocorrência de mesmo arquivo anexado.

Emissão de alertas de epidemia.

1.1.35. As Funcionalidades do Filtro de Conteúdo devem:

Permitir a criação de filtros distintos para entrada, saída e mensagens no message store;

Deve ter políticas baseadas em usuários e grupos de usuários;

Deve permitir, no mínimo, verificação de conteúdo em:

- Corpo da mensagem;
- Assunto;

- Remetente;
- Domínio;
- Nome de anexos;
- Extensão de anexos.

Deve permitir a utilização de valores expressos literalmente, através de expressões regulares e utilização de wildcards;

Deve permitir, no mínimo, as seguintes ações para o filtro de conteúdo:

- Quarentenar o anexo, indicando ação no corpo da mensagem;
- Substituir a mensagem por um alerta;
- Apagar o anexo, indicando ação no corpo da mensagem;
- Apagar a mensagem inteira;
- Apenas alertar;
- Adicionar texto ao assunto da mensagem.

Deve permitir a detecção pelo tipo real do arquivo e não apenas pela extensão do mesmo.

1.1.36. As Funcionalidades do AntiSpam devem minimamente:

Ter capacidade de detecção de Spam através de mecanismos de heurística;

Deve ter capacidade de detecção de spam através de assinaturas;

Deve ter capacidade de implementar filtros de URL;

Deve permitir utilizar RBLs (Real-time Black lists) de terceiros;

Deve ter capacidade de bloquear mensagens através de serviço de reputação identificando, no mínimo:

- Origens seguras;
- Origens com alto tráfego de spam;
- Origens de malware.

Deve ter capacidade de permitir configuração de uma “lista negra” centralizada;

Deve ter capacidade de permitir criar uma “lista branca” de remetentes e destinatários;

Deve ter capacidade de permitir configurar o nível de sensibilidade do mecanismo anti-spam;

Deve ter capacidade de permitir, no mínimo, as seguintes ações para o anti-spam:

- Rejeitar / Deletar a mensagem;
- Entregar a mensagem para determinado e-mail;
- Adicionar texto ao assunto da mensagem (TAG);
- Adicionar informações ao header da mensagem (x-header);

- Enviar a mensagem à pasta de Spam do usuário;
- Apenas alertar.

Deve ter capacidade de implementar reputação local de acordo com ambiente analisado;

Deve possuir uma fila rápida de entrega caso o remetente seja considerado confiável. Essa fila rápida terá menos verificações de SPAM para melhorar a performance no processamento das mensagens.

1.1.37. Os Relatórios devem minimamente:

Deve ter capacidade de permitir gerar relatórios e enviar automaticamente por e-mail;

Deve possuir, no mínimo, os seguintes relatórios:

- Resumo por Servidor;
- Resumo Consolidado;
- Detalhado de Malware;
- Detalhado do filtro de conteúdo;
- Detalhado ao anti-spam;
- Detalhado de informações do sistema.

1.2. **Gateway de Segurança para WEB** – A solução de "Gateway de Segurança da Web", deve proteger contra as ameaças da Web 2.0, incluindo URLs maliciosos, spywares, botnets, vírus e outros tipos de malware, além de fornecer controles para uso da Internet e de aplicativos. Sua plataforma deve ser escalonável, permitindo uma verificação rápida e simultânea quanto a presença de malware e conteúdos inapropriados da Web.

1.2.1. A solução deverá ser “Bundle” (Hardware/Software) ou software appliance obrigatoriamente do mesmo fabricante ou em regime OEM, ou homologado pelo fabricante da solução de Filtro WEB;

1.2.2. A solução deve garantir redundância e alta disponibilidade, provendo toda a infraestrutura de hardware e/ou software suficientes e necessários ao seu completo funcionamento;

1.2.3. Deverá suportar carga total de transações mesmo em momento de falha de um dos componentes da solução, ou seja, com 50% do hardware disponível;

1.2.4. A solução deve ser escalar e suportar pelo menos 30.000 requisições HTTP por segundo;

1.2.5. A solução deve ser escalar e suportar pelo menos 15.000 requisições HTTPS por segundo;

1.2.6. A solução deve ser escalável e suportar pelo menos 75.000 novas conexões TCP por segundo até o limite da capacidade de conexões simultâneas da solução;

1.2.7. A solução deve ser capaz de descriptografar tráfego SSL sem perda de performance, para um volume de no mínimo 50% do tráfego de internet passante e contratado;

1.2.8. A solução deve suportar no mínimo 20 algorítimo de criptografia;

1.2.9. Deve ter a capacidade de reconhecer, filtrar, executar controle e bloqueios para WEB 2.0, conforme abaixo:

Liberar apenas canais específicos do YouTube, segmentando por usuário ou grupos de usuários;

Bloquear canais específicos do YouTube, segmentando por usuário ou grupos de usuários;

Bloquear vídeos do YouTube por palavras chaves, segmentando por usuário ou grupos de usuários;

Bloquear Chat do Facebook;

Bloquear criação de Eventos do Facebook;

Reconhecer e filtrar tráfego IM (MSN Messenger, Yahoo Messenger);

Reconhecer e filtrar tráfego SMTP, POP3 e IMAP;

Reconhecer e filtrar tráfego P2P (BitTorrent, Gnutella, eDonkey, Kazaa);

Reconhecer e filtrar tráfego controle remote (LogMeIn, Windows Terminal Services, WebEX);

Reconhecer e filtrar tráfego de vídeo (Windows Media, Quick Time).

1.2.10. Fornecimento de Solução de Proxy e Filtro de Conteúdo, com as seguintes funcionalidades:

Proxy;

Proxy Reverso;

Proxy Cliente;

Cache;

Filtro de Conteúdo Web (URL Filtering).

1.2.11. Fornecimento da Solução para Confecção de Relatórios Técnicos e Gerenciais para a Solução de Proxy e Filtro de Conteúdo, deverá ser totalmente compatível e integrada com os appliances de Proxy e Filtro de conteúdo;

1.2.12. Fornecimento de Solução para Gerenciamento Centralizado com as seguintes funcionalidades:

Soluções de Proxy e Filtro de conteúdo;

Soluções de Antivírus para Proxy e Filtro de conteúdo;

Deverá ser composta de elementos de hardware e software, que integrados formam as seguintes funcionalidades:

Unificação e deployment de políticas;

Unificação de Backup e Restore;

Gerenciamento centralizado de no mínimo 5 Appliances.

1.2.13. A Solução de Proxy e Filtro de conteúdo – Hardware (Appliances) deverá conter:

A solução deverá ser capaz de em um único dispositivo de Hardware do tipo Appliance ou software appliance para atendimento simultâneo das funcionalidades de Proxy, Proxy Reverso, Proxy Cliente, Cache, Filtro de Conteúdo Web (URL Filtering);

Seguindo com as melhores práticas de segurança, não serão aceitos como solução de Hardware, equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;

Descrição das capacidades dos Appliances para Solução de Proxy e Filtro de conteúdo:

- Equipamento licenciado com capacidade de suportar até 500 usuários simultâneos e 12 Mbps de link;
- Descrição das capacidades dos appliances:
  - Capacidade para processar, no mínimo, 12 Mbps de tráfego;
  - Capacidade mínima de 500 usuários simultâneos no modo de implementação inline;
  - Capacidade para processar, no mínimo, 2000 conexões HTTP/TCP por segundo;
  - Possuir, pelo menos, 3 interfaces ethernet 10/100/1000BT, sendo duas delas com capacidade de bypass, em caso de falha do equipamento e a terceira destinada a gerenciamento.
  - Possuir suporte a VLAN Tag no padrão IEEE 802.1q;
  - Possuir no mínimo 4GB de memória RAM;
  - Possuir capacidade de, pelo menos 250GB de espaço útil para armazenamento em disco;
  - Possuir, no mínimo, uma interface serial RS-232;
  - Placa para aceleração SSL incluída;
  - Deve possuir fonte com tensão de entrada 110/220VAC, 50-60 Hz, com cabo de alimentação.
  - Deve ser montável em rack padrão de 19 polegadas, caso seja necessário kit para montagem, este deve acompanhar o equipamento, sem custo adicional.

Funcionalidades da Solução de Proxy e Filtro de conteúdo – Características do cache de dados e aceleração:

a. A solução de cache deve suportar os protocolos HTTPS e HTTP realizando a função Proxy reverso e transparente ao mesmo tempo, no mesmo hardware;

b. Realizar cache de HTTP, HTTPS, MMS, RTSP e FTP;

c. Realizar Socks Proxy com suporte a encapsulamento socks;

d. Possui suporte ao protocolo WCCP, realizando cache transparente;

e. Possuir suporte ao protocolo WCCP versão 2 para integração com ambiente Cisco;

f. Possuir suporte para que qualquer tipo de tráfego seja redirecionado para o cache, como HTTP, HTTPS, DNS, FTP, MMS, RTSP;

g. Possuir suporte a supressão de headers HTTP que denunciem a existência do cache na rede;

h. A funcionalidade mencionada neste item deve existir em ambas as direções de comunicação, tanto cache-cliente como cache-servidor;

i. A funcionalidade mencionada neste item deverá permitir a substituição da informação do cabeçalho HTTP por uma string fixa, protegendo, assim, informações confidenciais;

j. Deverá permitir o bloqueio de clientes por versão de software ou tipo de Browser, permitindo que o cliente utilizando internet explorer opere normalmente enquanto bloqueie toda requisição feita pelo Netscape, por exemplo

k. Possuir suporte para cache transparente para os protocolos HTTP, HTTPS, RTSP (Real), Windows Media, DNS, FTP;

l. Todos esses protocolos devem ser suportados de forma integrada ao hardware e em implementações e de forma transparente, isto é, através do redirecionamento das requisições do usuário por um switch camada 4 ou 7, ou pelo protocolo WCCP;

m. Possuir suporte a “split” de streaming áudio/vídeo ao vivo e o cache de conteúdo sob demanda;

n. Possuir suporte a entrega de conteúdo em multicast para os usuários a partir de um stream em unicast, ou seja, “converte” unicast em multicast;

o. A função CDN (Content Delivery Networks) deve ser suportada pela solução para distribuição de conteúdos sob demanda e ao vivo utilizando os protocolos de RealVideo e Windows Media.

p. Implementar, de forma transparente, “tunneling” de tráfego desconhecido, de modo que um tráfego diferente de HTTP, por exemplo, que utilize a mesma porta TCP/80 do HTTP não sofra interferência em função da presença do cache na rede.

q. Implementar “IP Spoofing” do IP do cliente quando estiver comunicando com o servidor web original, e não utilizar o seu próprio endereço IP;

r. Permitir a integração nativa com sistemas de varredura de códigos maliciosos para os protocolos HTTP, HTTPS e FTP, utilizando o protocolo ICAP ou ICAP(S) para se comunicar com os sistemas antivírus externos;

s. A integração entre o Cache e o antivírus deve permitir que após receber a atualização das assinaturas de vírus pelo antivírus, o Cache efetue a checagem das páginas cacheadas contra a nova versão do arquivo de assinaturas;

t. O sistema antivírus não precisa ser fornecido como parte da solução;

u. Possuir suporte a autenticação LDAP, Domínio do Windows NT (NTLM), Active Directory, Microsoft Kerberos, RADIUS e certificados digitais;

v. Os mecanismos de autenticação podem ser configurados por protocolo, ou seja, pode-se configurar para autenticar o tráfego HTTP e não autenticar o tráfego RTSP;

w. Para os protocolos NTLM e LDAP, o cache deve ser capaz de realizar a autenticação e verificação de grupos de usuários no PDC/AD de um domínio, não dependendo de replicação de base de dados;

x. Deve suportar a autenticação de forma transparente (sem prompt de senha para o usuário, utilizando a autenticação do S.O. de rede). Essa funcionalidade deve existir tanto com o cache configurado como Proxy da rede, quanto como de forma transparente (o tráfego deverá ser redirecionado por um Switch camada 4/7 e o browser dos clientes não poderá conter nenhuma configuração de Proxy).

y. Deve implementar autenticação transparente através de cookie ou endereço IP;

z. Deve suportar aceleração de aplicações usando metodologias de gerenciamento de banda, otimização de protocolos, cache de objetos, cache de byte e compressão para as aplicações: E-mail (MAPI), compartilhamento de arquivos (CIFS, NFS), banco de dados (MS-SQL, SQLNet), transferência de arquivos (FTP), Web (HTTP), Web segura (HTTPS), Streaming Vídeo/Áudio (MMS, RTSP, QuickTime, Flash);

aa. Ter a capacidade de servir arquivos tipo "PAC" (Proxy automatic configuration) a partir do próprio appliance;

bb. Deve permitir o controle granular de aplicações, como redes sociais, webmail, etc. oferecendo o bloqueio de, pelo menos, as operações de upload de arquivos, download de arquivos e post de mensagens.

Características de segurança e gerenciamento:

a. Possuir suporte a configuração de regras de controle de acesso (filtros) que permitam:

- Controlar o acesso a determinadas URLs ou domínios Web, permitindo o uso de “wildcards”, máscaras ou expressões regulares;

- Restringir os endereços IP dos quais podem ser feitas requisições ao cache;
- Restringir os endereços IP pelos quais o cache pode ser gerenciado;
- Redirecionar requisições feitas a determinados objetos para outras URLs;
- Realizar o mapeamento de URLs, interceptando a URL requisitada e alterando para a URL mapeada.

b. A solução deverá dispor de inteligência que monitore as redes de distribuição de malware (MalNets) e seja capaz de identificar um ataque, mesmo antes deste ser iniciado;

c. Deve possibilitar a identificação de estações possivelmente infectadas por malware através de ferramenta de relatório;

d. Bloquear extensões definidas pelo tipo de MIME ou pela própria extensão (Ex: Application/Executable ou ".exe");

e. Bloquear "scripts" ativos como Active X, Java, Javascript, VBScript;

f. Os filtros devem ser separados para cada tipo de protocolo suportado;

g. Os filtros podem ser aplicados tanto às requisições dos usuários como às respostas dos servidores;

h. Bloquear arquivos pela leitura dos bytes iniciais do arquivo;

i. Possuir suporte a filtros de URL:

- Internos ao cache;
- Externos ao cache. Neste caso, o equipamento deve suportar a integração utilizando o protocolo ICAP versão 1.0.

j. A solução de geração de relatórios deve possuir integração com o AD para autenticar usuários com diferentes níveis de acesso aos relatórios:

- Possuir repositório local para criação de contas e senhas de usuário, incluindo o nível de acesso que esse usuário terá para funções de configuração e monitoração do equipamento.

k. Permitir a configuração de endereços IP para onde devem ser encaminhados alarmes e traps SNMP;

l. Possuir suporte ao ajuste de hora através do protocolo NTP;

m. Permitir atualização de imagens, upload e download dos arquivos de configuração usando algum dos protocolos a seguir: TFTP, HTTP ou FTP;

n. Possuir suporte ao backup/restore de configurações em servidores externos;

o. Suportar o gerenciamento via HTTP, HTTPS, telnet, SSH e porta serial;

p. Possuir suporte a configuração através do padrão Command Line Interface (CLI);

q. Possuir mecanismos para limitar o acesso às funções de gerenciamento dos equipamentos seja via Telnet, SSH, SNMP, Web browser ou console serial;

r. Possuir suporte ao protocolo SNMP v2c;

s. Suportar a utilização da MIB RFC1213, RFC2594 e Proxy MIB.

Características do software de Gerência:

a. Possuir Interface Gráfica de Usuário (GUI): deverão estar inclusos todos os softwares necessários para administração, configuração e gerenciamento através de Interface Gráfica de Usuários (GUI);

b. Permitir a configuração e monitoração através de um web browser;

c. Permitir a visualização dos seguintes itens:

- Tráfego nas portas ethernet;
- Status do cache, assim como de seus contadores (Exemplos: Cache-hits, e misses);
- Estado da memória, da CPU, dos discos e demais sistemas do equipamento;
- Volume de tráfego e quantidade de conexões.

d. Permitir a geração de relatório com a utilização histórica de CPU, memória e tráfego;

e. Geração de Relatórios do filtro de acesso a conteúdos na Internet:

- Acessos autorizados – relatório que demonstre a quantidade de acessos autorizados, bem como a quantidade de bytes trafegados, sendo possível a visualização por: usuário (cadastrado no MS Active Directory), grupo de usuários (cadastrado no MS Active Directory), IP de origem, aplicação, URL acessada;
- Utilização da internet por horário – relatório que demonstre a utilização da internet por períodos do dia;
- Downloads por extensão – relatório que demonstre as atividades de downloads da internet por extensão de arquivos baixados sendo possível a visualização por: extensão de arquivo, usuário (cadastrado no MS Active

Directory), grupo de usuários (cadastrado no MS Active Directory), IP de origem e tamanho dos arquivos;

- Top 10 sítios web mais acessados – relatório que demonstre, em ordem decrescente, os cem sítios web mais acessados;
- Top 10 categorias mais acessadas – relatório que demonstre, em ordem decrescente, as vinte categorias de sítios web mais acessadas;
- Top 10 usuários mais ativos – relatório que demonstre, em ordem decrescente, os cem usuários com a maior utilização dos serviços internet;
- Top 10 grupos de usuários mais ativos – relatório que demonstre, em ordem decrescente, os vinte grupos de usuários (cadastrado no MS Active Directory) com a maior utilização dos serviços internet;
- Devem ser oferecidos templates pré-formatados de relatórios com, no mínimo, 30 opções diferentes de consultas;
- Deve ser oferecida a opção de criação de relatórios tipo ad-hoc, com formato e campos customizáveis;
- Deve ser garantida a opção de alterar o período de consulta para a emissão de qualquer relatório fornecido pela solução;
- Os relatórios devem ser exportáveis nos formatos HTML, PDF e CSV;
- A solução deve possibilitar o envio automático por e-mail a usuários pré-definidos de qualquer um dos relatórios previstos.

f. Vir acompanhado de todos os manuais de instalação, configuração e utilização do produto.

Características do filtro de acesso a conteúdo na Internet:

a. Deverá estar licenciado para suportar até 500 usuários de filtro de conteúdo;

b. Garantir a monitoração do tráfego internet independente de plataforma, sistema operacional predominante na rede interna ou aplicação utilizada pelos usuários;

c. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

d. Bloquear as tentativas de acesso proibidas pela política antes que ocorra o download da página solicitada;

e. Permitir o cadastramento de diferentes perfis de acesso para administração da solução;

f. Prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso à determinada categoria de sites;

g. Integrar ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory e Radius reconhecendo contas e grupos de usuários cadastrados;

h. Suportar as metodologias pass-by ou pass-through de filtragem;

i. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços;

j. Fornecer documentação técnica, bem como manual de uso, em inglês ou português do Brasil;

k. Serviços/recursos de controles de acesso à internet:

- Controle de acesso à internet por endereço IP de origem e destino;
- Controle de acesso à internet por sub-rede;
- Controle de acesso à internet por usuário;
- Controle de acesso à internet por grupo de usuários;
- Controle de acesso à internet por protocolo;
- Controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Controle de acesso à internet por categorias de sítios web;
- Controle de acesso à internet por lista de sítios web proibidos customizável;
- Controle de acesso à internet por lista de sítios web permitidos customizável;
- Controle de downloads por nome, tipo ou extensão de arquivo;
- Controle pela leitura dos bytes iniciais do arquivo;
- Controle de tráfego internet de áudio e vídeo tipo streaming media.

l. Painel de visualização das atividades web demonstrando em tempo real a utilização dos serviços internet e o consumo da banda de acesso;

m. Mensagem de bloqueio customizável para resposta aos usuários na tentativa de acesso a recursos proibidos pela política;

n. Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sítios web de busca;

o. Definição e aplicação de políticas por meio de expressões regulares;

p. Permitir a criação de regras para bloqueio de categorias de sites e a criação de exceção a essa regra para uma ou mais URL desta categoria;

q. Classificação/categorização de sítios na Internet de acordo com o assunto;

r. Base de dados contendo, no mínimo, 15 milhões de sítios web já registrados;

s. Base com, no mínimo, 80 categorias diferentes;

t. Base com, no mínimo, 50 idiomas diferentes;

u. Categoria exclusiva para sítios web caracterizados como Proxy Anônimo:

- Categoria exclusiva para sítios web tipo Instituições Financeiras;
- Categoria exclusiva para sítios web tipo Webmail;
- Categoria exclusiva para sítios web tipo Blog/Fotolog;
- Categoria exclusiva para sítios web tipo Instituições de Saúde;
- Categoria exclusiva para sítios web tipo Notícias;
- Categoria exclusiva para sítios web tipo Phishing;
- Categoria exclusiva para sítios web tipo Hackers;
- Categoria exclusiva para sítios web tipo Pornografia;
- Categoria exclusiva para sítios web tipo Jogos;
- Categoria para sítios web tipo Racismo;
- Categoria exclusiva para sítios web tipo Comunidades Virtuais;
- Categoria exclusiva para sítios web tipo Compras;
- Categoria exclusiva para sítios web tipo Chat/Instant Messaging;
- Categoria exclusiva para sítios web tipo Instituições Educacionais;
- Categoria exclusiva para sítios web tipo P2P;

- Categoria exclusiva para sítios web tipo Audio Streaming;
- Categoria exclusiva para sítios web tipo Vídeo Streaming.

v. Permitir a criação de categorias personalizadas alimentadas conforme a necessidade do licitante;

w. Permitir ao licitante reclassificar, ao seu critério, os registros de sítios web que julgar necessário;

x. Possuir, integrado ao appliance, recurso de categorização de URLs dinâmico e em tempo real:

- Este recurso deve operar de forma totalmente automática, independe do administrador ou do usuário;
- Classificação/categorização de sítios web de acordo com o assunto – especificações adicionais;
- Para sites não categorizados na base local, o sistema deverá dispor de mecanismos para fazer a categorização do site em tempo real, de forma transparente ao usuário.

y. A base de sítios web deve ser atualizada, com periodicidade mínima diária;

z. A atualização da base de sítios web deve transcorrer de forma transparente sem comprometer a execução dos serviços;

aa. A ausência de atualização da base de sítios web, por qualquer motivo inclusive término do contrato, não deve interromper nem comprometer funcionalidades da solução;

bb. Os sítios web devem ser atualizados, sempre na categoria que reflita o seu conteúdo mais recente, ou seja, em caso de modificação, deve ser reclassificado para a categoria pertinente

cc. Sítios web de phishing, spyware ou que tenham sido usados para hospedar códigos maliciosos, depois de “descontaminados” devem retornar à categoria original.

1.2.14. A Solução para Confecção de Relatórios Técnicos e Gerenciais para a Solução de Proxy e Filtro de Conteúdo deve minimamente possuir:

Capacidade gerar relatórios baseado nos logs dos appliances do Objeto;

Licenciamento com capacidade para armazenar até, pelo menos, 2.5 bilhões de linhas de log;

Suportar instalação nos seguintes sistemas operacionais:

a. Windows Server 2003 e 2008, nas versões 32 e 64 bit;

b. Linux RedHat 4 e 5, nas versões 32 e 64 bit;

c. Ambiente VMware.

A solução de banco de dados deve ser proprietária. Caso não seja, deverá ser fornecida juntamente com a solução, sem custo adicional (Hardware dedicado e softwares licenciados – Sistema Operacional e Banco de Dados);

O módulo de relatórios deve fornecer informações em exibição gerencial e operacional;

Deve permitir extrair, necessariamente, os relatórios abaixo:

a. Relatório dos maiores usuários (nome de usuário) de internet e sites com maior volume de dados acessados por esses usuários;

b. Relatório de sites acessados por determinados usuários, baseado em nome de usuário;

c. Relatório de usuários que acessaram determinado site por determinado período;

d. Relatório dos usuários que tiveram mais requisições bloqueadas;

e. Relatório dos sites mais acessados por volume de dados (em MB);

f. Relatório dos computadores e usuários que mais acessaram páginas HTTP (em MB);

g. Relatório das estatísticas de acesso HTTP por regional do licitante em volume de dados (em MB);

h. Relatório das estatísticas de acesso HTTP por sub-rede IP do licitante em volume de dados (em MB);

i. Relatório das estatísticas de acesso HTTP por tipo de arquivo acessado em volume de dados (em MB).

Deve gerar registros de acesso (logs), em pelo menos, nos formatos: Squid, World Wide Web Consortium Extended Log File Format (W3C ELFF) e customizável;

Geração automatizada de relatórios conforme agendamentos feitos pelo administrador, possibilitando a entrega destes relatórios de maneira automatizada por e-mail;

Todos os relatórios mencionados devem possuir os dados detalhados e consolidados. Por exemplo, no relatório dos usuários que tiveram mais requisições bloqueadas, deve ser possível listar os dez usuários com mais requisições e quais foram às requisições bloqueadas para cada um deles;

Deve permitir exportar relatórios estatísticos e gerências de tráfego na Web, no mínimo, nos formatos: HTML, CSV e PDF;

Caso a solução ofertada para esta funcionalidade seja apenas composta por Software e execute em um servidor Windows virtualizado, apartado da Solução de Appliance de Proxy e Filtro de conteúdo, a Contratante irá fornecer esta infraestrutura de servidor e ambiente operacional necessária.

1.2.15. A Solução para Gerenciamento Centralizado – Hardware (Appliances) deverá possuir:

Fornecimento de um único dispositivo de Hardware do tipo Appliance ou software appliance para atendimento da funcionalidade de gerenciamento centralizado para Solução de Proxy e Filtro de conteúdo;

Deverá estar licenciado para gerenciar até 10 Appliances;

Seguindo com as melhores práticas de segurança, não serão aceitos como solução de Hardware, equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;

Capacidade técnica para gerenciar até 10 equipamentos;

Possuir, pelo menos, 2 interfaces ethernet 10/100/1000BT;

Possuir no mínimo 1 GB de memória RAM;

Possuir disco rígido com, pelo menos 320GB de espaço para armazenamento;

Possuir, no mínimo, uma interface serial RS-232;

Deve possuir fonte com tensão de entrada 110/220VAC, 50-60 Hz, com cabo de alimentação;

Deve ser montável em rack padrão de 19 polegadas, caso seja necessário kit para montagem, este deve acompanhar o equipamento, sem custo adicional;

Funcionalidades e características:

a. Deverá gerenciar todos appliances e softwares componentes das soluções de segurança Web;

b. Deverá ser capaz de gerenciar até 10 appliances e softwares em um único sistema;

c. Configurar e gerenciar a solução no tangente aos recursos de aceleração WAN;

d. Executar a funcionalidade de monitoração do status dos appliances componentes da solução em relação ao Hardware e Software (HealthCheck);

e. Gerenciamento remoto via interface gráfica para, no mínimo, 05 (cinco) usuários administrativos simultâneos com todas as funcionalidades ativas (GUI) ou Linha de comando (CLI);

f. Suportar autenticação de usuários do sistema via RADIUS, TACACS+ e LDAP/S;

g. Executar backup e restore da solução (Disaster Recovery);

h. Possibilitar o agendamento de tarefas a serem realizadas (Job Scheduling);

i. Executar a distribuição de políticas para os todos appliances componentes da solução;

j. Executar a distribuição de atualização de componentes (Software Upgrade) para os appliances componentes da solução;

k. Deverá suportar a modalidade de alta disponibilidade;

l. Deverá suportar configuração remota através de acesso via HTTPS, Telnet e SSH;

m. Permitir configurar e-mail para notificação de transferências com falha ou geração de TRAP SNMP para outro software de gerência;

n. Permitir gerenciamento baseado, no mínimo, em SNMPv2;

o. Armazenar arquivos de log e consolidar as informações de log dos equipamentos gerenciados.

1.3. **Proteção de Dados em Servidores Críticos –** A solução para "Proteção de Dados em Servidores Críticos", deve combinar Antivírus com uma prevenção avançada contra ameaças, IPS / IDS comportamental, Firewall, Reputação, visando fornecer uma defesa contra malware para Servidores e Aplicações Críticas. Integrando tecnologias de segurança essenciais em um único agente e console de gerenciamento, acarretando no aumenta da proteção.

1.3.1. Deve oferecer proteção proativa contra ataques tipo Dia-Zero diretamente no equipamento, para no mínimo:

Deve impedir a exploração maliciosa de sistemas e aplicações;

Deve prevenir a entrada e distribuição de códigos maliciosos.

1.3.2. Deve ter a capacidade de integração nativa com a tecnologia VMWare NSX, movendo de forma automática um determinado equipamento infectado para uma área de quarentena;

1.3.3. Deve ter a capacidade de liberar alguns serviços mesmo em área de quarentena, ao mover o equipamento identificado como infectado dentro do VMWare NSX;

1.3.4. Deve manter em conformidade com as políticas de seguranças através de verificações continua em clientes e servidores;

1.3.5. Deve efetuar "hardening" de sistemas operacionais, aplicações e bancos de dados;

1.3.6. Deve conter políticas de segurança nativas para aplicativos Microsoft;

1.3.7. Deve conter políticas de “hardening” padrões e nativas, possibilitando o fechamento do hardware, protegendo aplicativos de alto risco e base de dados, contra arquivos executáveis não autorizados a “rodar”;

1.3.8. Deve impedir a execução de aplicações não autorizadas;

1.3.9. Deve permitir ao Administrador bloquear trafego por porta, por protocolo, por IP ou por faixa de endereços IP;

1.3.10. Proteger arquivos e registros do sistema baseado em políticas;

1.3.11. Monitorar arquivos e registros do sistema baseado em políticas;

1.3.12. Deve possuir Sistema de Prevenção de Intrusos;

1.3.13. Deve possuir Sistema de Detecção de Intrusos;

1.3.14. Deve permitir ao administrador configurar filtros de eventos no agente, somente os eventos filtrados serão encaminhados para o servidor de gerenciamento;

1.3.15. Deve possuir sistema de atualização automática de políticas e pacotes de relatórios a partir do site do fabricante;

1.3.16. Deve ter a capacidade de importar e exportar políticas customizadas ou de terceiros;

1.3.17. Deve ter e capacidade de controlar o comportamento detectando e prevenindo ações especificas que uma aplicação ou usuários executem de forma a prejudicar o funcionamento do sistema ou aplicativo;

1.3.18. Deve possuir sistema de criação de usuários com perfis diferenciados de acesso aos recursos da console de gerenciamento;

1.3.19. Deve permitir o envio de alertas através de E-mail e SNMP baseados em filtros de eventos recebidos pela console de gerenciamento;

1.3.20. Deve possuir políticas predefinidas de monitoramento, de no mínimo os seguintes recursos:

Falha de acesso;

Logon com sucesso;

Detecção de logoff remoto;

Alteração de configuração pelo Usuário;

Alteração no grupo de gerenciamento.

1.3.21. Deve possuir agente remoto para monitorar arquivos e eventos em servidores sem o agente instalado;

1.3.22. Deve possuir recurso de prevenção contra acesso indevido de usuários e de aplicações a outros recursos do sistema, como arquivos, processos, bibliotecas e registros;

1.3.23. Deve ter a capacidade de através do recurso de controle de aplicação, monitorar com opção de bloqueio, as atividades da aplicação, assim como o recurso de rede e de dispositivos, exemplo controle de uso do USB e recursos de rede;

1.3.24. Deve ter a capacidade de prevenção contra ataques de exploração, com regras pré-definidas baseadas no comportamento padrão das aplicações do servidor;

1.3.25. Deve ter a capacidade de prevenção de intrusão baseado no comportamento das aplicações;

1.3.26. Deve possuir recurso nativo de firewall, restringindo atividades de rede por IP e Porta nos sentidos de entrada e saída;

1.3.27. Deve ter a capacidade de prevenção contra alteração de privilégios do servidor;

1.3.28. Deve ter a capacidade de prevenir contra alterações em arquivos e registros do servidor;

1.3.29. Deve ter a capacidade de proteção contra execução de instalações e operações não autorizadas no servidor;

1.3.30. Deve ter a capacidade de controlar e monitorar mídias removíveis;

1.3.31. Deve ter a opção de monitoramento granular de arquivos e diretórios dos servidores e estações;

1.3.32. Deve ter a capacidade de prevenir a adição de códigos de processos em memória para servidores Windows (memory injection protection);

1.3.33. Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros, possibilitando a coleta de logs de gerenciamento e correlação em “real-time”;

1.3.34. Deve ter a capacidade de implementar “sandbox” para as aplicações conhecidos do administrador, independente se são aplicações de mercado e proprietárias;

1.3.35. A solução deve ter a capacidade de no mínimo:

Bloquear instalações de aplicações indevidas;

Proteger o “core” do sistema operacional;

Proteger as áreas “RAW” dos discos locais.

1.3.36. Deve ter a capacidade de implementar listas avançadas de aplicações autorizadas (“Advanced White List”) a serem executadas, através da correlação das seguintes funcionalidades, sendo no mínimo os seguintes parâmetros:

Hash do arquivo executável para o processo específico (MD5 e SHA256);

Nome como é publicado, conforme é descrito no certificado emitido pelo fabricante da aplicação;

Assinatura digital das aplicações e aplicativos, incluindo componentes de sistema operacional, assinaturas Microsoft, assinaturas confiáveis, serviços e processos interativos;

Possibilidade de executar auditoria no AD, troca de usuário, reset de senha, permissão ou não, com relatórios sobre cada ajuste alterado na linha do tempo.

A solução deve ter a capacidade de implementar auditoria no Microsoft Active Directory, possibilitando elaborar relatórios com a periodicidade diária, semanal e mensal, para no mínimo:

a. Reset de senha;

b. Alteração de permissionamento;

c. Troca de usuário.

Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;

Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

a. Origem confiável;

b. Origem não confiável;

c. Tempo de existência do arquivo na internet;

d. Comportamento do arquivo;

e. Quantidade mínima de usuários que baixaram o arquivo da internet.

Capacidade de implementar regras distintas por grupo (ex. Departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;

Capacidade de identificar e proteger ataques direcionados, impossibilitando o início do ataque e não somente impedindo as ações após invasão do equipamento;

A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura virtual serviço de antivírus, para no mínimo:

a. VMware ESXi 5.1 e superior;
b. VMware vCenter 5.5 e superior;
c. VMware NSX.

A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura do VMware vSphere serviço de antivírus, funcionalidades de IDS e funcionalidades de IPS;

A solução deve ter a capacidade de implementar, em uma infraestrutura seja ela, física e virtual serviço de antivírus, funcionalidade de reputação de arquivos, funcionalidades de IDS, funcionalidades de IPS para no mínimo:

a. VMware ESXi 5.1 ou superior;
b. VMware vCenter 5.5 ou superior;
c. VMware NSX;
d. Windows 2000 Professional/Server/Advanced Server;
e. Windows XP Professional;
f. Windows Server 2003 Standard/ Enterprise 32-bit;
g. Windows Server 2003 Standard/ Enterprise 64-bit;
h. Red Hat Enterprise Linux ES 4.0;
i. SUSE Enterprise Linux 9.

A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura do VMware vSphere, funcionalidade de no mínimo:

a. Bloqueio a acesso não autorizado a Chaves SSL;
b. Tamper Protection de Binários;
c. Bloqueio a acesso não autorizado a arquivos de configurações;
d. Bloqueio a acesso não autorizado a chaves de registro;
e. Bloqueio a acesso não autorizado a arquivos de Logs;
f. Controle sobre privilégios de usuários e processos;
g. Monitoração da Integridade dos arquivos de vCenter;
h. Monitoração da Integridade dos arquivos dos Servidores ESXi 5.1 e superiores;

i. Monitoração da Integridade dos arquivos de configurações das VM Guest;

j. Monitoração direta dos LOGs nos servidores ESX, ESXi e vCenter.

A solução deve ter a capacidade de implementar as funcionalidades de controle de dispositivos e aplicações;

A solução deve ter a capacidade de implementar a funcionalidade de "File and Configuration Lock Down";

A solução deve implementar em um único agente as funcionalidades de HIPS, HIDS, Host Firewall, Application e Device Control.

1.3.37. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários da console de gerenciamento em ambientes físicos e virtuais:

Windows 7;

Windows Server 2003 Standard/ Enterprise 32-bit;

Windows Server 2003 Standard/ Enterprise 64-bit;

Windows Server 2008 e 2008 R2;

Windows Server 2012.

1.3.38. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do servidor de gerenciamento em ambientes físicos e virtuais:

Windows Server 2003 Standard/ Enterprise 32-bit;

Windows Server 2003 Standard/ Enterprise 64-bit;

Windows Server 2008 e 2008 R2;

Windows Server 2012.

1.3.39. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do agente:

1.3.39.1.1. Windows 7;

1.3.39.1.2. Windows Server 2003 Standard/ Enterprise 32-bit;

1.3.39.1.3. Windows Server 2003 Standard/ Enterprise 64-bit;

1.3.39.1.4. Windows 2008 e 2008 R2;

1.3.39.1.5. Windows 2012;

1.3.39.1.6. Red Hat Enterprise Linux ES 4.0 e 5.0;

1.3.39.1.7. SUSE Enterprise Linux 9, 10 e 11;

1.3.39.1.8. CentOS 6 Kernel 2.6.32-71.*el6, 2.6.32.220.*el6, 2.6.32-279.*el6, 2.6.32-358.*el6;

1.3.40. A solução deve ser suportada, no mínimo, nas seguintes versões de VMware:

VMware Workstation v5.0.0 e v5.5.4;

VMware ESX v3.0.1 e v3.0.2.

1.3.41. Os agentes devem ser suportados quando instalados nos seguintes sistemas operacionais tipo Guest em sistemas virtualizados VMWare:

Windows Server 2003 Standard/ Enterprise 32-bit;

Windows Server 2003 Standard/ Enterprise 64-bit;

Windows 2008 e 2008 R2;

Windows 2012;

Red Hat Enterprise Linux ES 4.0 e 5.0;

SUSE Enterprise Linux 9, 10 e 11;

CentOS 6 Kernel 2.6.32-71.*el6, 2.6.32.220.*el6, 2.6.32-279.*el6, 2.6.32-358.*el6.

1.3.42. O software deve suportar os componentes IDS e IPS, para no mínimo os seguintes sistemas operacionais:

Red Hat Enterprise Linux 4, 5 e 6;

CentOS 6;

SuSE Linux Enterprise Server 10 e 11;

Windows 2003 Standard e Enterprise (32 e 64 bit);

Windows 2008 Standard e Enterprise (32 e 64 bit).

1.3.43. O software deve suportar o componente IDS, para no mínimo os seguintes sistemas operacionais:

VMWare Server ESXi 5.5 Host;

VMWare Server ESXi 5.5 Host;

VMWare Server ESXi 5.0 Host;

VMWare Server ESXi 4.1 Host.

1.4. **Solução de Criptografia –** A solução de "Criptografia" deve ser capaz de cifrar todos os arquivos do disco rígido, setor por setor, de forma a proteger os dados confidenciais dos usuários sejam em desktop, notebook ou dispositivos móveis como Smartphones e tablets proporcionando um alto nível de segurança no que diz respeito a confidencialidade dos dados. Os dados devem ser decifrados apenas por usuários com devidas permissões.

1.4.1. A Solução de Criptografia para Endpoints deve possuir os seguintes requisitos gerais:

Suportar os seguintes sistemas operacionais: Suportar os seguintes sistemas operacionais:

a. Windows 7, 8, 8.1;

b. Windows Server 2008 R2, 2012 R2;

c. Ubuntu 14.04.1 LTS, 12.04.5 LTS (32-bit e 64-bit);

d. Red Hat Enterprise Linux/CentOS 7.1, 6.5, 6.0, 5.10, 5.9, (32-bit e 64-bit) e superiores.

Criptografia de Armazenamento Removível Baseada em Volumes;

Serviços de criptografia e funções de interação do usuário suportados para máquinas que não são integrantes do domínio;

A solução deve proteger dados gravados em dispositivos USB, fire-wire, pen-drives, CD/DVDs, discos rígidos externos, cartões digitais protegidos, ipods, câmeras digitais, e em dispositivos, mesmo quando não identificados como "removíveis";

Deve implementar a funcionalidade de “Chave de Múltipla Custódia“, onde existe a possibilidade de decriptar um volume por parte do administrador da ferramenta, apenas através da junção de múltiplas partes de chaves distintas em poder de administradores e atores diferentes.

A Instalação e Configuração do Cliente deve possuir as seguintes características:

a. Configuração simples e intuitiva de opções de instalação e políticas do cliente;

b. Configurações e políticas padrão do software cliente e instalação inclusas em um único pacote de instalação. Usa formato de instalação padrão (.MSI);

c. Capacidade de personalizar políticas de tempo de instalação para diferentes grupos de usuários;

d. O software cliente pode ser distribuído e instalado usando infraestrutura e processos existentes de distribuição de software;

e. Metodologia de implementação de cliente escalável para atender aos planos projetados de implementação;

f. Suporte à instalação silenciosa de software cliente;

g. A instalação e configuração do software não deve requerer a criação de compartilhamentos de rede, nem outras mudanças na infraestrutura da rede local;

h. A implementação do cliente deve requerer apenas 1 reinicialização no terminal, após a instalação.

As Opções de Políticas e Experiência do Usuário Final deve possuir as seguintes especificações:

a. Opção para tornar dispositivos removíveis de armazenamento somente para leitura até estarem criptografados;

b. Opção para forçar a criptografia de dispositivos removíveis de armazenamento;

c. Permitir que usuários apaguem, com segurança, o volume criptografado;

d. Permitir que usuários preservem os dados existentes no volume criptografado;

e. Os usuários criptografarão o volume com uma senha cuja força é determinada por uma política administrativa;

f. O volume criptografado deve ser acessado em qualquer terminal válido da plataforma com a senha de criptografia definida pelo usuário;

g. O recipiente da solução também deve poder ser descriptografado com uma chave de recuperação comandada por política;

h. Permitir que o usuário crie discos virtuais da solução a partir de pastas em um disco rígido local;

i. Os recipientes da solução podem ser gravados em CD/DVD;

j. Os CDs/DVDs criptografados com a solução devem poder ser acessados em qualquer terminal válido da plataforma, com a senha de criptografia;

k. Opção para permitir que os usuários alterem a senha da solução no primeiro uso. Isso permiterá que os administradores criem vários volumes criptografados e os dispersem para os usuários, conforme necessário, garantindo que serão criptografados com uma senha de usuário exclusiva;

l. Permitir que usuários alterem a senha da solução para um determinado dispositivo por meio de um utilitário na bandeja do sistema.

1.4.2. A Solução de criptografia de compartilhamentos de rede deve possuir os seguintes requisitos gerais:

Suportar os seguintes sistemas operacionais:

a. Windows 8.1 Enterprise (32-bit e 64-bit);

b. Windows 8.1 Pro (32-bit e 64-bit);

c. Windows 8 Enterprise (32-bit e 64-bit);

d. Windows 8 Pro (32-bit e 64-bit);

e. Windows 7 (32-bit e 64-bit);

f. Windows Server 2012 R2 (64-bit);

g. Windows Server 2012 (64-bit);

h. Windows Server 2008 R2 (64-bit);

i. Windows Server 2008 (32-bit);

j. Windows Server 2003 (32-bit e 64-bit).

A solução deve suportar no mínimo as seguintes áreas de armazenamento:

a. Compartilhamento de arquivos Windows (SMB, CIFS);

b. Samba, volúmes NAS e SAN;

c. Armazenamentos locais (internos e externos);

d. USB flash drives.

A solução deve suportar no mínimo os seguintes métodos de autenticação:

a. Chaves OpenPGP RFC 4880;

b. Certificados atendendo ao padrão X.509.

A solução deve suportar no mínimo o algoritmo de chaves simétricas 256-bit AES;

Configurações e políticas padrão do software cliente e instalação inclusas em um único pacote de instalação. Usa formato de instalação padrão (.MSI);

O software cliente deve poder ser distribuído e instalado usando infraestrutura e processos existentes de distribuição de software;

Metodologia de implementação de cliente escalável para atender aos planos projetados de implementação;

Suporte à instalação silenciosa de software cliente;

A instalação e configuração do software cliente não deve requerer privilégios de Administrador do Domínio;

A implementação do cliente deve requerer apenas 1 reinicialização no terminal, após a instalação;

Deve implementar a funcionalidade de “Chave de Múltipla Custódia”, onde existe a possibilidade de decriptar um volume por parte do administrador da ferramenta, apenas através da junção de múltiplas partes de chaves distintas em poder de administradores e atores diferentes.

As Opções de Políticas Administrativas devem possuir as seguintes especificações:

a. Permitir e Negar que usuários do terminal criem pastas da solução;

b. Permitir e Negar que usuários do terminal criptografem arquivos individuais com a solução;

c. Opção para forçar a criptografia de arquivos em pastas especificadas pelo administrador. Os arquivos nas pastas especificadas serão criptografados com a chave do usuário em cada terminal;

d. Opção para impedir a criptografia de arquivos em pastas especificadas pelo administrador;

e. Opção para criptografar arquivos criados com aplicativos de usuário definidos pelo administrador. Todos os arquivos definidos serão criptografados com a chave do usuário;

f. Opção para impedir a criptografia de arquivos criados por aplicativos específicos, como soluções de backup e FTP.

A Experiência do Usuário Final deve ser conforme as características descritas abaixo:

a. A solução deve ser inicializada pelo menu iniciar e pelo ícone na bandeja do sistema;

b. A funcionalidade da solução deve poder ser acessada pelo menu de contexto do Windows, clicando com o botão direito;

c. O usuário deve poder criar uma pasta protegida da solução;

d. O usuário deve poder adicionar usuários a uma pasta protegida da solução;

e. Os usuários adicionados a uma pasta protegida devem poder receber vários níveis de controle de acesso;

f. Usuários adicionais da pasta protegida devem poder adicionar outros usuários;

g. O usuário deve poder remover a criptografia da solução de um arquivo específico se for o administrador da pasta;

h. Os usuários da pasta da solução com permissão de administrador de grupo, ou administrador, podem remover o acesso de outros usuários à pasta criptografada da solução;

i. Quando usuários forem removidos da lista de acesso de uma pasta, os arquivos ali contidos serão atualizados para refletir a mudança;

j. Opção para importar lista de acesso de usuários de outra pasta protegida pela solução;

k. Arquivos protegidos em uma pasta da solução mostrarão uma dica visual ao usuário final, na forma de um ícone de cadeado azul e branco, sobre o ícone normal do arquivo;

l. Um usuário com a solução instalada, mas sem acesso a uma pasta específica, não poderá navegar pelo conteúdo de uma pasta protegida;

m. Um usuário sem a solução instalada poderá navegar pelo conteúdo de uma pasta criptografada pela solução, mas não poderá ler os arquivos criptografados;

n. As pastas da solução podem existir em um disco rígido local;

o. As pastas da solução podem existir em um dispositivo removível de armazenamento;

p. As pastas da solução podem existir em um servidor de arquivos na rede.

1.4.3. A Solução de criptografia de mensagens deve possuir os seguintes requisitos gerais:

Suportar os seguintes sistemas operacionais:

a. Windows 8 Enterprise (32-bit e 64-bit);

b. Windows 8 Pro (32-bit e 64-bit);

c. Windows 7 (32-bit e 64-bit);

d. Windows Server 2003;

A solução deve suportar as opções de autenticações, para no mínimo as seguintes:

a. Chaves OpenPGP RFC 4880;
b. Chaves padrão X.509.

A solução deve atender a no mínimo os seguintes padrões de mensageria:

a. SMTP/SMTPS
b. PGP/MIME RFC 3156;
c. POP/POPS
d. OpenPGP RFC 4880;
e. STARTTLS para POP/IMAP/SMTP
f. S/MIME v3 RFC 2633;
g. X.509 v3;
h. IMAP/IMAPS.

A solução deve suportar no mínimo os seguintes clientes de e-mail:

a. Outlook 2013 (32-bit e 64-bit)/Exchange Server 2013;
b. Outlook 2013 (32-bit e 64-bit)/Exchange Server 2010;
c. Outlook 2013 (32-bit e 64-bit)/Office 365 Cloud Server;
d. Outlook 2010 (32-bit e 64-bit)/Exchange Server 2010;
e. Outlook 2010 (32-bit e 64-bit)/Office 365 Cloud Server;
f. Outlook 2007 SP2 (Outlook 12)/Exchange Server 2007;
g. Outlook 2007 SP2 (Outlook 12)/Office 365 Cloud Server;
h. Outlook 2003 SP3/Exchange Server 2003 SP3;
i. Windows Mail 6.0;
j. Outlook Express 6 SP1;

A solução deve suportar no mínimo os seguintes Servidores de Correio Eletrônicos

a. Microsoft Exchange 2003, 2007 e 2010 SP1;

A solução deve suportar os algoritmos de Hashes, para no mínimo:

a. SHA-2 (até 512-bit);
b. SHA-1;
c. MD5;
d. RIPEMD-160.

A solução deve suportar no mínimo os algoritmos para a infraestrutura de chaves públicas;

a. Diffie-Hellman;
b. DSA (chaves de 1024-bit);

c. RSA (Chaves de até 4096-bit).

A solução deve disponibilizar um Web Mail Criptografado, com suporte a no mínimo os seguintes navegadores:

a. Internet Explorer 6, 7 e superiores;

b. Firefox 12 e superiores (Windows);

c. Firefox 16 e superiores (MAC OS);

d. Safari 5.1 e superiores.

A solução deve ter suporte à no mínimo os seguintes servidores:

a. Microsoft Exchange 2013;

b. Microsoft Exchange 2010 SP1;

c. Microsoft Exchange Server 2007;

d. Microsoft Exchange Server 2003 SP2;

O servidor de gerenciamento deve suportar o modelo "Soft Appliance" sendo instalado em uma seleção de hardware certificada e independente;

O servidor de gerenciamento deve suportar as plataformas de virtualização VMWare ESX 3.5.0, 4.0, ESXi 3.5.0;

Suportar criptografia forte e confiável baseada em padrões abertos e protegidos de mensagens, OpenPGP e S/MIME;

Suportar criptografia do corpo da mensagem e todos os anexos, além de suportar e também para várias codificações de conjuntos de caracteres;

Suportar criptografia no gateway e ponto a ponto com política central para controlar o comportamento e a interoperação entre ambos;

Suportar gerenciamento e publicação de chave central/certificados;

Suportar criptografia ponto a ponto pela integração com o Outlook, baseado em IMAP/POP/SMTP;

Suportar a recuperação de chave baseada em política ou pela organização, que pode ser dividida para armazenamento e uso seguro;

Ter a capacidade de criptografar tanto mensagem, quanto anexos da mesma mensagem, para no mínimo uma capacidade de 15MB.

1.4.4. O Servidor de Gerenciamento de Chave e Política deve possuir as seguintes especificações:

Deve ter a capacidade de suportar gerenciamento de chave e controle de políticas tanto para o e-mail do gateway (proxy SMTP) como para um cliente ponto a ponto opcional, sem a necessidade de neste momento estar licenciado;

Suporte para estender a mesma plataforma/servidor de gerenciamento para controlar diversas necessidades adicionais de criptografia de clientes;

Suportar opções de políticas granulares de e-mail para ativar a segurança de mensagens e diferentes ações com base nos destinatários;

Suportar autenticação administrativa opcional de dois fatores, através de integração nativa a partir de solução do mesmo fabricante;

Suportar funções administrativas;

Suportar múltiplos servidores de gerenciamento sincronizados para redundância, redirecionamento e escalabilidade;

Suportar agendamento automatizado e seguro do backup e opções integradas de recuperação;

Suportar registros detalhados, incluindo suporte para syslog remoto e relatórios integrados;

Suportar SNMP para monitoramento do sistema e alertas;

Suportar para hospedagem de um serviço de diretório de chave verificada para troca de chaves com parceiros e terceiros;

Suportar um repositório de chaves públicas hospedado por fornecedor para a troca e verificação de chaves com terceiros;

Suportar o uso do diretório existente LDAP para identidades de e-mail, autenticação e grupos de políticas, sendo no mínimo compatível com:

a. LDAPv2;

b. LDAPv3;

c. Servidor RSA Radius com RSA Authentication Manager.

Suportar sincronismo com estrutura de diretórios para demais tarefas e módulos, para no mínimo:

a. LDAPv2;

b. LDAPv3;

c. LDAPS;

d. Microsoft Active Directory 2012;

e. Microsoft Active Directory 2010;

f. Microsoft Active Directory 2008;

g. Microsoft Active Directory 2003;

Suportar gerenciamento automatizado de chave, como renovação, expiração e revogação, com suporte CRL integrado;

Suportar roteamento granular baseado em políticas para servidores de arquivo SMTP;

Suportar múltiplas opções flexíveis de distribuição de e-mail e os formatos de mensagem padronizados;

Suportar personalização/branding do portal baseado na web e para todos os modelos de mensagens;

Suportar geração automática de chaves e certificados e gerenciamento de ciclo de vida controlado por política administrativa;

Suportar política administrativa para permitir a redefinição de senhas de usuários externos do portal da web, de modo manual ou automático, via e-mail;

Suportar verificação automatizada de chaves e interoperação com outros parceiros que também usam a mesma solução do servidor central.

A Instalação e Configuração do Cliente deve possuir as especificações técnicas descritas abaixo:

a. Um único pacote MSI instala vários aplicativos de criptografia gerenciados por uma chave central e um servidor de políticas;

b. Criptografa, descriptografa, assina digitalmente e verifica mensagens de e-mail de modo automático e transparente, de acordo com políticas individuais ou de gerenciamento centralizado;

c. Quando implementado com uma solução de criptografia no gateway, o cliente pode distribuir mensagens de modo seguro para usuários externos que não possuem uma solução de criptografia de e-mail, independente do servidor de criptografia no gateway estar, ou não, no fluxo de e-mail;

d. Capacidade de impor políticas para usuários off-line controlando o que acontece com o e-mail quando o servidor de gerenciamento não pode ser alcançado pelo cliente de criptografia;

e. Capacidade de bloquear quais recursos estão habilitados, visíveis para os usuários e são obrigatórios - incluindo a criptografia manual opcional e botões que se integram com o Microsoft Outlook;

f. Opção administrativa para controlar a frequência com que um cliente recupera políticas atualizadas;

g. Capacidade de fornecer autenticação opcional de dois fatores usando smartcards, criando uma nova chave ou usando uma já existente.

A Experiência do Usuário Final deve seguir as especificações descritas abaixo:

a. Nenhuma alteração é necessária no comportamento do usuário, fornecendo uma experiência completamente transparente para usuários internos tanto da criptografia no gateway quando da criptografia ponto a ponto;

b. Capacidade opcional de ativar a criptografia de mensagens para usuários internos por meio de opções granulares de políticas, como os botões de assinatura/criptografia no Microsoft Outlook, usando uma linha de assunto especificada, e usando o identificador de confidencialidade no cabeçalho;

c. Permite que se use, com facilidade, as chaves e certificados de usuários externos para criptografia nativa S/MIME, quando possível;

d. Opção de distribuição segura, e sem identificar o cliente, para usuários externos sem chaves que aceitam respostas e suportam várias funções de autenticação;

e. Suporte à criptografia do formato PDF para o envio de mensagens em PDF criptografadas para usuários externos, para distribuição automatizada de extratos, podendo ser uma opção de distribuição selecionada pelo usuário, se isso for permitido pela política administrativa;

f. Opção para confirmação/certificação de entrega de mensagens em PDF criptografadas, exigindo uma senha única para cada mensagem a fim de informar quando um usuário acessou a senha da mensagem PDF criptografada;

g. Capacidade para permitir a destinatários externos, sem chaves de criptografia, selecionar a opção de entrega mais segura permitida pela política administrativa e alterá-la, quando necessário, pelo portal de mensagens seguras na web.

1.5. **<u>Solução para Prevenção de Ataques Direcionados</u> –** A solução para "Prevenção de Ataques Direcionados" deve ser capaz de identificar, antes que causem algum dano, possíveis ameaças avançadas que possam surgir no ambiente, sejam ela advindas da utilização de mídias removíveis, da internet ou até mesmo através de e-mails. Deve ser capaz de detectar, priorizar, investigar e corrigir possíveis ataques direcionados que estejam tentando causar danos ao ambiente computacional.

1.5.1. A solução deverá prover as funcionalidades de gerenciamento centralizado para os módulos de análise dos ambientes de endpoint, rede e e-mail;

1.5.2. A solução deve ter como característica básica a correlacionar as informações detectadas pelo módulo de APT de endpoint, módulo de APT de rede e módulo de APT de e-mail. Não serão aceitas correlações advindas somente das tecnologias de IPS/IDS;

1.5.3. O módulo de análise de e-mail deve ter a capacidade de identificar uma ameaça, mesmo que esta seja originada a partir de uma URL curta, fazendo uma inspeção no conteúdo original, mesmo antes do usuário ter acesso ao conteúdo indicado pela URL, possibilitando categorizar a origem da informação;

1.5.4. A tecnologia de Sand-box deve ser executada em ambiente tanto virtual como em bare-metal, utilizando como fonte de informação a rede mundial de inteligência do fabricante, a qual deve contar com a coleta de informações em no mínimo 90 milhões de máquinas, 3,7 petabytes de dados em seus registros;

1.5.5. O módulo de proteção no endpoint contra ataques de APT não pode ser um novo agente de segurança dentro da máquina cliente, as funções de APT deve ser realizadas pelo mesmo agente de proteção contra vírus, malwares;

1.5.6. O agente de proteção no endpoint contra ataques de APT deve executar esta proteção a partir do mesmo módulo que faz a proteção contra vírus, malware,... sem a necessidade de novos processos, DLL's, utilizando os mesmos já existentes para proteção das ameaças mais comuns (vírus, malwares,...), mantendo desta forma o mesmo processamento, sem consumo adicional de recursos;

1.5.7. A partir da console de gerenciamento da solução contra ataque de APT, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint, para que aquele determinado equipamento deve ir para uma área de quarentena;

1.5.8. A partir da solução contra ataques de APT, deve ser possível trabalhar em no mínimo 3 camadas distintas, conforme abaixo:

Detectar, onde é possível identificar as incursões;

Responder, onde é possível fazer a contenção e correção dos problemas;

Recuperar, onde é possível reestabelecer a operação.

1.5.9. A solução contra ataques deve ser capaz de identificar e agir contra os métodos de evasão dos dados, ou seja, identificar os AET (Advanced Evasive Threat);

1.5.10. A solução deve ter a capacidade de indicar o índice de comprometimento (IoC Indicators-of-Compromise) de um ataque, indicando em modo gráfico as relações e conexões existentes;

1.5.11. A solução contra os ataques de APT deve identificar o índice de comprometimento (IoC Indicators-of-Compromise) de um ataque, elencando no mínimo as seguintes informações:

Atividades suspeitas na organização;

Arquivos utilizados em determinado ataque;

Mensagens trocadas com os Arquivos suspeitos, identificando sua origem;

Endereçamentos IPs e domínios dos arquivos suspeitos.

1.5.12. A partir da console de gerencia deve ser possível identificar os IoCs nos agentes de Endpoint, possibilitando a identificação a partir de no mínimo:

Hash do arquivo;

Nome do arquivo;

Chave de Registro;

IP de origem;

URL.

1.5.13. A partir da console da solução contra os ataques de APT, deve ser possível executar diversas ações sobre os arquivos suspeitos, para no mínimo:

Categorizar e incluir em uma “Blacklist”;

Categorizar e incluir em uma “Whitelist”;

Submeter para análise em uma SandBox externa ao ambiente de produção;

Submeter o arquivo para apreciação de uma organização externa ao fabricante da solução, tal como VirusTotal;

Copiar o arquivo para uma área de armazenamento possibilitando verificação futura;

Deleção do Arquivo.

1.5.14. A solução contra ataques de APT (Advanced Persistent Threats) deve implementar a tecnologia de EDR (Endpoint Detection and Response), fornecendo uma visão única de todos os Indicadores de Comprometimento (IoC - Indicators of Compromise);

1.5.15. A solução contra ataques de APT (Advanced Persistent Threats) deve fornecer uma visão gráfica completa de como todos os IoC's estão ligados uns aos outros possibilitando determinar no mínimo:

Os arquivos usados em um determinado ataque;

Endereços de e-mail em que os arquivos pertencentes ao ataque foram originados;

Endereços IP onde os arquivos foram baixados.

1.5.16. A solução deverá ser executada em Hardware e Software específicos (appliance) com sistema operacional especializado ou em Software Appliance. Todas as funcionalidades deverão ser executadas no mesmo equipamento. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante;

1.5.17. O Hardware deve possuir as seguintes especificações:

Possuir no máximo 2U padrão 19" Rack;

Possuir no mínimo 02 (dois) processadores Hexa Core (6 cores);

Possuir no mínimo 32 GB de memória RAM;

Possuir no mínimo 02 (dois) discos rígidos 146GB;

Possuir configuração mínima de RAID entre os discos;

Possuir no mínimo 02 interfaces 10/100/1000BaseTX ou 10Gbps ;

Possuir fonte redundante e hot swappable;

Possuir interface de console do tipo RS-232, ou similar.

1.5.18. Implementar gerenciamento centralizado com no mínimo as seguintes funções: criação de regras de tratamento de malware, administração de usuários, configurações de host e network;

1.5.19. Implementar a funcionalidade de event server, com mecanismo de rotação automático dos arquivos de evento;

1.5.20. Implementar mecanismo de triangulação e correlação dos vetores de ataque;

1.5.21. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

1.5.22. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 ou similar;

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

1.5.24. Implementar sincronização de hora através de protocolo NTP;

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

1.5.26. 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;

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

1.5.28. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização de no mínimo as seguintes informações: Sumário de detecção e proteção, gráfico de top infecções, e gráfico da quantidade de e-mails monitorados;

1.5.29. Implementar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar o modo de operação;

1.5.30. Implementar a atualização (updates) dos appliances via mecanismo de push dos seguintes módulos: segurança de conteúdo e atualização de patch;

1.5.31. A solução deverá prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de call-backs;

1.5.32. Deve ter a capacidade para detecção de “Web Exploits” e “Command & Control”;

1.5.33. A solução deverá suportar no mínimo 2.000 usuários simultâneos;

1.5.34. A solução deverá ser executada em Hardware e Software específicos (appliance) com sistema operacional especializado ou em Software Appliance. Todas as funcionalidades deverão ser executadas no mesmo equipamento, com exceção das funcionalidades de relatórios, as quais deverão ser executadas em appliance ou servidor dedicado para este fim. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante;

1.5.35. Suportar os protocolos HTTP (Inbound), e protocolos TCP e UDP sem exceções (outbound);

1.5.36. Implementar e identificar existência de Malware em comunicações de entrada e saída;

1.5.37. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN;

1.5.38. Implementar detecção de Malwares que utilizem mecanismo de exploit em arquivos PDF;

1.5.39. Implementar detecção de Malwares que utilizem mecanismo do tipo zero-day ou semelhante nas seguintes aplicações: Microsoft Internet Explorer, Mozilla FireFox, Adobe Acrobat Reader, Adobe Acrobat, Microsoft Silverlight, SUN Java e RealPlayer, possibilitando integração com os módulos de Segurança de Endpoint (servidor e cliente), assim como, com o módulo de Segurança Avançada de Endpoint;

1.5.40. Implementar Rede de Inteligência proprietária do fabricantes existente em no mínimo 05 (cinco) localidades de forma a cobrir ataques originados de qualquer localidade global, com mecanismo opcional de retroalimentação de Malwares não identificados;

1.5.41. 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;

1.5.42. Deve ser capaz de utilizar o agente de Endpoint do próprio fabricante como agente de APT, sem a necessidade de implementação de agente exclusivo;

1.5.43. Deve ser capaz de utilizar, receber e consumir as informações advindas das aplicações Check Point, para refinar o comportamento local da rede, de forma a personalizar o resultado das inspeções, correlacionando TODAS as informações recebidas internamente com as recebidas através rede mundial de informações do próprio fabricante;

1.5.44. Deve ter integrações nativas com as, criptografia, IPS comportamental, GRC e proteção de endpoint;

1.5.45. Implementar no mínimo 02 modos de operação: in-line e out-of-band;

1.5.46. Implementar integração com ferramentas de SIEM;

1.5.47. Implementar mecanismo de integração com servidores Syslog;

1.5.48. A Analise de Malware Rede deve possuir as seguintes caracerísticas:

Implementar atualização a base de dados da Rede de Inteligência de forma automático;

Toda análise deve ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema;

Toda a verificação e análise de Malwares e/ou códigos maliciosos deve ocorrem em tempo real, não sendo aceitas verificações em cache engine ou batch mode;

O módulo de rede deve ter a capacidade de analisar a reputação categorizando se o(s) arquivo(s) ou aplicação(ões), minimamente em:

a. Já é conhecida ou não no ambiente computacional;

b. Indicando a quanto tempo existe na rede mundial de computadores;

c. Onde foi detectada sua primeira aparição e sob quais circunstâncias;

d. Identificar suas mutações e alvos de ataques.

O módulo de rede deve ter a capacidade de implementar tecnologia de IPS, utilizada dentre outras funcionalidades para identificar máquinas compromissadas com o possível ataque;

O módulo de rede deve ter a capacidade de implementar funcionalidades de Antivírus, blacklist para endereços IP's, URL e Domínios;

O módulo de rede deve ter capacidade de executar o conteúdo suspeito em um ambiente apartado baseado em cloud, evitando contato com o ambiente de produção, sendo implementado em dois modelos, tanto em ambiente virtual, quanto em ambiente bare-metal, evitando desta forma, o sucesso de ataques que exploram vulnerabilidade em ambientes virtuais;

O módulo de rede deve ter a capacidade de emular o comportamento humano na utilização de sistemas operacionais, aplicações onde suas vulnerabilidades são comumente exploradas, correlacionando tais resultados com uma análise comportamental entregue pela rede de inteligência mundial do fabricante.

1.5.49. O Console de Gerenciamento deve possuir as seguintes características:

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS:

Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 e similar;

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

Implementar sincronização de hora através de protocolo NTP;

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

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;

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

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

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 troughput de tráfego monitorado.

1.6. **Solução de Identificação Forte de Dispositivos -** Essa solução deve ser capaz de gerar um código identificador único para cada dispositivo que realiza acesso a um sistema Web, seja ele um desktop ou um dispositivo móvel, baseando-se em uma série de elementos de hardware e software e um código identificador único baseado nas características do navegador para os casos de acesso proveniente de browser de internet.

1.6.1. A solução de identificação de dispositivos desktop deve minimamente:

Atuar na forma de um componente de segurança em nível de sistema operacional, identificando o desktop do usuário no sistema Web do cliente;

Ser capaz de criar uma identificação única do desktop, com base em elementos de hardware e software, de forma a permitir o rastreamento da origem de acesso às aplicações, autorizando ou não o seu acesso;

Possuir capacidade de criptografar quaisquer dados entre o sistema web protegido e o ambiente computacional do usuário;

Possuir mecanismo de atualização automática, sem intervenção do usuário final;

Ter a capacidade de integrar-se ao sistema Web do cliente;

Ser compatível com os principais navegadores de internet do mercado: Microsoft Internet Explorer, versões 11 e Edge, Mozilla Firefox, Safari e Google Chrome, em suas versões mais atuais;

Possuir capacidade de automonitoramento dos arquivos que compõe a solução, restabelecendo-os em caso de alguma tentativa de corrompê-los ou de sua deleção;

Ser compatível com os principais sistemas operacionais do mercado: Microsoft Windows 7, 8.1 e 10, OSX 10.7, Ubuntu Linux (14, 15 e 16), Mint Linux 16 e 17, OpenSuse Linux 42.1, Debian Linux 8.5 e Canaima Linux (3.1 e 3.4).

1.6.2. Para dispositivo móvel a solução deve minimamente:

Possuir capacidade de gerar um identificador único e não reprodutível baseado em informações de hardware e software do dispositivo móvel;

Possuir capacidade de criptografar as informações trocadas entre o dispositivo móvel e o servidor de aplicação do aplicativo;

Ser compatível com as plataformas Android, do Google, e IOS da Apple;

Ter a capacidade de realizar a identificação de dispositivos móveis e disponibilizá-la sob a forma de um SDK – Kit de Desenvolvimento de Software, para ser facilmente incorporado aos aplicativos móveis distribuídos aos seus usuários;

O SDK (Kit de Desenvolvimento de Software) para a parte de servidores da solução, deverá ser compatível com aplicações Java v1.5, e .NET Framework v3.5, e suas versões superiores;

O SDK (Kit de Desenvolvimento de Software) deve possuir as seguintes funções:

a. Método que gere uma semente com informações de sessão;

b. Método de recuperação de identificação de um dispositivo móvel;

c. Método que valide a identificação de um dispositivo móvel;

d. Método de recuperação de identificação de sessão;

e. Método de criptografia/decriptografia dos dados transmitidos entre aplicativo e servidor.

Ter a capacidade de identificar dispositivos que façam uso de técnicas de “Jailbreak” e “Root” para o sistema iOS e Android, respectivamente;

Identificar emuladores ou simuladores de dispositivos móveis;

Identificar os sistemas operacionais e suas versões;

Permitir a identificação geográfica por meio de coordenadas oferecidas pelo GPS;

Ser capaz de integrar às aplicações do cliente e enviar informações relativas ao login do usuário;

Possuir código identificador e registrado em toda a estrutura de eventos gerados, contribuindo assim para auditorias futuras.

1.6.3. Para browser a solução deve minimamente:

Atuar na forma de uma biblioteca JavaScript capaz de identificar navegadores de internet;

Ser compatível com os principais navegadores de internet do mercado: Microsoft Internet Explorer, versões 11 e Edge, Mozilla Firefox, Safari e Google Chrome, em suas versões mais atuais;

Ser capaz de acoplar-se com o componente de segurança para desktop, fornecendo uma identificação única de máquina;

Possuir Kit de Desenvolvimento de Software para a parte de servidores da solução compatível com o Microsoft Windows Server 2008 ou superior;

O SDK (Kit de Desenvolvimento de Software) da parte de servidores deve oferecer os seguintes métodos:

a. Método capaz de retornar o acesso com maior grau de similaridade a partir de uma lista de acessos;

b. Método capaz de gerar um token de acesso;

c. Método capaz de realizar comparação entre duas impressões digitais dos navegadores;

d. Método capaz de pesquisar na base de dados da console de monitoramento e de combate à fraude, os últimos N acessos para um dado usuário retornando o grau de similaridade entre eles.

Mitigar tentativas de ataque por automação ao sistema Web protegido do cliente com base em métricas de digitação do usuário final;

Detectar e bloquear tentativas de cópias e colagens dentro de páginas Web, forçando assim, o seu preenchimento por digitação natural;

Possuir mecanismos de autoproteção contra engenharia reversa para as bibliotecas em JavaScript, tais como: Minificação do código-fonte; Ofuscação do código-fonte; Anti-debugging; Anti-tampering.

1.6.4. A Console de Administração, Gerenciamento e Monitoramento de Eventos de segurança deve:

Permitir acesso por meio de interface WEB;

Realizar o registro e acompanhamento de eventos que permitam a gerência das demais funcionalidades;

Realizar a recepção dos eventos em tempo real, descontando eventuais problemas de comunicação na rede do cliente;

Possuir capacidade de visualização de eventos em tempo real;

Possuir Interface gráfica no idioma português (Brasil);

Permitir registro de todas as atividades realizadas pelos operadores na interface para posteriores consultas;

Possibilitar o cadastro de usuário com diferentes níveis de acesso a todas as estruturas de configurações e informações disponíveis na console;

Possuir funcionalidade de reciclagem de logs, enviando-os a uma base de segundo nível diferente da exibida na interface principal, melhorando assim, a navegabilidade entre os registros;

Permitir que o acesso a interface gráfica seja por meio de usuário e senha configuráveis na própria console de gerenciamento;

Possuir compatibilidade com o protocolo de aplicação LDAP (Lightweight Directory Access Protocol);

Possibilitar o registro na base de informações da console de gerenciamento incluindo informações sobre a origem geográfica aproximada com base no endereço IP ou GPS (dispositivo móvel) registrada no momento do acesso ao sistema protegido do cliente;

Permitir que as informações constantes na interface gráfica sejam estruturadas por meio de consultas customizadas no padrão SQL;

Permitir a aplicação de filtros, agrupamentos e ordenações sobre o resultado das consultas;

Oferecer mecanismo de alerta para situações onde há eventos gerados a partir de computadores com alto nível de risco;

Oferecer mecanismo de envio de mensagem de alerta, parametrizado pelo usuário da console, quando detectada a propagação em massa de um mesmo evento em um dado período de tempo;

Permitir o rastreamento de estações de trabalho que tenham sido comprometidas por qualquer atividade maliciosa durante o acesso à aplicação WEB do cliente;

Enviar de registros (logs) de forma criptografada;

Possuir base compatível com banco de dados Microsoft SQL Server versão 2008 R2 ou superior e banco de dados Oracle 11G ou superior;

Disponibilizar relatórios sintéticos pré-determinados permitindo a visualização dos eventos por período contendo informações, tais como:

a. Quantidade de acessos por usuário a partir de um mesmo dispositivo móvel;

b. Número de acessos às aplicações por período;

c. Número de dispositivos móveis por usuário, utilizados para acesso às aplicações;

d. Número de usuários por dispositivos móveis, utilizados para acesso às aplicações;

e. Acessos a partir de dispositivos móveis que cometeram fraude;

f. Invasor encontrado em memória;

g. Invasor encontrado em arquivo;

h. Login de acesso à aplicaçãoweb;

i. Página falsa detectada;

j. Página suspeita detectada;

k. Alerta de acesso de máquina cadastrada em blacklist;

l. Alerta de acesso de máquina cadastrada em whitelist;

m. URL bloqueada pela blacklist.

1.7. **<u>Solução de Segurança da Informação e Monitoramento do Acesso a Aplicações Web com Recursos Avançados de Combate a Fraudes</u>** - Essa solução deve ser capaz de proporcionar um acesso seguro, cômodo e econômico, sem atritos para o usuário final. A Plataforma deve conferir ainda um único ponto de visão as ameaças digitais direcionadas ao endpoint, além de proporcionar uma administração centralizada, conferindo assim, a habilidade de combater de forma adaptativa aos novos riscos e mudanças inerentes da internet. Tecnologia de proteções para endpoint, nomeadas de Zero Day, e de reconhecimento visual de páginas devem se fazer presentes nesta solução.

1.7.1. Para aplicação em Desktop a solução deve minimamente:

Atuar na forma de um componente de segurança em nível de sistema operacional, protegendo o acesso do sistema Web do cliente contra ameaças digitais;

Oferecer proteção efetiva mesmo que o computador do usuário já esteja infectado por programas maliciosos;

Inibir a ação de grampos digitais de teclado, mouse e tela (keylogger, mouseloggers e capturadores de tela) e espiões de navegadores (spyware);

Possuir mecanismos de identificação de presença ou ausência de interação humana, bloqueando uso de processos automatizados maliciosos;

Proteger contra ataques do tipo envenenamento de transação, no qual um terceiro consegue aproveitar a autenticação feita pelo próprio usuário e se utilizar da sessão;

Proteger contra ataques que utilizem a técnica de tecla emulada;

Proteger contra ataques que se baseiem na utilização de sessões abertas através de certificação digital (envenenamento de transação);

Monitorar conexões maliciosas de artefatos maliciosos;

Identificar e proteger contra ataques de página falsa por heurística de análise visual (Somente em ambientes Microsoft Windows);

Proteger contra ataques que se baseiem na utilização de sessões abertas através de certificação digital (envenenamento de transação);

Proteger contra alterações no DNS local da máquina;

Identificar proxies maliciosos através de mecanismos de detecção baseado em heurística e através de uma base de definições;

Possuir proteção contra as técnicas “man-in-the-middle” e “man-in-the-browser”;

Oferecer proteção contra códigos maliciosos, tais como, trojans, worms, backdoor e rootkits;

Possuir uma base de assinaturas como mecanismo de contingência que é atualizada de forma automática;

Identificar se o login do usuário foi comprometido por alguma aplicação em execução no computador do usuário final;

Oferecer proteção contra uso de credenciais em processos suspeitos;

Possuir capacidade de bloqueio (Blacklist) ou a liberação (Whitelist) de certos elementos no computador do usuário. Tais como: Endereços de domínios e URLs; Endereços IPs; Arquivos e Programas; Caminhos de arquivos;

Possuir mecanismo de atualização automática, sem intervenção do usuário final;

Ser capaz de integrasse ao sistema Web do cliente;

Ser compatível com os principais navegadores de internet do mercado: Microsoft Internet Explorer, versões 11 e Edge, Mozilla Firefox, Safari e Google Chrome, em suas versões mais atuais;

Ter a capacidade de ofertar uma identificação única de estações de trabalho, com base em elementos de hardware e software, de forma a permitir o rastreamento da origem de acesso às aplicações, autorizando ou não o seu acesso;

Possuir proteção contra terminações não autorizadas do componente de segurança, de forma que seu processo em memória não possa ser terminado/desativado/inibido, tanto por ataques por programas maliciosos quanto pelos usuários;

Possuir a capacidade de automonitoramento dos arquivos que compõe a Solução, restabelecendo-os em caso de alguma tentativa de corrompê-los ou de sua deleção;

Possuir proteção contra ataques de automação e monitoramento do uso de credenciais em processos de terceiros em plataforma Linux;

Compatível com os principais sistemas operacionais do mercado: Microsoft Windows 7, 8.1 e 10, OSX 10.7, Ubuntu Linux (14, 15 e 16), Mint Linux 16 e 17, OpenSuse Linux 42.1, Debian Linux 8.5 e Canaima Linux (3.1 e 3.4).

1.8. Serviços de Manutenção evolutiva e Atualizações.

1.8.1. Os critérios descritos no item 1.8 e seus subitens devem ser aplicados aos itens de 1 ao 7 da tabela 3.2 deste Termo de Referência.

1.8.2. A CONTRATADA deve disponibilizar serviços de suporte técnico e manutenção incluem o direito as atualizações de todos os componentes fornecidos de acordo com a disponibilização do fabricante para novas versões incluindo melhorias, evoluções, novas funcionalidades e correções de defeitos diferentes daqueles caracterizados e atendidos pela garantia legal da contratação.

1.8.3. Prestar os serviços de suporte técnico e manutenção tecnológica da solução nos dias úteis das 09h00 às 18h00 com atendimento remoto ou presencial, quando assim julgado pelo atendente, pelo fabricante ou revenda autorizada pelo fabricante da solução.

1.8.4. Os serviços de suporte técnico e manutenção da Solução deverão ser executados mensalmente.

1.8.5. A qualquer momento a CONTRATANTE poderá solicitar relatórios contendo as informações de suporte técnico e manutenção tecnológica sempre que solicitado, apresentando as informações do período de apuração solicitado.

1.8.6. Relatório, quando solicitado, deverá apresentar minimamente:

a. Quadro resumo apresentando:
b. Quantidade de atualizações;
c. Quantidade de chamados em aberto;
d. Quantidade de chamados fechados;
e. Quantidade de chamados abertos;
f. Detalhamento dos chamados, apresentando, quando aplicável:
g. Data de abertura;
h. Solicitante;
i. Data de atendimento;
j. Data de apresentação e efetiva adoção da solução de contorno;
k. Data de apresentação da proposta de solução definitiva.

1.8.7. Disponibilizar canal via WEB ou e-mail para abertura de chamados bem como solicitação a documentações e versões da solução ou qualquer de seus componentes.

1.8.8. Todos os chamados apresentarão, ao menos as seguintes informações:

a. Dados do requisitante;
b. Descrição direta do problema relatado;
c. Dados do sistema operacional utilizado;
d. Navegador e versão utilizado;

1.8.9. A Contratada deverá disponibilizar recurso humano designado para fornecer assistência ao gerenciamento de todos os incidentes de suporte cadastrados.

1.8.10. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto no item 1.8.9, deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante.

1.8.11. Deverão ser fornecidos para consumo 120 dias em meio período, durante o horário comercial de um engenheiro do fabricante, devidamente registrado no quadro de funcionários do fabricante, através do regime de CLT, e será designado para tarefas, de no mínimo, manutenção proativa, reparos e análise de capacidade, esta comprovação deverá ser entregue juntamente com a entrega dos manuais de comprovação técnica, em conjunto com a fase de homologação.

O previsto no item 1.8.11 não é caracterizado uma consultoria, trata-se de possibilidade de acesso aos engenheiros do fabricante, garantindo as melhores práticas no processo da implementação da solução adquirida.

1.9. Unidade de Serviço Técnico - UST (Operação Assistida)-

1.9.1. As Unidades de Serviço Técnico serão utilizadas sob demanda, a critério do Contratante, para realização de atividades relacionadas à solução de segurança, tais como, mas sem se limitar a:

Procedimentos em conjunto com o fabricante da solução, para situações em que o site do Contratante esteja com previsão e/ou sofrendo ataque, destinado a prover o conhecimento para as medidas necessárias à defesa do ambiente;

Procedimentos de ajuste para manter a solução adquirida pelo Contratante provendo a melhor utilização de suas funcionalidades;

Reuniões técnicas, mensais ou a critério do Contratante, para planejamento e execução de serviços com vistas à melhoria do ambiente instalado;

Reuniões gerenciais, mensais ou a critério do Contratante, para avaliação e acompanhamento dos serviços oferecidos.

1.9.2. Os serviços de operação assistida consistem na prestação de, no mínimo, os serviços listados no Apêndice B deste Termo de Referência.

1.9.3. Sempre que necessário, a Contratada deverá efetuar vistoria técnica nas dependências do Contratante de modo a realizar análise e implementar as alterações necessárias;

1.9.4. Os serviços de operação assistida serão prestados remotamente, quando possível, e presencialmente, sempre que se fizer necessário. A definição da necessidade de prestação de suporte presencial caberá à Contratante em conjunto com a contratada.

1.9.5. Para atendimento ao serviço de operação assistida a Contratada somente poderá empregar profissionais capacitados nos produtos fornecidos;

1.9.6. Os serviços de operação assistida serão adquiridos por meio de Unidades de Serviço Técnico (UST).

1.9.7. A unidade de medida adotada (UST) corresponde ao esforço padronizado para determinada complexidade, independentemente da quantidade de recursos humanos alocados. O pagamento é condicionado à prestação dos serviços e atendimento aos níveis de serviços especificados.

1.9.8. O Contratante oficializará a solicitação deste apoio por meio da emissão de uma “Ordem de Serviço – OS”;

1.9.9. A Ordem de Serviço deverá conter no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;

1.9.10. Os serviços prestados deverão estar no mínimo de acordo com as especificações constantes na Ordem de Serviço;

1.9.11. O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a “Ordem de Serviço – OS” é emitida pelo Contratante, durante a execução – com o acompanhamento e supervisão de responsáveis do Contratante, e ao término da execução – com o fornecimento de “Relatórios de Atividade da Operação Assistida” pela Contratada e atesto dos mesmos por responsáveis do Contratante;

1.9.12. O “Relatório de Atividade da Operação Assistida” deverá conter:

Identificação do Relatório de Atividade Operação Assistida;

Data da Emissão;

Número do Contrato;

Descrição detalhada das atividades executadas e, se for o caso, o detalhamento da solução proposta para os problemas apresentados.

1.9.13. A partir da emissão da "Ordem de Serviço – OS", a Contratada terá até 05 (cinco) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;

1.9.14. O Contratante comunicará à Contratada quando uma "Ordem de Serviço – OS" estiver sendo elaborada para que a Contratada possa se manifestar no interesse de agendamento de reunião para definição de procedimentos e horas necessárias para execução dos serviços;

1.9.15. Os procedimentos previstos inicialmente quando da abertura da "Ordem de Serviço – OS" serão validados no final das atividades e poderão sofrer adequações para estarem de acordo com o que foi efetivamente executado;

1.9.16. A Contratante fará uso e efetuará o pagamento apenas das USTs necessárias à implementação e manutenção dos serviços que solicitar, até o limite máximo das USTs estimadas. A Contratante não realizará pagamento prévio de USTs sob qualquer hipótese.

1.9.17. A quantidade de USTs por serviços ofertados não poderá ser superior ao quantitativo definido no Apêndice B deste Termo de Referência.

1.9.18. A quantidade de USTs de serviços não listados no Apêndice B, mas requisitados pela Contratante, deverá ser negociada por meio de OS, de acordo com o modelo fornecido no Apêndice G (Modelo de Ordem de Serviço).

1.9.19. Os valores de referência UST especificados no Apêndice B terão seu cômputo ajustado de acordo com a natureza da solicitação, conforme detalhado na tabela abaixo.

Natureza da solicitação

Natureza da tarefa	Complexidade	Ajuste no valor de referência (fator multiplicador)
Planejamento/criação/diagnóstico	Alta	1
Execução/alteração/implantação	Média	0,8
Exclusão	Baixa	0,6
Monitoração	Muito baixa	0,4

1.9.20. As tarefas de complexidade alta, média e baixa serão cobradas com base em cada solicitação atendida. As tarefas de monitoração compreendem todos os chamados relativos ao serviço previamente planejado e executado, e será cobrada uma única vez por mês, independentemente do número de chamados de monitoração para aquele serviço abertos naquele mês.

1.9.21. Este serviço deve estar disponível para acionamento no sistema 24 horas por dia x 7 dias por semana.

----------FIM DO APÊNDICE "A"----------

DEFENSORIA PÚBLICA DA UNIÃO

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

APÊNDICE B

SERVIÇOS DE OPERAÇÃO ASSISTIDA

	Descrição do serviço	Valor de referência (em UST)	Complexidade	Valor (em UST)	Prazo máximo (em horas úteis)
a.	Serviço para Solução de Proteção de Estação de Trabalho, Servidores e Mensageria.	0,8	Alta	0,8	80
			Média	0,64	160
			Baixa	0,48	24
			Muito baixa	0,32	16
b.	Serviço para Gateway de Segurança WEB.	1,1	Alta	1,1	32
			Média	0,88	120
			Baixa	0,66	8
			Muito baixa	0,44	8
c.	Serviço para Proteção de Dados em Servidores Críticos.	0,8	Alta	0,8	80
			Média	0,64	160
			Baixa	0,48	24
			Muito baixa	0,32	16
e.	Serviço para Solução de Criptografia	0,9	Alta	0,9	24
			Média	0,72	32
			Baixa	0,54	24
			Muito baixa	0,36	8
f.	Serviço para Solução para Prevenção de Ataques Direcionados.	1,1	Alta	1,1	80
			Média	0,88	240
			Baixa	0,66	32
			Muito baixa	0,44	32
g.	Serviço para Solução de Identificação Forte de Dispositivos	1,9	Alta	2,6	23,5
			Média	2,08	603,6
h.	Serviço para Solução de Segurança da Informação e Monitoramento do Acesso a Aplicações Web com Recursos Avançados de Combate a Fraudes	2,8	Alta	3	40
			Média	2,4	86

a) Serviço para Solução de Proteção de Estação de Trabalho, Servidores e Mensageria – Consiste na execução de atividades relacionadas ao componente de Proteção de Estação de Trabalho, Servidores e Mensageria que deve ter uma combinação de Antivírus, IDS/IPS, Firewall entre outras.

b) Serviço para Gateway de Segurança WEB – Consiste no desenvolvimento de tarefas que possibilitem realizar um planejamento, diagnóstico, implementação, monitoração, dentre outras do componente de gateway de segurança web.

c) Serviço para Proteção de Dados em Servidores Críticos – Deve realizar ações para garantir o pleno funcionamento do componente de proteção de dados, assim como sua monitoração e diagnóstico.

d) Serviço para Solução de Criptografia – Este serviço deve dispor de atividades como implantação, configuração e teste do componente de criptografia, assim como demais atividades relacionadas a este componente.

e) Serviço para Solução para Prevenção de Ataques Direcionados – Consiste na aplicação de regras e em diagnosticar que as melhores práticas estejam aplicadas ao componente antes, durante ou depois de sua implementação.

f) Serviço para Solução de Identificação Forte de Dispositivos – Consiste em fornecer recursos que possam executar tarefas que estejam diretamente relacionadas ao componente para identificação forte de dispositivos.

g) Serviço para Solução de Segurança da Informação e Monitoramento do Acesso a Aplicações Web com Recursos Avançados de Combate a Fraudes – Consiste em fornecer recursos que possam executar tarefas que estejam diretamente relacionadas ao componente de Segurança e Monitoramento do Acesso.

----------**FIM DO APÊNDICE “B”**----------

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

APÊNDICE "C"

MODELO DE PROPOSTA DE PREÇOS

(em papel timbrado da empresa e assinado)

À DEFENSORIA PÚBLICA DA UNIÃO

Proposta que faz a empresa _____ _____ para o fornecimento de licença de uso, sua respectiva manutenção e suporte técnico em ambiente corporativo da Solução de Segurança e Gerenciamento Seguro da Informação e Solução integrada Segurança Digital com conceito de blindagem do domínio web, incluindo a prestação de serviços técnicos especializados, operação, fornecimento da aquisição e manutenção, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União – DPU.

Fornecimento de licença de uso, sua respectiva manutenção e suporte técnico em ambiente corporativo da Solução de Segurança e Gerenciamento Seguro da Informação e Solução integrada Segurança Digital com conceito de blindagem do domínio web, incluindo a prestação de serviços técnicos especializados, operação, fornecimento da aquisição e manutenção, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União – DPU

LOTE	ITEM	UNIDADE	DESCRIÇÃO	QTDE	Valor Unitário	Valor Total
1	1	Usuários	Solução de Proteção de Estação de Trabalho, Servidores e Mensageria.	2000		
	2	Serviço	Manutenção evolutiva e atualização da Solução de Proteção de Estação de Trabalho, Servidores e Mensageria, pelo período de 12 (doze) meses.	2000		
	3	Conexões Simultâneas	Gateway de Segurança WEB.	2000		
	4	Serviço	Manutenção evolutiva e atualização do Gateway de Segurança WEB, pelo período de 12 (doze) meses.	2000		
	5	Servidores	Proteção de Dados em Servidores Críticos.	300		

	6	Serviço	Manutenção evolutiva e atualização da Proteção de Dados em Servidores Críticos, pelo período de 12 (doze) meses.	300			
	7	Usuários	Solução de Criptografia	700			
	8	Serviço	Manutenção evolutiva e atualização da Solução de Criptografia, pelo período de 12 (doze) meses.	700			
	9	Usuários	Solução para Prevenção de Ataques Direcionados.	2000			
	10	Serviço	Manutenção evolutiva e atualização da Solução para Prevenção de Ataques Direcionados, pelo período de 12 (doze) meses.	2000			
	11	Licença Perpétua	Solução Suite de Identificação Forte de Dispositivos.	1			
	12	Serviço	Manutenção evolutiva e atualização da Solução Suite de Identificação Forte de Dispositivos, pelo período de 12 (doze) meses.	1			
	13	Licença Perpétua	Solução de Segurança da Informação e Monitoramento do Acesso a Aplicações Web com Recursos Avançados de Combate a Fraudes.	1			
	14	Serviço	Manutenção evolutiva e atualização da Solução de Segurança da Informação e Monitoramento do Acesso a Aplicações Web com Recursos Avançados de Combate a Fraudes, pelo período de 12 (doze) meses.	1			
	15	UST**	Unidade de Serviço Técnico (Operação Assistida)	2554			

VALOR TOTAL SERVIÇOS(CUSTEIO):
VALOR TOTAL LICENÇAS(INVESTIMENTO):
VALOR TOTAL GERAL:

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

Declaro que no preço cotado estão inclusas todas as despesas que incidem direta e indiretamente sobre os serviços prestados, tais como impostos, taxas, tributos, insumos, mão-de-obra e outras.

Dados da empresa:
Razão Social: _____
CNPJ (MF) nº: _____
Inscrição Estadual nº: _____
Endereço: _____
Fone: _____ Fax: _____
Cidade: _____ Estado: ___ CEP:_____

A presente proposta tem validade de **60 (sessenta) dias.**
Local e data

_____
Assinatura e carimbo do Representante Legal da Empresa
Observação: Emitir em papel que identifique a licitante

----------FIM DO APÊNDICE "C"----------

APÊNDICE "D"

MODELO DE DECLARAÇÃO DE VISTORIA

DECLARAÇÃO DE VISTORIA

Pela presente declaramos conhecer e compreender por inteiro o teor do PREGÃO ELETRÔNICO nº _____/2017, cujo objeto é a Contratação de empresa especializada para fornecimento da aquisição, manutenção, atualização e upgrade de Solução de Segurança Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União – DPU, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente.

Declaramos, outrossim, ter visitado o local dos serviços a serem executados em companhia do representante da Secretaria de Tecnologia da Informação.

Empresa:_____
C.N.P.J.(MF):_____Tel/Fax:_____
__
Endereço:_____
_
Nome do Representante: _____
Endereço Eletrônico (e-mail):
_____

_____
Representante da Empresa

Declaro que o representante da empresa acima identificada visitou os locais de execução dos serviços.

Brasília, de de 2017

Secretaria de Tecnologia da Informação – STI
Defensoria Pública da União

----------FIM DO APÊNDICE "D"----------

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

APÊNDICE "E"

MODELO DE DECLARAÇÃO DE RECUSA DE VISTORIA

DECLARAÇÃO DE RECUSA DE VISTORIA

Pela presente declaramos conhecer e compreender por inteiro o teor do PREGÃO ELETRÔNICO nº _____/2017, cujo objeto é a Contratação de empresa especializada para fornecimento da aquisição, manutenção, atualização e upgrade de Solução de Segurança Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União – DPU, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente.

Outrossim, optamos pela não realização da vistoria técnica nas instalações físicas da Secretaria de Tecnologia da Informação/DPU, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos.

Empresa:_____
C.N.P.J.(MF):_____Tel/Fax:_____
__
Endereço:_____
_
Nome do Representante: _____
Endereço Eletrônico (e-mail):
_____

_____
Representante da Empresa

Declaro que o representante da empresa acima identificada optou pela não realização de vistoria técnica nos locais de execução dos serviços.

Brasília, de de 2017

Secretaria de Tecnologia da Informação – STI
Defensoria Pública da União

----------FIM DO APÊNDICE "E"----------

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

APÊNDICE "F"

MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO Nº **Contrato Número** **Contratada**	**PRAZO:** Execução Início: Execução Final:
Área Requisitante:	**Unidade de Medida:** **Quantidade: _____ Valor R$ _____**

LISTA DE ATIVIDADES

Item	Descrição	Qtde.	Valor R$
	TOTAL PREVISTO DA OS		

Aprovação	
Fiscal Demandante	Fiscal Administrativo
Fiscal Técnico	

----------FIM DO APÊNDICE "F"----------

ANEXO II

ATA DE REGISTRO DE PREÇO

Aos _____ dias do mês de _____ do ano de dois mil e dezessete, na sede da DPU - Defensoria Pública da União, localizada Setor de Autarquias Norte - SAUN, Quadra 05, Lote C, Bloco C, Centro Empresarial CNC - Bairro Asa Norte - CEP 70040-250 - Brasília - DF, inscrita no CNPJ sob n.º 00375114/0001-16, neste ato representada pelo Secretário Geral-Executivo,_____, e a empresa _____, inscrita no CNPJ sob n.º_____, estabelecida na Rua, Estado do _____, neste ato representada pelo seu _____, Sr. _____, resolvem nos termos do Decreto 7.892/2013, bem como da Lei 8.666/93, da Lei 10.520/2002 e Lei Complementar 147/2014, e em conformidade com o Pregão Eletrônico n.º ____/2017, devidamente homologado à fol. ____ do aludido processo, REGISTRAR PREÇOS, para eventual aquisição dos objetos a seguir, conforme especificações constantes no Termo de Referência respectivo.

ITEM	LOCAL DE ENTREGA	QUANTIDADE DE REGISTRO	PREÇO UNITÁRIO	PREÇO TOTAL

EMPRESA:	
CNPJ:	
ENDEREÇO:	
TELEFONE:	
PESSOA PARA CONTATO:	
E-MAIL:	

CLÁUSULA PRIMEIRA – DO OBJETO

Constitui objeto da presente Ata de Registro de Preços, a Contratação de Soluções de Segurança integradas compreendendo: Fornecimento de licença de uso, sua respectiva manutenção e suporte técnico em ambiente corporativo da Solução de Segurança e Gerenciamento Seguro da Informação e Solução integrada Segurança Digital com conceito de blindagem do domínio web, incluindo a prestação de serviços técnicos especializados, operação, fornecimento da aquisição e manutenção, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União - DPU - em âmbito nacional, conforme quantidades, condições e especificações constantes no Termo de Referência.

CLÁUSULA SEGUNDA - DA VALIDADE DOS PREÇOS

Esta Ata de Registro de Preços, documento vinculativo obrigacional com característica de compromisso para futura contratação, terá validade de 12 (doze) meses, a contar da data de sua homologação.

Parágrafo Primeiro - Durante o prazo de validade desta Ata de Registro de Preços a CONTRATANTE não estará obrigada a adquirir o material referido na Cláusula Primeira exclusivamente pelo Sistema de Registro de Preços, podendo fazê-lo por meio de outra licitação quando julgar conveniente, sem que caiba recurso ou indenização de qualquer espécie ao FORNECEDOR REGISTRADO, sendo, entretanto, assegurada aos beneficiários do registro, a preferência de fornecimento em igualdade de condições.

Parágrafo Segundo - A partir da assinatura da Ata de Registro de Preços o FORNECEDOR REGISTRADO assume o compromisso de atender, durante o prazo de sua vigência, os pedidos realizados e se obriga a cumprir, na íntegra, todas as condições estabelecidas, ficando sujeito, inclusive, às penalidades legalmente cabíveis pelo descumprimento de quaisquer de suas cláusulas.

Parágrafo Terceiro - A contratação decorrente desta Ata será formalizada pela emissão de Nota de Empenho de Despesa e competente Autorização de Material, a qual deverá ser assinada e retirada pelo Fornecedor no prazo máximo de 03 (três) dias úteis a contar da comunicação da CONTRATANTE.

Parágrafo Quarto - Mediante a retirada da Nota de Empenho e Autorização de Material, estará caracterizado o compromisso de entrega do material.

CLÁUSULA TERCEIRA – DOS PREÇOS

Os preços, expressos em Real (R$), serão fixos e irreajustáveis pelo período de 12 (doze) meses, contado a partir da assinatura da presente Ata de Registro de Preços.

CLÁUSULA QUARTA - DO CONTROLE E ALTERAÇÃO DE PREÇOS

A Ata de Registro de Preços não poderá sofrer alterações, conforme estabelece o art. 12, §1º, do Decreto nº 7.892/2013.

Parágrafo Primeiro - O preço registrado poderá ser revisto em face de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos bens registrados.

Parágrafo Segundo - Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado a CONTRATANTE convocará o FORNECEDOR visando à negociação para redução de preços e sua adequação ao praticado pelo mercado.

Parágrafo Terceiro - Frustrada a negociação, o FORNECEDOR será liberado do compromisso assumido.

Parágrafo Quarto - Na hipótese do parágrafo anterior, a CONTRATANTE convocará os demais fornecedores visando igual oportunidade de negociação.

Parágrafo Quinto - Quando o preço de mercado tornar-se superior aos preços registrados e o FORNECEDOR, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, a CONTRATANTE poderá:

I – Liberar o FORNECEDOR do compromisso assumido, sem aplicação de penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, se a comunicação ocorrer antes do pedido de fornecimento;

II - Convocar os demais fornecedores visando igual oportunidade de negociação.

Parágrafo Sexto - Não havendo êxito nas negociações, a CONTRATANTE procederá a revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

CLÁUSULA QUINTA - DO LOCAL E PRAZO DE ENTREGA

Parágrafo Primeiro - A execução do projeto será realizada de acordo com o cronograma abaixo.

Os prazos estabelecidos são os prazos máximos de duração de cada fase.

Item	Descrição do evento	Prazo Máximo	Responsável
1	Abertura da ordem de serviço	D1	Contratante
2	Projeto de Implementação	D2 = D1 + 1	Contratada
3	Reunião Inicial de Projeto	D3 = D2 + 1	Contratante e Contratada
4	Entrega dos produtos	D4 = D1 + 7	Contratada
5	Instalação, configuração e implantação	D5 = D4 + 40	Contratada
6	Treinamento	D6 = D4 + 10	Contratada

Parágrafo Segundo – Os equipamentos deverão ser entregues no endereço constante no ITEM 22.11 do Termo de Referência

Parágrafo Terceiro - As quantidades e o prazo de entrega dos objetos obedecerão aos critérios estabelecidos no Termo de Referência, e no Edital do Pregão ___/2017.

CLÁUSULA SEXTA - DAS CONDIÇÕES DE FORNECIMENTO

O recebimento do material deverá ser acompanhado e fiscalizado por um representante da Administração, especialmente designado, pelo chefe imediato do setor em que será feita a entrega do material.

Parágrafo Primeiro - O material, objeto do Termo de Referência estará condicionado à conferência para aceitação/aprovação final, a ser realizada pelo servidor responsável pelo recebimento do material que o efetuará provisoriamente e definitivamente, nos termos da alínea "a" e "b" do art. 73, inc. II, da Lei n.º 8.666/93.

Parágrafo Segundo - O material será recebido da seguinte forma:

a) Provisoriamente – para efeito de posterior verificação da conformidade do material com as especificações;

b) Definitivamente – após a verificação da qualidade e quantidade dos materiais e consequente aceitação, no prazo máximo de 10 (dez) dias úteis após a aceitação provisória observada o art. 69 da Lei 8.666 que determina: "O contratado é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto da Ata em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados".

CLÁUSULA SÉTIMA – DA FORMALIZAÇÃO

Será firmado contrato de fornecimento e garantia do objeto com a licitante vencedora, o qual tomará por base os dispositivos da Lei nº 8.666/93, as condições estabelecidas neste Edital e seus anexos, bem como, as constantes da proposta apresentada pela adjudicatária.

Parágrafo Primeiro - Após regular convocação por parte da Defensoria Pública da União, a empresa adjudicatária terá prazo máximo de 05 (cinco) dias úteis para assinar a ATA, sob pena de, não o fazendo, decair do direito à contratação e sujeitar-se às penalidades previstas no artigo 7º, da Lei 10.520/02.

Parágrafo Segundo - O prazo fixado no subitem anterior poderá ser prorrogado uma única vez e por igual período, desde que a solicitação respectiva seja apresentada ainda durante o transcurso do interstício inicial, bem como que ocorra motivo justo e aceito pela Defensoria Pública da União.

Parágrafo Terceiro - É facultado à Administração, quando o convocado não assinar o referido documento no prazo e condições estabelecidas, chamar as licitantes remanescentes, obedecida à ordem de classificação, para fazê-lo em igual prazo, nas condições de suas propostas, ou conforme negociação, podendo ainda, revogar a licitação independentemente da cominação prevista no art. 81 da Lei n. 8.666/93.

CLÁUSULA OITAVA - DO PAGAMENTO

A empresa deverá apresentar a nota fiscal à Unidade da Defensoria, para que esta realize a liquidação e encaminhe o pagamento da despesa para a Defensoria Pública-Geral da União em Brasília/DF, mediante ordem bancária creditada em conta corrente, no prazo de 10 (dez) dias úteis contados da apresentação dos documentos na Secretaria de Execução de Orçamento e Finanças - SEOF, situada no Setor de Autarquias Norte - SAUN, Quadra 05, Lote C, Bloco C, Centro Empresarial CNC - Bairro Asa Norte - CEP 70040-250 - Brasília – DF.

Parágrafo Primeiro - A Defensoria Pública-Geral da União reserva-se o direito de recusar o pagamento se no ato da atestação os produtos fornecidos não estiverem em perfeitas condições de consumo ou em desacordo com as especificações apresentadas e aceitas.

Parágrafo Segundo - A Defensoria Pública-Geral da União poderá deduzir da importância a pagar os valores correspondentes a multas ou indenizações devidas pela empresa, nos termos desta contratação.

Parágrafo Terceiro - O prazo de pagamento dos serviços será contado a partir da data da liquidação da Unidade.

Parágrafo Quarto - Para execução do pagamento, o contratado deverá fazer constar da Nota Fiscal/Fatura correspondente, emitida sem rasura, em letra legível, se o caso, em nome da DEFENSORIA PÚBLICA DA UNIÃO – DPU, CNPJ sob o nº **00.375.140/0001-16**, o número de sua conta bancária, o nome do Banco e a respectiva Agência.

Parágrafo Quinto - Caso o contratado seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

Parágrafo Sexto - Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, o documento fiscal será devolvido ao contratado e o pagamento ficará pendente até que tenham sido adotadas as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal não acarretando qualquer ônus a DPU.

Parágrafo Sétimo - O pagamento somente será efetuado se cumpridas, pelo contratado, todas as condições estabelecidas neste Edital, e também com a efetiva prestação dos serviços.

Parágrafo Oitavo - É vedada a emissão e/ou circulação de efeitos de créditos para representação do preço mensal bem assim a cessão total ou parcial dos direitos creditórios dele decorrentes. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa

de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes formulas:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) $I = \frac{(6/100)}{365}$ I = 0, 00016438
TX = Percentual da taxa anual = 6%

Parágrafo Nono - Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos, e ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa.

CLÁUSULA NONA - RESPONSABILIDADES DA EMPRESA REGISTRADA

I- Manter atualizados seus dados cadastrais na Defensoria Pública da União.

II- Credenciar devidamente o seu Preposto para representá-lo em todas as questões relativas a execução do que fora contratado, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa entre a Defensoria Pública da União e a Contratada, sem custo adicional;

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

IV- Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

V- Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

VI- Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

VII- Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

VIII- Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

IX- Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

X- Atender as solicitações da Contratante quanto à substituição dos empregados disponibilizados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito no Termo de Referência;

XI- Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos objetos do Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobranças extras.

XII- Comunicar a Contratante, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos de entrega, propondo as ações corretivas necessárias para a execução dos mesmos.

XIII- Cumprir fielmente as obrigações assumidas, observando as definições técnicas do Termo de Referência.

XIV- Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

XV- Reparar, corrigir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios defeitos ou incorreções que forem detectados durante a vigência do contrato, cuja responsabilidade lhe seja atribuível, exclusivamente.

XVI- Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

XVII- Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

XVIII- Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

XIX- Manter, durante a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da sua assinatura.

XX- Entregar os produtos e serviços dentro do prazo estipulado em sua proposta comercial.

CLÁUSULA DÉCIMA - RESPONSABILIDADES DA CONTRATANTE

I- Designar formalmente, na forma do art. 67 da Lei nº 8.666/93, combinada com o art. 24 da IN nº 4/2014, da SLTI/MP, representantes para gerenciar o contrato.

II-Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, ao qual caberá anotar em registro próprio as falhas detectadas e as medidas corretivas necessárias.

III- Encaminhar formalmente as demandas, por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência.

IV- Exercer a fiscalização da execução do contrato, por meio de servidor especialmente designado para este fim, independentemente do acompanhamento e controle exercido pela Contratada.

V-Examinar todos os produtos e serviços recebidos, antes de sua utilização, e decidir sobre a sua aceitação ou rejeição.

VI- Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com os termos do contrato assinado.

VII- Proporcionar todas as condições e prestar as informações necessárias para que a Contratada possa cumprir com suas obrigações, dentro das normas e condições contratuais.

VIII- Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo preposto da Contratada.

IX- Comunicar oficialmente à Contratada quaisquer falhas verificadas no cumprimento do contrato.

X- Acompanhar a execução dos serviços objeto do Termo de Referência.

XI- Notificar a contratada sobre imperfeições, falhas ou irregularidades constatadas nos serviços prestados, para que sejam adotadas as medidas corretivas necessárias.

XII- Glosar, em parte ou integral, o pagamento de serviços não aprovados pela fiscalização do contrato e aplicar as respectivas penalidades.

XIII- Efetuar o pagamento devido pelos serviços efetuados, desde que cumpridas todas as formalidades e exigências contratuais.

CLÁUSULA DÉCIMA PRIMEIRA - DOS ACRÉSCIMOS E SUPRESSÕES

As quantidades inicialmente contratadas não poderão ser acrescidas ou suprimidas, conforme estabelece o art. 12, §1º, do Decreto nº 7.892/2013.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, do Decreto nº 3.555, de 2000 e do Decreto nº 5.450, de 2005, a licitante/Adjudicatária/Fornecedor registrado, que:

I- Não assinar a ATA, quando convocada dentro do prazo de validade da proposta;
II- Apresentar documentação falsa;
III- Deixar de entregar os documentos exigidos no certame;
IV- Não mantiver a sua proposta dentro de prazo de validade;
V- Comportar-se de modo inidôneo;
VI- Cometer fraude fiscal;
VII- Fizer declaração falsa;
VIII- Ensejar o retardamento da execução do certame.

Parágrafo Primeiro - Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar à Contratada, observando a gravidade das faltas cometidas, as seguintes sanções:

I- Advertência;
II- Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;
III- Multa:
a. compensatória, no percentual de 10% (dez por cento), calculada sobre o valor total do contrato, pela recusa em assiná-lo, no prazo máximo de 5 (cinco) dias úteis, após regularmente convocada, sem prejuízo da aplicação de outras sanções;
b. compensatória, no percentual de 5% (cinco por cento) do valor da fatura correspondente ao mês em que foi constatada a falta;
c. moratória, no percentual correspondente a 0,5 (meio por cento), calculada sobre o valor total do contrato, por dia de inadimplência, até o limite máximo de 10% (dez por cento), ou seja, por 20 (vinte) dias, o que poderá ensejar a rescisão do contrato;
d. moratória, no percentual de 10% (dez por cento), calculada sobre o valor total da contratação, pela inadimplência além do prazo acima, o que poderá ensejar a rescisão do contrato.
IV- Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir à Administração pelos prejuízos resultantes, e após decorrido o prazo da sanção aplicada de suspensão temporária de participação em licitação e impedimento de contratar.
V- As sanções previstas nos itens I, II e IV, poderão ser aplicadas juntamente com as sanções previstas no item III, facultada a defesa prévia da Contratada, em processo próprio de penalidade.

VI- Sanção estabelecida no subitem IV, é de competência exclusiva do Ministro de Estado, facultada a defesa da Contratada, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

VII- No caso de aplicação das sanções estabelecidas nos subitens acima, assim são definidas as possíveis faltas cometidas pela Contratada:

a. Faltas leves: puníveis com a aplicação de penalidade de advertência e multas, caracterizando-se pela inexecução parcial de deveres de pequena monta, assim entendidas como aquelas que não acarretam prejuízos relevantes aos serviços da Administração e a despeito delas, a regular prestação dos serviços não fica inviabilizada;

b. Faltas graves: puníveis com a aplicação das penalidades de advertência e multas, caracterizando-se pela inexecução parcial ou total das obrigações que acarretam prejuízos aos serviços da Administração, inviabilizando total ou parcialmente a execução do contrato, notadamente em decorrência de conduta culposa da Contratada;

c. Faltas gravíssimas: puníveis com a aplicação das penalidades de multas e impedimento de licitar e contratar com a União, Distrito Federal, Estados e Municípios, pelo prazo de até 5 (cinco) anos, caracterizando-se pela inexecução parcial ou total das obrigações que acarretam prejuízos relevantes aos serviços da Administração, inviabilizando a execução do contrato em decorrência de conduta culposa ou dolosa da Contratada.

VIII- As multas deverão ser recolhidas no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada pela Defensoria Pública da União;

IX- O valor das multas poderá ser descontado da nota fiscal ou do crédito existente da Defensoria Pública da União em relação à Contratada.

Parágrafo Segundo - As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência administrativa, mediante ato da Administração, devidamente justificado.

Parágrafo Terceiro - As penalidades serão obrigatoriamente registradas no SICAF e no caso da aplicação da penalidade descrita no parágrafo primeiro, inciso III, a Contratada deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste subitem e das demais cominações legais.

Parágrafo Quarto - A sanção estabelecida no parágrafo primeiro, inciso III, é de competência exclusiva do Ministro de Estado, facultada a defesa da Contratada, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

Parágrafo Quinto - As multas deverão ser recolhidas no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada pela Defensoria Pública da União.

Parágrafo Sexto - O valor das multas poderá ser descontado da nota fiscal ou do crédito existente da Defensoria Pública da União em relação à Contratada.

Parágrafo Sétimo - As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência administrativa, mediante ato da Administração, devidamente justificado.

Parágrafo Oitavo - As penalidades serão obrigatoriamente registradas no SICAF e no caso da aplicação da penalidade descrita no parágrafo primeiro, inciso III, a Contratada deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste subitem e das demais cominações legais.

Parágrafo Nono – As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis.

Parágrafo Décimo – Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

I- Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II- Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

III- Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

Parágrafo Décimo Primeiro – A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Contratante, observado o princípio da proporcionalidade.

Parágrafo Décimo Segundo – A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimentbaito previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

CLÁUSULA DÉCIMA TERCEIRA - DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS.

O FORNECEDOR terá seu registro cancelado quando:

I - Descumprir as condições da Ata de Registro de Preços;

II - Não retirar a respectiva nota de empenho e Autorização de Material, no prazo estabelecido pelo CONTRATANTE, sem justificativa aceitável;

III - Não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

IV - Tiver presentes razões de interesse público.

Parágrafo Primeiro - O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do CONTRATANTE.

Parágrafo Segundo - O FORNECEDOR poderá solicitar o cancelamento do seu registro de preço na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior devidamente comprovados.

CLÁUSULA DÉCIMA QUARTA - DA DOTAÇÃO ORÇAMENTÁRIA

Os recursos orçamentários destinados ao pagamento das despesas consequentes do presente Edital decorrerão de dotação orçamentária prevista no Orçamento Geral da União para a Defensoria Pública da União, Exercício 2017, referente ao programa de trabalho e natureza da despesa a serem informados posteriormente pela Coordenação de Orçamento e Finanças.

CLÁUSULA DÉCIMA QUINTA - DA ADESÃO À ATA DE REGISTRO DE PREÇOS

Parágrafo Primeiro - Não será permitida adesão desta ata de registro de preços.

CLÁUSULA DÉCIMA SEXTA - DAS DISPOSIÇÕES FINAIS

Integram esta Ata de Registro de Preços, o Edital do Pregão Eletrônico nº XX/20XX, o Termo de Referência, bem como a proposta da empresa vencedora do certame.

Parágrafo Primeiro - Os casos omissos serão resolvidos com observância das disposições constantes na Lei n° 8.666, de 21.06.1993, no Decreto n° 7.892, de 23.01.2013, na Lei n° 10.520, de 17.07.2002, no Decreto n° 3.555, de 08.08.2000 e no Decreto n° 5.450, de 31.05.2005, com suas alterações.

Parágrafo Segundo - A publicação resumida desta Ata de Registro de Preços na imprensa oficial, condição indispensável para sua eficácia, será providenciada pela Contratante.

Parágrafo Terceiro - As questões decorrentes da utilização da presente ata, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no foro da cidade de Brasília – DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro.

E, por estarem assim, justas e contratadas, firmam o presente instrumento em 02 (duas) vias de igual teor e forma, na presença das testemunhas que também o subscrevem.

xxxxxxxxxxxxx	xxxxxxxxxxxxxxxx
Contratante	Fornecedor

TESTEMUNHAS:

Nome:	Nome:
CPF :	CPF :
R.G.:	

ANEXO III

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS DA HABILITAÇÃO

.....(nome da empresa) CNPJ/MF nº ....., sediada à ....., declara sob as penas da lei, que até a presente data inexistem fatos impeditivos de sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

.....(local e data).....

.....
(assinatura autorizada devidamente identificada)

ANEXO IV

MODELO DE DECLARAÇÃO DE TRABALHO DE MENOR

Ref.: Pregão XX/2017.

....., inscrito no CPJ n.º ....., por intermédio de seu representante legal o (a) Sr.(a) ....., portador de Identidade n.º .....e do CPF N.º ....., DECLARA para fins do disposto no inciso V do art. da Lei nº 8.666 de 21/06/1993, acrescido pela Lei n.º 9.854, de 27/10/1999, que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menores de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

Em caso afirmativo, assinalar a ressalva acima.

.....
(local e data)

.....
(representante legal)

ANEXO V

MODELO DE DECLARAÇÃO DE ENQUADRAMENTO NA LEI COMPLEMENTAR N°123, DE 14/12/2006

(em papel timbrado da empresa)

Ref.: (Pregão nº)

A empresa....., inscrita no CNPJ nº ....., por intermédio de seu representante legal, o(a) Sr(a) ....., portador(a) da Carteira de Identidade nº ..... e do CPF nº ....., **DECLARA**, sob as penas da lei, que atende os dispositivos da Lei Complementar nº 123, de 14 de Dezembro de 2006, notadamente o Art. 3º, para efeito do exercício do direito aos benefícios estendidos pelo referido diploma, sendo que a aferição poderá ser feita em momento posterior.

Ressalva: ( ) Microempresa ( ) Empresa de Pequeno Porte

Local e data.

_____

(Representante legal)

OBS: Esta declaração deverá ter firma reconhecida em Cartório e ser apresentada em documento original.

ANEXO VI

MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

(Identificação da Licitação)

(Identificação completa do representante da licitante), como representante devidamente constituído de (Identificação completa da licitante) doravante denominado (Licitante), para fins do disposto no item (completar) do Edital (completar com identificação do edital), declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta apresentada para participar do Pregão Eletrônico _____/2017 foi elaborada de maneira independente (pelo Licitante), e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato da (identificação da licitação), por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar do Pregão Eletrônico ___/2017 não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2017, por qualquer meio ou por qualquer pessoa;

(c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2017 quanto a participar ou não da referida licitação;

(d) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico ____/2017 não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2017 antes da adjudicação do objeto da referida licitação;

(e) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico ____/2017 não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante de (órgão licitante) antes da abertura oficial das propostas; e

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

_____, em ___ de _____ de _____

(representante legal do licitante/ consórcio, no âmbito da licitação, com identificação completa).

ANEXO VII

MODELO DE PROPOSTA COMERCIAL

O modelo de propostas de preços deverá estar de acordo com o constante no apêndice “C” do Termo de Referência, anexo I, desde Edital.

ANEXO VIII

MODELO DE DECLARAÇÃO DE CERTIFICAÇÃO DE TECNOLOGIA DESENVOLVIDA NO PAÍS E PROCESSO PRODUTIVO BÁSICO PARA USUFRUTO DOS BENEFÍCIOS PREVISTOS NO DECRETO Nº 7.174/2010

(identificação completa do representante da licitante), como representante devidamente constituído de (identificação completa da licitante), doravante denominado (licitante), para fins do disposto no item (completar) do edital (completar com identificação do edital), declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

( ) *Possui a Certificação de Tecnologia Desenvolvida no País****, nos termos da Lei 8.248, de 23 de outubro de 1991, do Decreto 5.906, de 26 de setembro de 2006, ou do Decreto 6.008, de 29 de dezembro de 2006,***

( ) *Possui a Certificação de Processo Produtivo Básico (PPB)****, nos termos da Lei 8.248, de 23 de outubro de 1991, do Decreto 5.906, de 26 de setembro de 2006, ou do Decreto 6.008, de 29 de dezembro de 2006.***

Ainda, afirma que está plenamente ciente do teor e da extensão desta Declaração e que detém plenos poderes e informações para firmá-la.

_____, em _____ de _____ de _____

assinatura

(representante legal do licitante, no âmbito da licitação, com identificação completa)

OBS.: Marcar com "X" apenas as certificações que possuir.

DEFENSORIA PÚBLICA DA UNIÃO

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

ANEXO IX

MINUTA DE CONTRATO

CONTRATO nº _____/2017 QUE ENTRE SI CELEBRAM A DEFENSORIA PÚBLICA DA UNIÃO E A EMPRESA_____PARA SOLUÇÕES DE SEGURANÇA INTEGRADAS E SOLUÇÕES DE INFORMÁTICA INTEGRADAS

A União por intermédio da DEFENSORIA PÚBLICA DA UNIÃO, inscrita no CNPJ sob o nº 00.375.114/0001-16, localizada no Setor de Autarquias Norte - SAUN, Quadra 05, Lote C, Bloco C, Centro Empresarial CNC - Bairro Asa Norte - CEP 70040-250 - Brasília - DF, doravante denominada CONTRATANTE, neste ato representada pelo _____, _____, brasileiro, inscrito no CPF sob o nº _____ e no RG sob o nº _____, residente e domiciliado em _____, nomeado pela Portaria nº _____, de ___ de _____ de 2015, publicada no Diário Oficial da União, em ____ de _____ de 2015, no uso das atribuições que lhe conferem a Portaria nº 84 de 14 de fevereiro de 2014, publicada no Diário Oficial da União de 18 de fevereiro de 2014, e de outro lado a empresa _____, inscrita no CNPJ sob n.º _____, com Sede _____, em _____, neste ato representada pelo(a) Senhor(a) _____, portador(a) da Carteira de Identidade n.º _____ SSP/_____, inscrito(a) no CPF sob o n.º _____, doravante denominada CONTRATADA, conforme processo número 08038.008252/2017-18 as partes celebram o presente contrato, sujeitando-se subsidiariamente as normas da Lei n° 8.666, de 21 de junho de 1993 e demais legislações correlatas, bem como às cláusulas a seguir.

CLÁSULA PRIMEIRA – DO OBJETO

Contratação de Soluções de Segurança integradas compreendendo: Fornecimento de licença de uso, sua respectiva manutenção e suporte técnico em ambiente corporativo da Solução de Segurança e Gerenciamento Seguro da Informação e Solução integrada Segurança Digital com conceito de blindagem do domínio web, incluindo a prestação de serviços técnicos especializados, operação, fornecimento da aquisição e manutenção, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Defensoria Pública da União – DPU, nas condições técnicas estabelecidas no Edital e seus Anexos.

CLÁUSULA SEGUNDA – DO VALOR DO CONTRATO

1. O valor estimado/global deste contrato para o período de sua vigência é de R$ _____(_____), correspondendo ao valor estimado mensal de R$ ____(____).

2. O valor empenhado para o exercício de 2017 é de R$ _____(_____).

CLÁUSULA TERCEIRA - DA DESPESA

1. A despesa neste exercício com a execução dos serviços de que trata o objeto, corre à conta do elemento orçamentário _____ – _____, da Atividade _____–.

2. A despesa para os exercícios subsequentes, quando for o caso, será alocada à dotação orçamentária prevista para atendimento dessa finalidade, a ser consignada à Defensoria Pública da União, pela Lei Orçamentária Anual.

CLÁUSULA QUARTA - DA VIGÊNCIA E DA EFICÁCIA

1. O prazo de vigência deste contrato é de **12 (doze) meses,** prorrogáveis, nos termos do inciso II do art. 57 da Lei n.º 8.666/93 e alterações posteriores, contado da data da sua assinatura, tendo eficácia legal após a sua assinatura, sendo o início e vencimento em dia de expediente, devendo-se excluir o primeiro e incluir o último.

2. A critério do Contratante e com anuência da Cotratada, este contrato pode ser prorrogado por iguais e sucessivos períodos, mediante termo aditivo, até o limite de 60 (sessenta meses).

3. A prorrogação do contrato será precedida da realização de pesquisas de preços de mercado ou de preços contratados por outros órgãos e entidades da Administração Pública, visando a assegurar a manutenção da contratação mais vantajosa para a Defensoria Pública da União.

4 A prorrogação de contrato, quando vantajosa para a Defensoria Pública da União, será promovida mediante celebração de termo aditivo, o qual deverá ser submetido à aprovação da consultoria jurídica do órgão contratante.

5. Nas prorrogações contratuais, os custos não renováveis já pagos ou amortizados no primeiro ano da contratação deverão ser eliminados como condição para a renovação;

CLÁUSULA QUINTA – DO INÍCIO DA PRESTAÇÃO DOS SERVIÇOS

1. O início da prestação dos serviços constantes neste Contrato será a data de sua assinatura.

CLÁUSULA SEXTA – DA GARANTIA

1. Como garantia da execução plena do objetivo e fiel cumprimento dos termos do Contrato, a empresa contratada prestará garantia no valor correspondente a 5% do valor global do Contrato, com validade de 03 (três) meses após o término da vigência contratual (totalizando 15 meses), devendo ser renovada a cada prorrogação efetivada no contrato, observados ainda os seguintes requisitos:

a) a contratada deverá apresentar, no prazo máximo de 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária;
b) a garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

   i. Prejuízos advindos do não cumprimento do objeto de contrato e do não adimplemento das demais obrigações nele previstas;
   ii. Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
   iii. Multas moratórias e punitivas aplicadas pela Administração à contratada; e
   iv. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela contratada;

c) a modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nos itens da alínea “b”;
d) a garantia em dinheiro deverá ser efetuada em conta específica com correção monetária, em favor do contratante;
e) a inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);
f) o atraso superior a 25 (vinte cinco) dias autoriza a Defensoria Pública da União a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;
g) o garantidor não é parte interessada para figurar em processo administrativo instaurado pelo contratado com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;
h) a garantia será considerada extinta;

   i. Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração de representante da Defensoria Pública da União, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e
   ii. Após o término da vigência do contrato, devendo o instrumento convocatório estabelecer o prazo de extinção da garantia, que poderá ser estendido em caso de ocorrência de sinistro;

i) A Defensoria Pública da União não executará a garantia nas seguintes hipóteses:

   i. Caso fortuito ou força maior;
   ii. Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;
   iii. Descumprimento das obrigações pela contratada decorrente de atos ou fatos da Administração ou;
   iv. Prática de atos ilícitos dolosos por seus servidores;
j) Não serão admitidas outras hipóteses de não execução da garantia, que não as previstas na alínea “o”;

CLÁUSULA SÉTIMA - DOS ENCARGOS DO CONTRATANTE

1. Coordenar e monitorar as ações pertinentes ao desenvolvimento das atividades executadas pela empresa Contratada;

2. Definir mecanismos de gerenciamento e controle das atividades desenvolvidas pela contratada, assim como avaliar a execução mensal das atividades em andamento e a serem desenvolvidas, relativas aos serviços contratados;

3. A Contratante disponibilizará o espaço no CPD e refrigeração suficiente para comportar os equipamentos novos a serem adquiridos, assim como, a infraestrutura elétrica até o quadro de energia com capacidades (corrente e tensão) suficientes de suportar todos os equipamentos novos, durante todo o período de instalação e/ou migração conforme item 20.3 do Termo de Referência.

4. Comunicar à empresa contratada a necessidade de substituição de qualquer profissional que seja considerado inadequado para o exercício da função;

5. Efetuar o pagamento mensal devido pela execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;

6. Permitir acesso dos profissionais da contratada às dependências, equipamentos, softwares e sistemas de informação da DPU, conforme necessário para execução dos serviços;

7. Prestar as informações e os esclarecimentos pertinentes solicitados pelos profissionais da contratada ou por preposto dessa;

8. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;

9. Avaliar e homologar relatório mensal dos serviços executados pela contratada observando as metas de nível de serviço alcançadas;

10. Disponibilizar cópia da norma de segurança da informação e das demais normas pertinentes à execução dos serviços.

CLÁUSULA OITAVA - DOS ENCARGOS DA CONTRATADA

1.Manter atualizados seus dados cadastrais na Defensoria Pública da União.

2.Credenciar devidamente o seu Preposto para representá-lo em todas as questões relativas a execução do que fora contratado, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa entre a Defensoria Pública da União e a Contratada, sem custo adicional.

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

4.Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

5.Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

6. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;
7. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;
8. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
9. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
10. Atender as solicitações da Contratante quanto à substituição dos empregados disponibilizados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;
11. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos objetos deste Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobranças extras.
12. Comunicar a Contratante, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos de entrega, propondo as ações corretivas necessárias para a execução dos mesmos.
13. Cumprir fielmente as obrigações assumidas, observando as definições técnicas deste Termo de Referência.
14. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.
15. Reparar, corrigir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios defeitos ou incorreções que forem detectados durante a vigência do contrato, cuja responsabilidade lhe seja atribuível, exclusivamente.
16. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;
17. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;
18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.
19. Manter, durante a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da sua assinatura.
20. Entregar os produtos e serviços dentro do prazo estipulado em sua proposta comercial.

CLÁUSULA NONA – OUTRAS CONDIÇÕES CONTRATUAIS

1. A contratada e os profissionais alocados na execução dos serviços transferem para a DPU, de forma incondicional, todos os direitos referentes à propriedade intelectual sobre procedimentos, roteiros de atendimento e demais documentos produzidos no âmbito do contrato

2. A DPU poderá, excepcionalmente, solicitar a execução dos serviços em dias, horários e locais distintos dos estabelecidos nas especificações técnicas, mediante alteração temporária das escalas

de trabalho de um ou mais membros das equipes, devendo essa necessidade ser comunicada previamente à contratada

3. É vedada a contratação, pela empresa prestadora de serviço, para atuar no âmbito do presente contrato, de servidor ativo ou aposentado do quadro da DPU ou ocupante de cargo em comissão, assim como de cônjuge ou companheiro(a)

4. É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da Administração da DPU

5. Quando do encerramento do contrato, a contratada deverá repassar aos profissionais indicados pela DPU os documentos, procedimentos e demais conhecimentos necessários para continuidade dos serviços de suporte aos usuários de soluções de TIC

6. A CONTRATANTE poderá, excepcionalmente, solicitar o deslocamento de um profissional de uma unidade para outra unidade mais próxima, para a execução dos serviços, objeto desta contratação, sem prejuízo da execução dos serviços da unidade que este profissional está alocado e onde as despesas extraordinárias de diárias e passagens ficará a cargo da CONTRATADA.

CLÁUSULA DÉCIMA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

1. O acompanhamento e fiscalização da execução do contrato que consistirá na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato, será exercido por servidor da Defensoria Pública-Geral da União, especialmente designado na forma do art. 67 da Lei nº 8.666/93 e do art. 6º do Decreto nº 2.271/97.

2. Além das disposições previstas no item anterior, a fiscalização dos serviços deverá seguir o disposto do Art. 34 da IN/MPOG 04/2014.

3. A fiscalização poderá recusar os serviços quando entender que os mesmos não sejam os especificados, ou quando entender que o serviço esteja irregular.

3.1. A fiscalização do recolhimento dos encargos previdenciários e trabalhistas dar-se-á, também, mediante consulta direta aos órgãos competentes sobre a situação de empregados da contratada, aleatoriamente definidos.

4. A Contratada poderá, também, ser instada a apresentar as respectivas comprovações de recolhimento, fazendo-o imediatamente após a exigência formal da Contratante.

4.1. Na ocorrência de omissões ou lacunas nos recolhimentos de que trata este item, a Contratada terá o prazo de 48 (quarenta e oito) horas para comprovar-se adimplente em relação a todos os empregados, bem como para sanar a irregularidade detectada, sem prejuízo de eventuais sanções e penalidades previstas no Edital e no Contrato.

5. A Contratada fica obrigada a executar os serviços referentes ao objeto licitado relacionado neste Edital, não se admitindo quaisquer modificações sem a prévia autorização da fiscalização.

6. Durante a vigência dos contratos, a execução dos serviços será fiscalizada por representante da Defensoria Pública da União, designado pelo Defensor Público-Geral da União.

7. Caberá ao gestor do contrato o recebimento da nota fiscal/fatura apresentada pela contratada e a devida atestação dos serviços, para fins de liquidação e pagamento.

8. Durante a vigência do contrato, a prestação dos serviços será acompanhada e fiscalizada por servidor público designado para esse fim. As decisões e providências que ultrapassarem a competência do servidor designado deverão ser solicitadas a seus superiores em tempo hábil para a adoção das medidas convenientes.

CLÁUSULA DÉCIMA PRIMEIRA – DA LIQUIDAÇÃO E DO PAGAMENTO

1. DA LIQUIDAÇÃO E DO PAGAMENTO

2. Será indicado o crédito e respectivo empenho para atender à despesa no exercício em curso, bem como, de cada parcela da despesa relativa à parte a ser executada em exercício futuro, com a declaração de que, em termos aditivos ou apostilamentos, indicar-se-ão os créditos e empenhos para sua cobertura.

3. Liquidação:

3.1. Executados os serviços, a CONTRATADA deve apresentar, mensalmente, para liquidação e pagamento da despesa nota fiscal/fatura discriminada, em 2 (duas) vias, acompanhada dos documentos comprobatórios do cumprimento das obrigações decorrentes deste contrato;

3.1.1. A comprovação de que trata este item é demonstrada mediante apresentação de documentos oficiais, individualizados e identificados por contrato, correspondentes ao mês do adimplemento da obrigação ou do mês anterior, quando não vencidas as referidas obrigações;

3.2. A Nota Fiscal/Fatura deverá ser encaminhada à Defensoria Pública da União no Estado, onde serão prestados os serviços, até o 2º (segundo) dia útil do mês subsequente à prestação dos serviços e ser obrigatoriamente acompanhada das seguintes comprovações:

3.2.1. Do pagamento da remuneração e das contribuições sociais (Fundo de Garantia do Tempo de Serviço e Previdência Social), correspondentes ao mês da última Nota Fiscal/Fatura vencida, compatível com os empregados vinculados à execução contratual, nominalmente identificados, na forma do § 4ºdo Artigo 31 da Lei n.º 9.032, de 28 de abril de 1995;

3.2.2. Da regularidade fiscal, constatada através de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no Artigo 29 da Lei 8.666/93;

3.2.3. Do cumprimento das obrigações trabalhistas, correspondentes à última Nota Fiscal/Fatura que tenha sido paga pela Administração; e

3.2.4. Da apresentação da cópia do relatório mensal emitido pelo fiscal do contrato/DPU, consubstanciado no Acordo de Níveis de Serviço, devidamente assinado pelo representante da empresa contratada.

3.3. O CONTRATANTE somente efetuará o pagamento após atestado de que o serviço foi executado em conformidade com as especificações deste contrato e comprovado o pagamento de salários e benefícios dos empregados alocados pela CONTRATADA e dos respectivos encargos;

3.4. Para efeito de cada pagamento mensal a CONTRATADA deverá apresentar, obrigatoriamente, junto com as notas fiscais/faturas:

3.4.1. Guia do Recolhimento do INSS do mês anterior ao serviço que se refere a fatura;

3.4.2. Guia de recolhimento do FGTS do mês anterior ao serviço que se refere a fatura;

3.4.3. GFIP correspondente as guias de recolhimento do INSS e FGTS, relativas ao mês anterior ao do faturamento, discriminando o nome de cada um dos empregados beneficiados, por tomador de serviço da defensoria Pública-Geral da União;

3.4.4. Certidão Negativa de Débito da Previdência Social – CND;

3.4.5. Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União;

3.4.6. Certidão Negativa de Débitos das Fazendas Federal, Estadual e Municipal de seu domicílio ou sede;

3.4.7. Certidão de Regularidade do FGTS – CRF.

3.5. O CONTRATANTE pode deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela CONTRATADA, nos termos deste contrato.

3.6. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente qualquer obrigação documental ou financeira, inclusive a entrega da garantia contratual a que se refere à cláusula sexta, sem que isso gere direito a reajustamento de preços ou atualização monetária.

4. Pagamento:

4.1. O pagamento será efetuado em função dos resultados obtidos pela CONTRATADA, consoante ao previsto nos Acórdãos nº 1.382/2009 – Plenário e nº 2.220/2008 – Plenário, do Tribunal de Contas da União, e na Instrução Normativa nº 04/2014-SLTI/MPOG;

4.2. O pagamento será efetuado mensalmente, devendo o valor global ser dividido em 12 (doze) parcelas iguais e após o atesto do Fiscal do Contrato na Nota Fiscal/Fatura, relativo aos serviços baseadas em UST (Unidade de Serviço Técnico) efetivamente executados no período e mediante a apresentação da Nota Fiscal/Fatura e Relatório Mensal dos Serviços Executados. A Contratada deverá estar em situação regular no SICAF. Este deverá ser efetuado até 15 dias da apresentação da Nota Fiscal/ Fatura e Relatório Mensal;

4.3. O pagamento balizar-se-á pela avaliação da qualidade do fornecimento e pelo “Nível Mínimo de Serviço Exigido;

4.4. O faturamento será mensal, mediante apresentação de pré-fatura, já descontadas as glosas aplicadas em função do não atendimento aos resultados esperados e níveis de qualidade definidos nas Tarefas;

4.5. As glosas deverão ser aplicadas quando os serviços/produtos não atenderem aos níveis de qualidade e resultados esperados;

4.6. Em quaisquer casos de aplicação de glosas, deverão ser anexados os documentos e relatórios comprobatórios do não atendimento aos resultados esperados ou níveis de qualidade exigidos.

4.7. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo CONTRATANTE, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, a ser incluído na fatura/nota fiscal do mês seguinte ao da ocorrência.

4.8. Estes encargos moratórios são calculados por meio da aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

Na qual:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}00016438,$$

no qual i = taxa percentual anual no valor de 6%.

4.9. A CONTRATADA deverá manter atualizada as vigências da garantia contratual durante toda a execução do contrato e até a comprovação de todos os pagamentos (trabalhistas, previdência social, fiscais, etc.) devidos pela empresa, prevendo-se, para tanto, pelo menos mais um mês de garantia após término do contrato.

4.10. Caso seja detectada qualquer irregularidade atinente ao pagamento a menor de salários e outras vantagens previstas em contrato, bem como de encargos previdenciários e de FGTS, a CONTRATADA autoriza a retenção na fatura dos valores equivalentes;

CLÁUSULA DÉCIMA SEGUNDA - DA ALTERAÇÃO DO CONTRATO

1. As quantidades inicialmente contratadas não poderão ser acrescidas ou suprimidas, conforme estabelece o art. 12, §1º, do Decreto nº 7.892/2013.

CLÁUSULA DÉCIMA TERCEIRA - DA REPACTUAÇÃO DO CONTRATO

1. A repactuação de preços, como espécie de reajuste contratual, deverá ser utilizada nas contratações de serviços continuados com dedicação exclusiva de mão de obra, desde que seja observado o interregno mínimo de um ano das datas dos orçamentos aos quais as propostas se referir, ou da data da última e repactuação, conforme estabelece o art. 5º do Decreto nº 2.271, de 1997.

2. A repactuação para fazer face à elevação dos custos da contratação, respeitada a anualidade disposta no caput, e que vier a ocorrer durante a vigência do contrato, é direito do contratado, e não poderá alterar o equilíbrio econômico e financeiro dos contratos, conforme estabelece o art. 37, inciso XXI da Constituição da República Federativa do Brasil, sendo assegurado ao prestador receber pagamento mantidas as condições efetivas da proposta.

3. A repactuação poderá ser dividida em tantas parcelas quanto forem necessárias em respeito ao princípio da anualidade do reajuste dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço.

4. A repactuação para reajuste do contrato em razão de novo acordo, dissídio ou convenção coletiva deve repassar integralmente o aumento de custos da mão de obra decorrente desses instrumentos.

5. O interregno mínimo de 1 (um) ano para a primeira repactuação será contado a partir da data do acordo, convenção ou dissídio coletivo de trabalho ou equivalente, vigente à época da apresentação da proposta, quando a variação dos custos for decorrente da mão-de-obra e estiver vinculada às datas-base destes instrumentos.

6. Nas repactuações subsequentes à primeira, a anualidade será contada a partir da data do fato gerador que deu ensejo à última repactuação.

7. As repactuações serão precedidas de solicitação da contratada, acompanhada de demonstração analítica da alteração dos custos, por meio de apresentação da planilha de custos e formação de preços ou do novo acordo convenção ou dissídio coletivo que fundamenta a repactuação, conforme for à variação de custos objeto da repactuação.

8. É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa, acordo coletivo ou convenção coletiva.

9. Quando da solicitação da repactuação, para fazer jus à variação de custos decorrente do mercado, esta somente será concedida mediante a comprovação pelo contratado do aumento dos custos, considerando-se:

I - Os preços praticados no mercado ou em outros contratos da Administração;

II - As particularidades do contrato em vigência;

III - A nova planilha com a variação dos custos apresentada;

IV-Indicadores setoriais, tabelas de fabricantes, valores oficiais de referência, tarifas públicas ou outros equivalentes; e

V - A disponibilidade orçamentária do órgão ou entidade contratante.

10. A decisão sobre o pedido de repactuação deve ser feita no prazo máximo de sessenta dias, contados a partir da solicitação e da entrega dos comprovantes de variação dos custos.

11. As repactuações, como espécie de reajuste, serão formalizadas por meio de apostilamento, e não poderão alterar o equilíbrio econômico e financeiro dos contratos, exceto quando coincidirem com a prorrogação contratual, em que deverão ser formalizadas por aditamento.

12. O prazo referido no subitem 10 ficará suspenso enquanto a contratada não cumprir os atos ou apresentar a documentação solicitada pela contratante para a comprovação da variação dos custos;

13. As repactuações a que o contratado fazer jus e não forem solicitadas durante a vigência do contrato serão objeto de preclusão na data da assinatura da prorrogação contratual ou com o encerramento do contrato.

14. Os novos valores contratuais decorrentes das repactuações terão suas vigências iniciadas observando-se o seguinte:

I - a partir da ocorrência do fato gerador que deu causa à repactuação;

II - em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão das próximas repactuações futuras; ou

III - em data anterior à ocorrência do fato gerador, exclusivamente quando a repactuação envolver revisão do custo de mão-de-obra em que o próprio fato gerador, na forma de acordo, convenção ou sentença normativa, contemplar data de vigência retroativa, podendo esta ser considerada para efeito de compensação do pagamento devido, assim como para a contagem da anualidade em repactuações futuras;

IV - Os efeitos financeiros da repactuação deverão ocorrer exclusivamente para os itens que a motivaram, e apenas em relação à diferença porventura existente.

15. A As repactuações não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 65 da Lei nº 8.666, de 1993.

16. A empresa contratada para a execução de remanescente de serviço tem direito a repactuação nas mesmas condições e prazos a que fazia jus a empresa anteriormente contratada, devendo os seus preços serem corrigidos antes do início da contratação, conforme determina o art. 24, inciso XI da Lei nº 8.666, de 1993.

CLÁUSULA DÉCIMA QUARTA - DAS SANÇÕES

1. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar à Contratada, observando a gravidade das faltas cometidas, as seguintes sanções:

I. Advertência;

II. Multa:

a. compensatória, no percentual de 10% (dez por cento), calculada sobre o valor total do contrato, pela recusa em assiná-lo, no prazo máximo de 5 (cinco) dias úteis, após regularmente convocada, sem prejuízo da aplicação de outras sanções;

b. compensatória, no percentual de 5% (cinco por cento) do valor da fatura correspondente ao mês em que foi constatada a falta;

c. moratória, no percentual correspondente a 0,5 (meio por cento), calculada sobre o valor total do contrato, por dia de inadimplência, até o limite máximo de 10% (dez por cento), ou seja, por 20 (vinte) dias, o que poderá ensejar a rescisão do contrato;

d. moratória, no percentual de 10% (dez por cento), calculada sobre o valor total da contratação, pela inadimplência além do prazo acima, o que poderá ensejar a rescisão do contrato.

III. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir à Administração pelos prejuízos resultantes, e após decorrido o prazo da sanção aplicada de suspensão temporária de participação em licitação e impedimento de contratar.

IV. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração.

V. As sanções previstas no subitem 1.I, poderão ser aplicadas juntamente com as sanções previstas no subitem 1.II, facultada a defesa prévia da Contratada, em processo próprio de penalidade.

VI. A sanção estabelecida no subitem 1.III é de competência exclusiva do Ministro de Estado, facultada a defesa da Contratada, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

VII. No caso de aplicação das sanções estabelecidas nos subitens acima, assim são definidas as possíveis faltas cometidas pela Contratada:

a. Faltas leves: puníveis com a aplicação de penalidade de advertência e multas, caracterizando-se pela inexecução parcial de deveres de pequena

monta, assim entendidas como aquelas que não acarretam prejuízos relevantes aos serviços da Administração e a despeito delas, a regular prestação dos serviços não fica inviabilizada;

b. Faltas graves: puníveis com a aplicação das penalidades de advertência e multas, caracterizando-se pela inexecução parcial ou total das obrigações que acarretam prejuízos aos serviços da Administração, inviabilizando total ou parcialmente a execução do contrato, notadamente em decorrência de conduta culposa da Contratada;

c. Faltas gravíssimas: puníveis com a aplicação das penalidades de multas e impedimento de licitar e contratar com a União, Distrito Federal, Estados e Municípios, pelo prazo de até 5 (cinco) anos, caracterizando-se pela inexecução parcial ou total das obrigações que acarretam prejuízos relevantes aos serviços da Administração, inviabilizando a execução do contrato em decorrência de conduta culposa ou dolosa da Contratada.

VIII. As multas deverão ser recolhidas no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada pela Defensoria Pública da União.

IX. O valor das multas poderá ser descontado da nota fiscal ou do crédito existente da Defensoria Pública da União em relação à Contratada.

2. As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência administrativa, mediante ato da Administração, devidamente justificado.

3. As penalidades serão obrigatoriamente registradas no SICAF e no caso da aplicação da penalidade descrita no subitem 1.III, a Contratada deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste subitem e das demais cominações legais.

4. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis.

5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

a. Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
b. Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;
c. Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Contratante, observado o princípio da proporcionalidade.

7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

CLÁUSULA DÉCIMA QUINTA - DA RESCISÃO

1. A inexecução total ou parcial deste contrato enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei n.º 8.666/93.

2. A rescisão deste contrato poderá ser:

2.1. determinada por ato unilateral e escrito do CONTRATANTE, nos casos enumerados nos incisos I a XII e XVII do artigo 78 da Lei mencionada, notificando-se a CONTRATADA com a antecedência mínima de 30 (trinta) dias, exceto quanto ao inciso XVII;

2.2. amigável, por acordo entre as partes, reduzida a termo no processo de licitação, desde que haja conveniência para o CONTRATANTE;

2.3. judicial, nos termos da legislação vigente sobre a matéria.

3. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

3.1. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

4. Configurará falta grave, compreendida como falha na execução do contrato, o não recolhimento do FGTS dos empregados e das contribuições sociais previdenciárias, bem como o não pagamento do salário, do vale-transporte e do auxílio alimentação, que poderá dar ensejo à rescisão do contrato, sem prejuízo da aplicação de sanção pecuniária e da declaração de impedimento para licitar e contratar com a União, nos termos do art 7º da Lei. 10.520 de 17 de julho de 2002.

CLÁUSULA DÉCIMA SEXTA - DO FORO

1. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro, por mais privilegiado que seja, salvo nos casos previstos no art. 102, inciso I, alínea "d", da Constituição Federal.

E, para firmeza e validade do que foi pactuado, lavrou-se o presente Contrato em 3 (três) vias de igual teor e forma, para que surtam um só efeito, as quais, depois de lidas, são assinadas pelos representantes da parte, CONTRATANTE e CONTRATADA, e pelas testemunhas abaixo.

Brasília - DF, em / /2017.

_____	_____
CONTRATANTE	**CONTRATADA**

TESTEMUNHAS:

NOME: _____	**NOME: _____**
CPF: _____	**CPF: _____**
C.I.: _____	**C.I.: _____**

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

ANEXO X

PLANILHA DE PREÇOS MÉDIOS

DEFENSORIA PÚBLICA DA UNIÃO

DEFENSORIA PÚBLICA-GERAL DA UNIÃO

Secretaria de Logística e Patrimônio

DEFENSORIA PÚBLICA DA UNIÃO	MAPA COMPARATIVO - Aquisição																	
OBJETO			EMPRESA 1		EMPRESA 2		EMPRESA 3		EMPRESA 4		EMPRESA 5		MÉDIA DE PREÇO UNITÁRIO	MÉDIA DE PREÇO TOTAL
ITEM	OBJETO	QUANT.	VALOR UNITÁRIO	VALOR TOTAL	VALOR UNITÁRIO	VALOR TOTAL	VALOR UNITÁRIO	VALOR TOTAL	VALOR UNITÁRIO	VALOR TOTAL	VALOR UNITÁRIO	VALOR TOTAL		
1	Solução de Proteção de estação de trabalho, Servidores e mensageria	2.000	R$ 180,68	R$ 361.360,00	R$ 162,77	R$ 325.540,00	R$ 187,19	R$ 374.380,00	R$ 154,63	R$ 309.260,00	R$ 170,91	R$ 341.820,00	R$ 171,24	R$ 342.472,00
2	Manutenção Evolutiva e Atualização da Solução de Prteção de Estação de Trabalh, Servidores e Mensageria, pelo período de 12(doze) meses.	2.000	R$ 97,29	R$ 194.580,00	R$ 87,65	R$ 175.300,00	R$ 100,79	R$ 201.580,00	R$ 83,26	R$ 166.520,00	R$ 92,03	R$ 184.060,00	R$ 92,20	R$ 184.408,00
3	Gateway de Segurança WEB.	2.000	R$ 85,67	R$ 171.340,00	R$ 77,18	R$ 154.360,00	R$ 88,76	R$ 177.520,00	R$ 73,32	R$ 146.640,00	R$ 81,04	R$ 162.080,00	R$ 81,19	R$ 162.388,00
4	Manutenção evolutiva e atualização do Gateway de segurança WEB, pelo periodo de 12 meses.	2.000	R$ 46,13	R$ 92.260,00	R$ 41,56	R$ 83.120,00	R$ 7,79	R$ 15.580,00	R$ 39,48	R$ 78.960,00	R$ 43,64	R$ 87.280,00	R$ 35,72	R$ 71.440,00
5	Proteção de Dados em Serviços Críticos.	300	R$ 3.038,07	R$ 911.421,00	R$ 2.737,00	R$ 821.100,00	R$ 3.147,55	R$ 944.265,00	R$ 2.600,15	R$ 780.045,00	R$ 2.873,85	R$ 862.155,00	R$ 2.879,32	R$ 863.797,20
6	Manutenção Evolutiva e Etualização da Proteção de Dados em Serviços Críticos, pelo periodo de 12 (doze) meses.	300	R$ 1.635,88	R$ 490.764,00	R$ 1.473,77	R$ 442.131,00	R$ 1.694,00	R$ 508.200,00	R$ 1.400,08	R$ 420.024,00	R$ 1.547,46	R$ 464.238,00	R$ 1.550,24	R$ 465.071,40
7	Solução de Criptografia.	700	R$ 531,78	R$ 372.246,00	R$ 479,08	R$ 335.356,00	R$ 550,94	R$ 385.658,00	R$ 445,12	R$ 311.584,00	R$ 503,03	R$ 352.121,00	R$ 501,99	R$ 351.393,00
8	Manutenção Evolutiva e Atualização da Solução de criptografia pelo periodo de 12 (doze) meses.	700	R$ 286,34	R$ 200.438,00	R$ 257,97	R$ 180.579,00	R$ 296,66	R$ 207.662,00	R$ 245,07	R$ 171.549,00	R$ 270,86	R$ 189.602,00	R$ 271,38	R$ 189.966,00
9	Solução para a prevenção de Ataques Direcionados.	2.000	R$ 521,34	R$ 1.042.680,00	R$ 469,68	R$ 939.360,00	R$ 540,13	R$ 1.080.260,00	R$ 446,19	R$ 892.380,00	R$ 493,16	R$ 986.320,00	R$ 494,10	R$ 988.200,00
10	Manutenção evolutiva e Atualização da Solução para a Prevenção de Ataques Direcionados, pelo período de 12 (doze) Meses.	2.000	R$ 280,72	R$ 561.440,00	R$ 252,90	R$ 505.800,00	R$ 290,84	R$ 581.680,00	R$ 240,26	R$ 480.520,00	R$ 265,55	R$ 531.100,00	R$ 266,05	R$ 532.108,00
11	Solção Suite de identificação Forte de Dispositivos.	1	R$ 987.681,10	R$ 987.681,10	R$ 889.802,80	R$ 889.802,80	R$ 1.023.273,22	R$ 1.023.273,22	R$ 845.312,66	R$ 845.312,66	R$ 934.292,94	R$ 934.292,94	R$ 936.072,54	R$ 936.072,54
12	Manutenção Evolutivae Atualização da Solução Suite de Identificação Fortede Dispositivos, peloperíodo de 12 (doze) meses.	1	R$ 197.536,22	R$ 197.536,22	R$ 177.960,56	R$ 177.960,56	R$ 204.654,64	R$ 204.654,64	R$ 169.062,53	R$ 169.062,53	R$ 186.858,59	R$ 186.858,59	R$ 187.214,51	R$ 187.214,51
13	Solução de Segurança da Informação e Monitoramneto do Acesso a Aplicaçoes Web com Recursos Avançados de Combate a Fraudes.	1	R$ 2.170.727,70	R$ 2.170.727,70	R$ 1.955.610,54	R$ 1.955.610,54	R$ 2.248.952,12	R$ 2.248.952,12	R$ 1.857.830,01	R$ 1.857.830,01	R$ 2.053.391,07	R$ 2.053.391,07	R$ 2.057.302,29	R$ 2.057.302,29
14	Manutenção evolutiva e atualização da Solução de Segurança da Informação e Monitoramento do Acesso a Aplicaçoes Web com Recursos Avançados de Combate a Fraudes, pelo período de 12 (doze) meses.	1	R$ 434.145,54	R$ 434.145,54	R$ 391.122,11	R$ 391.122,11	R$ 449.790,42	R$ 449.790,42	R$ 371.566,00	R$ 371.566,00	R$ 410.678,21	R$ 410.678,21	R$ 411.460,46	R$ 411.460,46
15	Unidade de Serviço Tecnico (Operação Assistida).	2.554	R$ 335,66	R$ 857.275,64	R$ 599,00	R$ 1.529.846,00	R$ 347,76	R$ 888.179,04	R$ 287,28	R$ 733.713,12	R$ 317,52	R$ 810.946,08	R$ 377,44	R$ 963.991,98
TOTAL:				R$ 9.045.895,20		R$ 8.906.988,01		R$ 9.291.634,44		R$ 7.734.966,32		R$ 8.556.942,89	R$ 3.598.770,68	R$ 8.707.285,37