COTAÇÃO DE PREÇO

Brasília/DF, 6 de março de 2020.

Senhor Fornecedor,

Solicitamos a gentileza de nos apresentar proposta de preço para a aquisição(ões) do(s) material(is) e/ou serviço(s) especificado(s) abaixo, **até o dia 27/3/2020.**

ITEM	ESPECIFICAÇÃO	UN	QUANT.
1.	Solução de Segurança Cibernética, conforme especificação abaixo.	UN	1

I) A PROPOSTA DEVERÁ CONTER

1. Dados da empresa (CNPJ, Razão Social, endereço e contato);
2. Especificação detalhada do produto/serviço;
3. Garantia do material, quando o caso;
4. Valor unitário, valor total e unidade de medida (valores em reais);
5. Incluir no valor dos itens, impostos e demais taxas;
6. Prazo para entrega em dias úteis ou corridos;
7. Validade da proposta (pelo menos 30 dias úteis);
8. Data da proposta atualizada;
9. **Forma de pagamento (até 10 dias úteis após a entrega do material e aceite da N.F., por meio de transferência bancária ou boleto bancário);**
10. Dados bancários (conta jurídica - vinculada ao CNPJ); e
11. Assinatura do responsável.

II) NORMAS ESPECÍFICAS

1. Incluso no valor dos materiais/serviços todos os custos diretos e indiretos para perfeita execução dos trabalhos, inclusive as despesas com materiais, mão de obra, transportes, custos financeiros, encargos e impostos necessários.
2. A proposta poderá ser enviada por e-mail para: gecoc.eqcbe@poupex.com.br
3. A Entrega/execução deverá ser feita no End.: **Avenida Duque de Caxias S/N, Parte "A", Setor Militar Urbano. CEP: 70630-902. Brasília-DF - ALMOXARIFADO**

III) DADOS PARA ENVIO DA PROPOSTA

Associação de Poupança e Empréstimo – POUPEX.
CNPJ: 00.655.522/0001-21.
End.: Avenida Duque de Caxias s/n°, Parte "A", Setor Militar Urbano. CEP: 70630-902. Brasília-DF.
Divisão de Compras e Licitações – Equipe de Compras de Bens – DICOL/EQCBE.
FONE: (61) 3314-7880/ FAX: (61) 3314-7620.

1 – OBJETO DA CONTRATAÇÃO

Solução de Segurança Cibernética para proteção dos ativos informacionais da POUPEX e conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD e legislações vigentes.

2 – JUSTIFICAVA DA CONTRATAÇÃO

A evolução tecnológica é constante e torna-se um grande desafio para a POUPEX acompanhar e evoluir de maneira a utilizar os melhores métodos e ferramentas existentes, proporcionando, assim, um aumento da sua eficiência, eficácia e efetividade.

Dessa forma é primordial que a POUPEX atualize a solução tecnológica que realiza o controle de acesso externo aos sites disponibilizados. Cabe ressaltar a Lei Geral de Proteção de Dados (LGPD), Nº 13.709, de 14 de agosto de 2018, que tem por objetivo a proteção dos direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural. A lei entrará em vigor em agosto de 2020, possibilitando às empresas e organizações um período pequeno para adaptação. Nesta direção, a proteção dos ativos de informação requer a definição de investimentos para um melhor posicionamento das instituições em relação à produção, custódia e transporte de dados, principalmente no que diz respeito às informações pessoais dos cidadãos brasileiros. Assim posto, os ativos de informação guardam relação direta com riscos de Segurança da Informação e de Segurança Cibernética, uma vez que a dependência tecnológica das instituições é cada vez maior. As soluções de segurança devem atuar nas fases de detecção, prevenção e resposta aos ataques para demonstrar o esforço e investimento na proteção dos dados sensíveis de usuários e assim, cumprir os requisitos da LGPD.

As novas ameaças cibernéticas exploram diversas técnicas de invasão e persistência, aproveitando-se do fato de que as atuais ferramentas de segurança agem, na maioria das vezes, apenas de forma pontual na infraestrutura. Além disso, lançam mão da criptografia de modo a permanecer invisíveis e são distribuídas por diversos veículos, sendo web e e-mail os mais notáveis, por exemplo, e podem se manter ocultas até receberem instruções para se montarem, proliferarem e iniciar o ataque. As ferramentas clássicas de Segurança, tais como antivírus, firewall e antispam, atuando isoladamente em cada meio de comunicação, não são capazes de identificar os artefatos e as fases do ataque e, normalmente, não fazem um trabalho coordenado de modo a prover inteligência contra as ameaças. Como consequência, a capacidade de responder ao incidente é reduzida, podendo chegar a dias, semanas e até meses para tomar conhecimento do ataque e iniciar a mitigação.

Assumindo a premissa de que, a despeito de todos os esforços técnicos, ataques continuam a acontecer, tornando-se absolutamente crítico dispor de camadas de proteção para o Data Center. Tais camadas visam proteger os recursos e informações disponibilizados pela POUPEX, prevenindo, identificando e remediando ataques que possam comprometer a integridade, a disponibilidade e a privacidade das informações mantidas nesta instituição financeira.

3 – DESCRIÇÃO DA SOLUÇÃO

Os serviços de operação e monitoramento da Solução de Segurança deverão englobar hardware e softwares necessários à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos softwares utilizados nos serviços de segurança em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano).

O item 1 destina-se à prestação dos Serviços de "Solução de Inteligência Cibernética" da POUPEX, providos por serviços capazes de identificar, prevenir possibilita a automatização das fases de coleta e busca de informações com foco na indexação e busca avançada de informações existentes na Web e também em redes não indexadas

e redes sociais, realizando atendimento de diferentes objetivos de organizações preocupadas com Consciência Situacional em ambientes externos e muitas vezes desconhecidos.

O item 2 trata dos Serviços de "Solução de Monitoramento Analítico e Forense de Rede e Logs" responsáveis por coletar, armazenar, processar, monitorar e correlacionar logs de ativos e servidores da POUPEX, de modo a executar ações reativas e proativas, como envio de notificações e alertas aos administradores da rede do Contratante e da própria contratada. Os elementos a serem monitorados englobarão switches, roteadores, servidores de rede, servidores de aplicação e de banco de dados, além dos próprios equipamentos adotados nos serviços de operação e monitoramento aqui contratado.

O item 3 refere-se ao Serviços de "Solução de Duplo Fator de Autenticação",deixando a autenticação de 2 fatores ainda mais simples, mas igualmente segura, ao substituir os longos códigos de segurança e a necessidade de um dispositivo extra pelo toque de um botão.

O item 4 refere-se aos Serviços de "Solução para Compliance de Equipamentos de terceiros", vem da necessidade de controle sobre equipamentos de terceiros (BYOD). Essa solução deve prover formas de gestão de acesso a informações, compartilhamento de dados e tratamento de informações da instituição em equipamentos que não são fornecidos por ela.

O item 5 trata dos Serviços de "Segurança de Proteção de EndPoint", responsável pela segurança dos endpoints, de forma centralizada contra vírus, warms, liberação e bloqueio de acessos feitos pelos usuários da rede corporativa à websites e assemelhados, conforme política de acesso à Internet definida pelo Contratante.

O item 6 refere-se aos Serviços de "Solução de Gestão de Vulnerabilidade" capazes de detectar, inventariar e avaliar vulnerabilidades encontradas nos sistemas e recursos de TI e na solução de segurança da Contratante, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas.

O item 7 refere-se aos Serviços de "Solução Cofre de Senha e Gestão de Altas Credenciais", é responsável por melhorar controle dos acessos por contas privilegiadas e genéricas, viabilizando a rastreabilidade dos autores responsáveis por atos praticados com estas credenciais, preservando as evidências e garantindo a auditabilidade das ações.

O item 8 refere-se aos Serviços de "Solução de Criação de Correção Temporária para Novas Vulnerabilidade", nada mais é que a blindagem de sistema e aplicações contra exploração de vulnerabilidades conhecidas. Funcionam com a análise de tráfego de dados sendo capaz de interceptar o ataque ainda em trânsito, sem a necessidade da aplicação do patch de segurança de forma emergencial. Outro benefício relevante refere-se aos sistemas que não são mais suportados por seu fabricante.

O item 9 refere-se aos Serviços de "Solução de filtragem de conteúdo de E-mail", que é um serviço que bloqueia mensagens indesejadas na caixa de entrada do e-mail corporativo. Ele bloqueia e-mails de propagandas, vírus e pornografia e outros configuráveis via ferramenta administrativa. Ele funciona basicamente através de um conjunto de regras que separam os e-mails em desejados e indesejados.

Bens e/ou Serviços

Nº	Bens e/ou Serviços	Quantidade
1	Solução de Inteligência Cibernética (compreendendo 01 licença de gerenciamento e 05 licenças de dispositivos para execução dos testes) - software e suporte técnico	01(uma) licença

2	Solução de Monitoramento Analítico e Forense de Rede e Logs - software e suporte técnico	01 (uma) licença
3	Solução de Duplo Fator De Autenticação - hardware e suporte técnico	50 (cinquenta) equipamentos
4	Solução para Compliance de Equipamentos de terceiros - software e suporte técnico	4.000 (quatro mil) licenças
5	Solução de Proteção de Endpoint - software e suporte técnico	2.300 (dois mil e trezentas) licenças
6	Solução de Gestão de Vulnerabilidade e Aplicações - software e suporte técnico	10 (dez) licenças para scanners ativos e 2.048 (duas mil e quarenta e oito) licenças para dispositivos
7	Solução Cofre de Senha e Gestão de Altas Credenciais - software e suporte técnico (compreendendo 150 licenças para usuários ou 5.400 dispositivos)	01 (uma) licença
8	Solução de Criação de Correção Temporária para Novas Vulnerabilidade - software e suporte técnico	300 (trezentas) licenças para servidores
9	Solução de filtragem de conteúdo de E-mail - software e suporte técnico	2000 (duas mill) licenças

4 – ESPECIFICAÇÃO DA SOLUÇÃO

A CONTRATADA deverá garantir que as soluções permaneçam acessíveis para consultas referentes às informações coletadas durante a vigência do contrato.

A CONTRATADA deverá prover garantia de atualização de licenciamentos do software por meio da disponibilização de programas, correções e atualizações críticas de segurança e serviços de suporte técnico remoto, durante a vigência do contrato.

Os softwares que compõem a Solução não poderão estar na situação de end-of-support ou end-of-life prevista, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante;

Todos os módulos deste documento devem vir com a última versão de software e/ou firmware disponível no momento da aquisição;

O Proponente deve apresentar proposta para todos as soluções deste documento.

ITEM 1 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE INTELIGÊNCIA CIBERNÉTICA

- **CARACTERÍSTICAS GERAIS DA SOLUÇÃO**
  - A solução deve ser capaz de instrumentar e orquestrar simulações de ataques em rede;
  - A solução deve apresentar interface gráfica (GUI) baseado na web que permite a manipulação da ferramenta;
  - A solução deve permitir a autenticação via Active Directory (AD);
  - Permitir o cadastro de áreas que representem a infraestrutura a ser analisada;
  - Permitir o cadastro de novos agentes de forma a acompanhar o crescimento/mudança da infraestrutura;
  - As simulações não podem ter como alvo qualquer máquina na rede;
  - As simulações devem ser feitas de forma que se possa:
    - Agendá-las para uma execução única no futuro;
    - Agendá-las para uma execução repetida no futuro;
    - Indicar o tipo de ataque a ser simulado;
    - Indicar a origem e destino dos ataques;
  - A solução deve detalhar os ataques disponíveis;
  - A solução deve permitir combinar múltiplos ataques para criar cenários próximos ao real;
  - A solução deve gerar gráficos e métricas das simulações executadas;
  - Os dados apresentados pelas simulações executadas devem poder ser filtradas por no mínimo:
    - Tempo do ataque;
    - Agentes;
    - Áreas.
  - A solução deve ser capaz de reportar individualmente o resultado dos ataques identificando as lacunas de segurança e indicando os ataques que:
    - Foram bloqueados;
    - Foram permitidos mas detectados;
    - Foram permitidos mas não-detectados.
  - A ferramenta deve ser capaz de integrar com no mínimo os seguintes componentes de segurança:
    - Firewall;
    - IDS;
    - DLP;
    - Proxy;
    - Endpoints;
    - SIEM.

- A solução deve ser capaz de adicionar novas simulações de ataque de forma a estar atualizado com novas ameaças;
- A solução deve ser capaz de ser instalada e configurada tanto na rede interna quanto na Internet;
- Os agentes devem ser capazes de serem instalados e configurados tanto na rede interna quanto na Internet;
- A ferramenta deve ser capaz de se comunicar com seus agentes quando estes se encontrarem em:
    - Redes NAT;
    - Atrás de um proxy.
- A solução deve ser capaz de notificar a finalização do ataque via Syslog para integração com ferramentas já existentes;
- A solução deve ser capaz de exportar os dados os via CSV;
- A solução deve testar pelo menos os seguintes tipos de ataque:
    - Autenticação e autorização:
        - Ataques de Força bruta;
        - Escalação de privilégio.
    - Comando e controle;
    - Exfiltração de dados;
    - Ataque de negação de serviço;
    - Consulta maliciosa de DNS;
    - Transferência de arquivos maliciosos;
    - Man-in-the-middle;
    - Evasão de políticas;
    - Acesso remoto:
        - Shell reversa;
        - Shell web.
    - Varredura e enumeração:
        - Fingerprint;
        - Ping Sweeps;
        - Descoberta de políticas;
        - Varredura de portas;
        - Varreduras de vulnerabilidades;
        - Web Crawlers.
    - Ataques web:
        - Injeção de comando;
        - CSRF;
        - SQL Injection;
        - XSS.
- Deve possuir testes para pelo menos as seguintes plataformas:
    - Android;
    - IOS;
    - Linux;
    - Mac;
    - Windows.
- Deve testar e qualificar pelo menos os seguintes estágios de ataque:
    - Reconhecimento;
    - Entrega;
    - Exploração;
    - Execução;
    - Comando e Controle;

- Ação no alvo.

➢ Deve apresentar os resultados seguindo o padrão do Mitre ATT&CK.

➢ **SOLUÇÃO DE INTELIGÊNCIA EM FONTES ABERTAS**

▪ **REQUISITOS NÃO FUNCIONAIS**

▪ **ESPECIFICAÇÕES TÉCNICAS**

➢ REQUISITOS TÉCNICOS GERAIS

- A Proponente deverá disponibilizar console de gerenciamento centralizado do sistema.

➢ REQUISITOS TÉCNICOS FUNCIONAIS

- O funcionamento do produto deverá ser em nuvem com acesso realizado via web pela CONTRATANTE;
- O sistema deverá possuir mecanismo de captura automatizado de informações em sites, chats e mídias sociais;
- Pesquisar informações em mídias sociais, deep web e dark web de forma nativa em pelo menos os seguintes tipos de fonte: Fóruns, Twitter, Facebook, Telegram, Pastebin, RSS feeds, IRC, Discord, Sites. Onion, Zone-h, Shodan, Certificate Transparency, WhatsApp, Mercado Livre, OLX, lojas de aplicativos;
- Deve realizar monitoramento de marcas na web;
- Deve fazer transcrição de áudio captado em grupos de mensageria (pelo menos Telegram e Whatsapp);
- Deve fazer OCR de imagens capturadas em grupos de mensageria (pelo menos Telegram e Whatsapp);
- Deve possuir fontes relevantes pré-configuradas na plataforma em fontes Whatsapp e Telegram relacionada à grupos de fraudadores brasileiros;
- Deve indexar base de vulnerabilidades em dispositivos de rede (CVE);
- Deve monitorar links patrocinados no Google, Bing e Yahoo;
- Deve permitir configurar os BOTs com usuários distintos para a mesma fonte de dados;
- Deve possuir API com controle de acesso baseado em usuário e projetos para consumo de informações via outras ferramentas;
- Deve permitir a configuração, gerenciamento e análise dos registros de erro dos BOTs via interface da solução;
- Deve permitir a identificação de *defacement* de páginas;
- Deve identificar a emissão de certificados de domínios monitorados;
- Deve identificar a criação de domínios de recursos monitorados.
- Deve permitir a notificação de eventos relevantes em forma de ocorrências para outros usuários em times dentro da organização;
- Deve permitir a associação de múltiplos eventos a uma mesma ocorrência;
- Deve ser possível visualizar diretamente nos eventos a(s) ocorrência(s) em que o dado evento foi associado;
- As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas;
- Deve ser possível notificar via e-mail a criação e modificação de ocorrências aos times envolvidos;

➢ REQUISITOS DE GERENCIAMENTO DA SOLUÇÃO

- Para efetuar o gerenciamento da solução, o sistema **deverá:**
  - ♦ Deve possuir interface de gerenciamento no idioma Português do Brasil;
  - ♦ Ter interface web via *cloud* pública;
  - ♦ Ser compatível com navegadores Mozilla Firefox, versão 60.0 ou superior, Google Chrome versão 65 ou superior;
  - ♦ Disponibilizar módulo de administração e gerenciamento de perfis de acesso e grupos de trabalho;
  - ♦ Deve permitir configuração de alertas diretamente via interface de gerenciamento;

- Permitir, no mínimo, configurar, habilitar e desabilitar múltiplos logins de usuários, complexidade de senhas, troca de senha no primeiro login, troca de senha periodicamente, ativação e desativação de usuários, definição de grupos e times;
- Permitir a criação de projetos para cada time, possibilitando que o usuário salve os resultados das pesquisas, individualmente por projeto;
- Disponibilizar usuário(s) ou grupo de usuários com perfil de administrador para acesso aos recursos da ferramenta, bem como acesso aos dados e alertas de outros usuários;
- Permitir a criação de grupos de usuários por perfil de acesso e visualização;
- Permitir que dentro dos grupos, sejam criados projetos onde todos os usuários participantes tenham acesso aos projetos relacionados ao grupo;
- Permitir que dentro do projeto, o usuário:
- Salve consultas para disponibilizar para outros usuários;
- Crie, gerencie e exclua alertas;
- Salve tabelas de dicionários para o uso em pesquisas;
- Possuir análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades:
- Visualização de perfis relacionados a palavras-chaves;
- Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;
- Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.
- Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;
- Exportar as informações identificadas em relatórios via XLS ou CSV, DOCX e PDF.

➢ COLETA DE DADOS EM FÓRUNS

- Para efetuar coleta de dados em fóruns, o sistema **deverá**:
  - Suportar, minimamente, os seguintes fóruns: PHPBB, PHPNUKE e vbulletin.
  - Coletar os dados que foram criados e modificados desde a última coleta.
  - Manter sincronia com a estrutura do fórum analisado. Caso sejam criadas novas estruturas, como novos fóruns ou subfóruns, tópicos ou mensagens, o sistema deverá catalogá-los e iniciar a coleta das informações imediatamente após adição da nova fonte;
  - Manter em sua base de dados informações sobre a última coleta, incluindo data, horário e fuso horário da última coleta realizada em cada fórum;
  - Deverá extrair, no mínimo, os seguintes metadados de cada mensagem: *data e hora com precisão de segundos* do momento do envio e do momento da coleta;
  - No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação;
  - Manter todos os metadados da coleta realizada (fonte, grupo, hash da coleta).

➢ COLETA DE DADOS EM REDES SOCIAIS

- Para efetuar a coleta de dados de contas em redes sociais, o sistema **deverá:**
  - Suportar minimamente as redes sociais Twitter, Instagram e Facebook;
  - Permitir o cadastramento de novas contas de redes sociais;
  - Coletar publicações já realizadas na conta em questão, mesmo que estas sejam anteriores à data de cadastramento no sistema;
  - Coletar as novas publicações feitas pela conta desde à última coleta;
  - Deverá extrair, no mínimo, os seguintes metadados de cada mensagem: data e hora com precisão de segundos do momento do envio e do momento da coleta;
  - Possuir mecanismo que busque automaticamente novas publicações das contas cadastradas conforme um agendamento pré-configurado.

- Coletar apenas as publicações que ainda não constam em sua base de dados. Alterações também deverão ser catalogadas e armazenadas. No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação.

➢ COLETA DE DADOS EM REDES DE COMPARTILHAMENTO DE TEXTOS

- Para efetuar a coleta de dados em redes de compartilhamentos de texto, a solução **deverá:**
  - Suportar automaticamente a rede de compartilhamento de textos pastebin;
  - Permitir o cadastramento de novas contas de redes de compartilhamento de textos, conforme necessidade da CONTRATANTE;
  - Coletar as publicações já realizadas na conta em questão, mesmo que estas sejam anteriores à data de cadastramento no sistema;
  - Coletar as novas publicações feitas pela conta desde à última coleta;
  - Deverá extrair, no mínimo, os seguintes metadados de cada mensagem: data e hora com precisão de segundos do momento do envio e do momento da coleta;
  - Possuir mecanismo que busque automaticamente novas publicações das contas cadastradas conforme um agendamento pré-configurado.
  - Coletar apenas as publicações que ainda não constam em sua base de dados. Alterações também deverão ser catalogadas e armazenadas. No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação.

➢ COLETA DE DADOS EM APLICATIVOS DE TROCA DE MENSAGENS

- Para efetuar a coleta de dados em aplicativos de troca de mensagens, a solução **deverá:**
  - Deverá suportar minimamente e de forma automática os seguintes aplicativos de troca de mensagens: WhatsApp, Telegram, Discord e IRC;
  - Permitir a inclusão e o monitoramento de novos grupos dos aplicativos de troca de mensagens;
  - Coletar as publicações já realizadas no grupo em questão, mesmo que estas sejam anteriores à data de cadastramento no sistema, desde que disponibilizada pelo aplicativo;
  - Coletar as novas publicações feitas pela conta desde à última coleta;
  - Deverá extrair, no mínimo, os seguintes metadados de cada mensagem: data e hora com precisão de segundos do momento do envio e do momento da coleta;
  - Possuir mecanismo que busque automaticamente novas publicações das contas cadastradas conforme um agendamento pré-configurado.
  - Coletar apenas as publicações que ainda não constam em sua base de dados. Alterações também deverão ser catalogadas e armazenadas. No caso de exclusão de publicações, as mesmas não deverão ser excluídas da aplicação.

➢ REQUISITOS DE BUSCA DO CONTEÚDO

- Para efetuar a busca de conteúdo, a solução **deverá:**
  - Disponibilizar mecanismo para busca das informações permitindo: busca por intervalo de data, busca por metadados e por base de dados;
  - Disponibilizar através de interface web, a busca utilizando mecanismos como: proximidade, *fuzzy* (difusa), lógica binária, expressões regulares, operadores lógicos (“AND, “OR” e “NOT”), caracteres *wildcard*;
  - Permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga;
  - Permitir a escolha da quantidade de resultados por página;
  - Permitir integração com API REST com suporte no retorno de informações no padrão XML ou JSON;
  - Permitir salvar o resultado da pesquisa.

➢ REQUISITOS DE ALERTAS

- Para efetuar a geração de alertas, a solução **deverá:**

- Disponibilizar ambiente para criação e controle de alertas com as mesmas possibilidades que o ambiente de busca oferece, exibindo os alertas já criados, respeitando as permissões de acesso dos usuários e grupos aos quais pertencem;
- Permitir a criação de alertas configurando sua periodicidade, expressão de busca e definir endereços eletrônicos para envio;
- Possibilitar ativação, desativação, edição e exclusão de alertas existentes conforme permissões de acesso;
- Executar automaticamente os alertas ativos, conforme o agendamento configurado;
- Enviar e-mails dos alertas, que deverão incluir os resultados encontrados, separados por base de dados, a quantidade de resultados encontrados e o *timestamp* do momento da geração do alerta;
- Possibilitar o envio de e-mails criptografados.
- O ambiente de alertas deverá disponibilizar a opção de testar os alertas existentes;
- Para a geração de um teste de alerta, o sistema deverá consultar a base de dados existente e enviar o e-mail com os resultados.

- A interface de acesso e consulta deve ser instalada na nuvem em ambiente da CONTRATADA.
- A solução deve ser licenciada para o uso de 05 usuários.

ITEM 2 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE MONITORAMENTO ANALÍTICO E FORENSE DE REDE E LOGS

- Possuir arquitetura de forma distribuída, possuindo no mínimo os seguintes módulos ou componentes: módulo de coleta de pacotes e logs, módulo de indexação, agregação e enriquecimento dos módulos de coleta, módulo de correlação avançado de alertas e tratamento de incidentes e módulo de gerência centralizada de todos os outros módulos envolvidos.
- Deve ser capaz de reter, por pelo menos 15 (quinze) dias, informações de dados brutos de pacotes, considerando um volume médio de tráfego de rede de 400 Mbps.
- Deve ser capaz de reter, por pelo menos 6 (seis) meses, informações de dados brutos de eventos/logs/flows, considerando um valor de 50GB/dia e de 5.000 flows/s.
- A solução deverá ser capaz de reter. Informações de metadados de pacotes e eventos/logs/flows por pelo menos 12 (doze) meses.
- O software deverá permitir o uso de interfaces nos Sistemas Operacionais com as seguintes velocidades 1000BaseT/SX/LR/SR/LX/LH, 10GBase-LR/SR e 40GBase-SR4;
- Ao final de cada período de retenção informado, a solução de suportar a compactação e o arquivamento das informações de dados e metadados em área de armazenamento via CIFS/NFS a ser disponibilizada.
- A solução oferecida deve permitir a correlação de eventos provenientes de pacotes e logs, devidamente estruturados em metadados;
- Permitir a administração, configuração, investigação, análise e resposta, de forma centralizada e em uma única console, dos recursos para captura de pacotes e eventos/logs/flows;
- Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
- Possuir compatibilidade e integração nativa com pelo menos uma solução de forense comportamental de endpoints (EDR), com intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa;
- A solução deve prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;
- Possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;
- A solução deve prover uma interface extremamente intuitiva, permitindo que em até três cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento da mesma;

- A solução deve integrar-se nativamente com uma solução de análise forense de estações, sendo capaz de utilizar dados e indicadores de comprometimento gerados pela mesma;
- Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
- Possuir regras pré-configuradas pelo fabricante de captura de pacotes e eventos/logs para a geração de alertas de ameaças cibernéticas de forma automática, além de permitir a criação e customização, via console, de novas regras de alertas;
- Permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por email;
- O fabricante deve possuir seu próprio centro de pesquisa e desenvolvimento e inteligência contra novas ameaças;
- A solução deve possuir mecanismos automáticos para atualização de regras diretamente com o fabricante, online através da Internet;
- Ser capaz de consultar, periodicamente, bases de conhecimento e inteligência de ameaças tanto em fontes abertas quanto fechadas, de forma a alimentar seus mecanismos, baseado em múltiplos eventos/logs, com identificação de potenciais problemas ou comportamentos anômalos;
- Ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:
  - relatórios de ameaças e segurança;
  - relatórios de botnets e centros de Comando e Controle;
  - identificação de exploit kits;
  - indicadores de ataques “zero-day”;
  - indicadores de comprometimento, suspeitas e avisos Informativos;
  - inteligência de tendências;
  - proxies anônimos;
  - classificação de sites;
  - endereços de rede TOR.
- Possuir módulo de análise de malware de mesmo fabricante integrado a solução;
- O módulo de análise de malware deve permitir o uso de regras YARA;
- Possuir integração nativa com soluções de gestão de centro de operações de segurança (Security Operations Center - SOC);
- Permitir, via console, a configuração de papéis /perfis de acesso ao conteúdo de dados e metadados de pacotes e eventos/logs/flows, auditoria de operação e administração da solução, além de se integrar com os recursos de autenticação e autorização suportando no mínimo, Microsoft Active Directory e Pluggable Authentication Module (PAM);
- Possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;
- Permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;
- Permitir a captura de dados de forma distribuída e toda a análise centralizada;
- Possuir controle de acesso baseado em papéis e perfis de usuários;
- Permitir gerar relatórios em formatos HTML, PDF e CSV;
- Possuir um módulo para construção de relatórios customizados pelo usuário, com funcionalidade do tipo arrastar-e-colar para definição dos campos e elementos dos mesmos;
- Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolos SYSLOG e SNMP;
- Permitir a definição e customização de alertas, relatórios e gráficos;
- A solução deve disponibilizar uma API ou SDK permitindo a integração e customização com a solução;
- Suportar a comunicação criptografada entre os componentes envolvidos;
- A solução deve fazer uso de protocolo proprietário entre os componentes, para garantir máximo desempenho;
- Possuir um módulo de monitoração de desempenho e saúde dos equipamentos envolvidos;
- Possuir métricas de saúde dos equipamentos como: utilização de CPU, temperatura da CPU, utilização de memória, disco rígido, status do serviço, status das conexões;

- Suportar armazenamento externo através de Direct-Attached Capacity (DAC) ou Storage Area Network (SAN);
- Possuir interface de rede dedicada para a aquisição (captura) de dados;
- Possuir relatórios de conformidade e regulamentações pré-definidos (out-of-the-box) como BASEL II, FERPA, FFIEC, FISMA, GLBA, HIPPA, ISO27002, NERC-CIP, NISPOM, PCI e SOX;
- A solução deve utilizar sistema operacional baseado em Linux;
- A solução deve segregar a visualização de relatórios apenas para usuários com a devida permissão;
- Possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
- Suportar a integração nativa com sistemas de GRC (Governance, Risk e Compliance), possibilitando a integração de dashboards entre as soluções e provendo contexto de governança a um incidente gerado pela solução proposta;
- Possuir a funcionalidade para resolução de endereços IP, como localização da cidade, país e organização das conexões;
- Ser capaz de exportar e importar arquivos contendo pacotes de tráfego de rede em seu formato bruto, com possibilidade de gerar e verificar a informação de integridade desses arquivos;
- Permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução web (HTTP), reconstrução e-mail (SMTP) e arquivos (binários);
- Suportar a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, e-mail, endereço, arquivos e ações;
- Suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;
- A solução deve implementar decifrar uma sessão de rede criptografada em qualquer protocolo da camada de aplicação da pilha TCP/IP, tendo conhecimento da chave privada de criptografia utilizada na transmissão, sem requerer o uso de soluções externas;
- Suportar a geração de hash (MD5 e SHA1) para verificação de integridade dos arquivos extraídos a partir do tráfego de rede capturado;
- Possuir a capacidade de extração de metadados do tráfego de dados capturado, com reconhecimento nativo de no mínimo os seguintes protocolos e aplicações: FTP, SFTP, SCP, Gtalk, H323, HTTP, HTTPS, IMAP, IRC, LotusNotes, MAIL (RFC822), MSN, Net2Phone, NETBIOS, POP3, RDP, RTP, SIP, SMB, SMIME, SMTP, SNMP, SSH, TELNET, TNS, DNS, TORRENT, P2P, ARP;
- Possuir a capacidade de criação de interpretadores (parsers) para protocolos, aplicações proprietárias e aplicações desconhecidas;
- Possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação;
- Permitir isolar sessões de tráfegos, com identificação de conteúdo (payload) de origem e destino, para os protocolos ICMP, TCP e UDP;
- Permitir a extração dos arquivos presentes no tráfego de rede capturado;
- A solução deve alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão dados brutos;
- Possuir mecanismos computacionais capazes de identificar potenciais problemas ou comportamentos anômalos, baseado em múltiplos eventos/logs, gerando alertas tanto no console centralizado quanto os enviando por e-mail;
- Possuir ferramenta para administração centralizada dos módulos de captura do tráfego de rede, permitindo a replicação de parâmetros de configuração entre os dispositivos a partir de uma única fonte;
- Permitir a criação customizada de interpretadores (parsers) para identificação de protocolos de rede específicos;
- Ser capaz de analisar tráfego IPv4 e IPv6;
- Permitir a customização de um interpretador de busca, cuja função é analisar todas as sessões de rede em busca de palavras chaves ou sentenças;
- A solução deve funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;

- Ser capaz de possuir mecanismos que assegurem que os pacotes capturados não sofreram violação de integridade e sigilo;
- Permitir nativamente, a análise automatizada e ampla de malwares e suas atividades de rede;
- Permitir a captura e análise de características suspeitas em arquivos de conteúdo executável na rede em tempo real;
- Possuir um mecanismo de pontuação de risco no momento da análise de malwares;
- Permitir plena integração com outras tecnologias de análise em sandbox, tanto em equipamento físico ou SaaS;
- Possuir painel configurável que permita a rápida visualização do status da segurança e acesso granular a sessão reconstruída equivalente ao tráfego que gerou o alerta;
- Possuir a capacidade de exibir visualmente os objetos trafegados pela rede sem a necessidade de manipular os dados diretamente na console ou banco de dados;
- Permitir que a partir de uma informação existente em um relatório, se verifique o tráfego de rede que a gerou através de recurso de “drill-down”;
- Ser capaz de identificar a troca de extensão de arquivos (arquivo .exe enviado como .jpg);
- Possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;
- Permitir o processamento de eventos/logs, apenas com a adição de componentes para tal finalidade, mantendo a taxonomia dos metadados;
- A solução deve ser capaz coletar e armazenar todos os logs de ativos de rede e dispositivos que são recebidos em sua interface de rede, gravando-os em formato original para posterior uso em fins forenses;
- Ser capaz de coletar os logs dos ativos de rede e dispositivos de forma não intrusiva, sem a instalação de agentes;
- Possuir a capacidade de geração de alertas sobre qualquer dado ou comportamento desejado e permitir o envio deste alerta a plataformas externas como SIEM ou SYSLOG;
- Suportar de forma nativa os logs de pelo menos 300 dispositivos diferentes de diversos fabricantes;
- Possuir capacidade de coletar logs de sistemas operacionais Windows, Linux, Unix, FreeBSD, Solaris e AIX;
- Ser capaz de coletar logs de firewalls, antivírus, IDSs, proxies, servidores web, servidores DNS, load balancers, roteadores, switches e demais dispositivos de rede;
- Possuir capacidade de coletar logs de IBM zOS e RACF;
- Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOG-NG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, CheckPoint LEA, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC, CISCO e CISCO Security Device Event Exchange (SDEE);
- A solução deve utilizar formatos de logs/eventos através de formatos nativos de cada fabricante do dispositivo, sem utilizar um tipo de formato comum definido pelo proponente da solução;
- A solução não deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto caso o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;
- Coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta;
- A solução deve ser fornecida com todos os sistemas operacionais e sistemas de gerenciamento de bando de dados necessários para o seu funcionamento;
- Permitir que os logs/eventos dos dispositivos da empresa sejam enriquecidos com informações de classificação de risco;
- Permitir a correlação de logs/eventos próximo ao tempo real;
- Implementar notificação através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
- Possuir um painel de controle, onde através de simples “drill-down” possa ver o log/evento coletado;
- A solução deve fornecer painel de controle que constantemente mostre o status do ambiente de correlação de eventos;

- Ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
- Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;
- Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
- Possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlação e eventos complexos em dados correlacionados;
- A solução deve detectar de forma nativa ataques do tipo syn flood a partir da coleta de Netflows;
- Ser capaz de receber logs/eventos oriundos de um relay de syslogs;
- Suportar o recebimento de eventos no formato Common Event Format (CEF);
- Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;
- Implementar notificação através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
- A solução deve fornecer painel de controle que constantemente mostre o status do ambiente de correlação de eventos;
- Permitir que o administrador possa filtrar eventos ao gerar relatórios;
- A solução deve oferecer uma plataforma unificada, acessível via browser web para realizar investigações, gestão de incidentes, gestão de alertas, gestão de relatórios, administração dos componentes e gestão de inteligência externa;
- Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
- Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.
- Suportar de forma nativa e automática o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas como NAS para pesquisa, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento off-line para possível restauração em WARM);
- Suportar nos sistemas de armazenamento de longo prazo algoritmos de compressão;
- Permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;
- Permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON, CSV;
- Possuir um módulo específico para tratar dados arquivados e/ou recuperados;
- Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:
  - Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
  - Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
  - Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;
  - Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
  - Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;
  - Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
  - Permitir inserir análise forense de host e rede como um complemento da análise do incidente;

- Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2);
- Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux;

❖ Implementar regras de comportamento suspeito de usuários, devendo ser capaz de detectar, pelo menos, as seguintes anomalias:
- Conta adicionada e removida do grupo de administradores
- Conta criada e excluída em seguida, dentro de um intervalo de tempo definido
- Conta adicionada ao grupo de administradores pelo mesmo usuário que executou o comando
- Registro de login de conta monitorada em uma watchlist
- Falhas de logins sucedidas por um login bem-sucedido a alteração de senha
- Falhas de logins sucedidas por um login bem-sucedido, acompanhado por alteração de senha
- Falhas de logins fora do horário comercial
- Falhas de logins de diferentes origens para o mesmo destino
- Falhas de logins de diferentes usuários para o mesmo destino
- Falhas de logins de um mesmo usuário de diferentes países
- Falhas de logins de uma mesma origem com diferentes usuários
- Logins bem-sucedidos de diferentes origens para diferentes destinos
- Logins bem-sucedidos de diferentes origens para o mesmo destino
- Múltiplos bloqueios de conta do mesmo usuário e de usuários diferentes
- Falhas de escalonamento de privilégios de um mesmo usuário
- Falhas de logins em um Domain Controller de um usuário administrador
- Limpeza em massa de logs de auditoria
- Limpeza dos logs de auditoria, firewall e compartilhamento do Windows
- Alteração da conta krbtgt em Domain Controller
- Suspeitas de movimentação lateral
- Logins através de vários servidores

❖ Suportar integração com tecnologia de análise comportamental de usuários e entidades (UEBA) do mesmo fabricante, baseado em técnicas de "machine learning" e análises estatísticas para a monitoração de segurança, gerando índices de riscos para eventos e entidades mapeadas;
❖ A solução deve exibir a data e hora do último login no rodapé da interaface, de forma garantir que a credencial não esteja sendo compartilhada;
❖ Permitir o processamento de informações estruturadas de ameaças STIX (“Structured Threat Information eXpression”);
❖ Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando à redução de erros de lógica e sintaxe;
❖ Permitir a customização de perfis de visualização de metadados de acordo com o objetivo da investigação (ex.: Análise Web, Análise e-mail, Análise de Arquivos, etc.);
❖ Possuir um menu de contexto na interface de investigações, de forma visualizar instantaneamente se endereços foram encontrados em Alertas, Incidentes ou Listas.

ITEM 3 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE DUPLO FATOR DE AUTENTICAÇÃO

❖ **CARACTERÍSTICAS GERAIS DA SOLUÇÃO**
❖ Deve ser uma solução de autenticação baseada em hardware que ofereça defesa contra phishing, elimine aquisições de contas e permita requisitos de conformidade para autenticação forte.
❖ Deve possuir pelo menos os seguintes protocolos:
- WebAuthn;
- FIDO2;

- FIDO U2F;
- Smart card (PIV);
- OTP;
- OpenPGP;
- OATH-TOTP;
- OATH-HOTP;
- Challenge-Response.

❖ Deve permitir a instalação de certificados digitais;
❖ Deve possuir conexão USB para autenticação em computadores e notebooks;
❖ Deve permitir a substituição de uso de senhas;
❖ Não pode possuir bateria;
❖ Possuir integração com Microsoft Active Directory e soluções de gestão de identidades.

ITEM 4 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO PARA COMPLIANCE DE EQUIPAMENTOS DE TERCEIROS

- Fornecer appliances virtuais, licenciamento e suporte necessário para a implementação e operação da solução para atender um parque de até 4000 (quatro mil) dispositivos conectados à rede; a solução deverá ser compatível com:
  - VMware ESXi v. 5.1 ou superior
  - Microsoft Hyper-V 2012, 2012R2 ou 2016
  - KVM em Red Hat Linux RHEL/CentOS7
- A solução deverá oferecer visibilidade e controle de acesso para todos os tipos de dispositivos (estações de trabalho, servidores, dispositivos móveis, IoT, impressoras, câmeras, e qualquer outro dispositivo que tenha endereço IP);
- A solução deverá apresentar mecanismo para gestão de convidados, terceiros e BYOD usando um captive portal;
  - A gestão de convidados deverá ser manual ou automática, e deverá apresentar ferramentas para que um sponsor possa gerenciar o acesso;
- A solução deverá suportar 802.1x, mas este protocolo não deve ser necessário para se implementar a solução;

➢ **Integração com o ambiente existente:**

- A solução deverá integrar-se nativamente com as seguintes bases de usuários:
  - OpenLDAP
  - Active Directory
  - RADIUS
  - TACACS
  - Oracle Directory Server
  - Base interna para gestão de visitantes
- Switches
  - A solução deverá integrar-se nativamente com no mínimo as seguintes marcas de switches:
    - ♦ Cisco
    - ♦ HPE
    - ♦ Juniper
    - ♦ Avaya
    - ♦ Huawei
    - ♦ Arista
    - ♦ H3C
    - ♦ Alcatel
    - ♦ Brocade

- Dell Force10
- Extreme
- Hirschmann
- Dasan
- FortiSwitch

- As integrações acima devem ser feitas via SNMP e/ou telnet e/ou SSH, sem depender de 802.1x;
- Para ao menos três das marcas acima, a solução deverá ser capaz de gerenciar listas de acesso (ACL) sem o uso de 802.1x;
- A solução também deverá suportar 802.1x e CoA para elementos de rede que o suportam.

- Wireless
  - A solução deverá integrar-se nativamente com no mínimo as seguintes plataformas de Wireless:
    - Cisco
    - Aruba
    - Motorola
    - Ruckus
    - Xirrus
    - AeroHive
  - As integrações acima devem ser feitas via SNMP e/ou telnet e/ou SSH, sem depender de 802.1x;
  - A solução também deverá suportar 802.1x e CoA para elementos de rede que o suportam.
- Firewalls
  - A solução deverá integrar-se nativamente com no mínimo as seguintes plataformas de Firewalls para obtenção de tabela ARP quando estes firewalls forem o Default Gateway do Ambiente:
    - Cisco ASA
    - CheckPoint
    - FortiGate
    - Juniper
    - Palo Alto
  - As integrações acima devem ser feitas via SNMP e/ou telnet e/ou SSH, sem depender de 802.1x;
- Nuvens Públicas da Amazon (AWS);
  - A solução deverá integrar-se nativamente com Amazon AWS:
    - A solução deverá permitir configurar a API Key da Amazon para coleta de objetos na núvem;
    - A solução deverá permitir leitura e alteração de parâmetros como Security Groups, ligar ou desligar uma máquina virtual, ou tomar outras ações via API;
- Nuvens Públicas Microsoft (Azure);
  - A solução deverá integrar-se nativamente com Microsoft Azure:
    - A solução deverá permitir configurar um Tenant ID, Client/App ID, e a Access Key para coleta de objetos na núvem;
    - A solução deverá permitir leitura e alteração de parâmetros como ligar ou desligar uma máquina virtual via API;
- Nuvem Privada Vmware;
  - A solução deverá integrar-se nativamente com Vmware vCenter:
    - A solução deverá permitir configurar um usuário e senha que terão acesso ao vCenter para coleta de máquinas virtuais criadas no ambiente;

- ♦ A solução deverá permitir alteração de parâmetros como Port Groups, status da VM e outros;
- A solução deverá interagir nativamente com Vmware NSX
  - ♦ A solução deverá permitir aplicar e remover um Security TAG ao host;
  - ♦ A solução deverá permitir inserir e remover um host de um Security Group;

▪ Análise de tráfego espelhado (SPAN, Mirror)
- A solução deverá ser capaz de ler tráfego espelhado uma ou múltiplas interfaces da rede para descoberta de dispositivos conectados, análise de tráfego, fingerprinting;
- A solução deverá ser capaz de interagir com o tráfego, usando porta espelho para fazer redirecionamento a um portal (captive portal) ou bloqueando determinados tráfegos;

▪ Suporte a Netflow
- A solução deverá ser capaz de ler tráfego NetFlow v9 ou SFlow para descoberta de dispositivos conectados, análise de tráfego e fingerprinting;

▪ Suporte a DHCP
- A solução deverá ser capaz de interpretar pacotes DHCP quando vistos pela interface espelhada;
- A solução deverá ser capaz de receber tráfego DHCP direcionado via DHCP Relay;
- DHCP deve ser usado para fazer fingerprinting de dispositivos;

▪ Suporte a DNS
- A solução deverá ser capaz de atuar como DNS Proxy, permitindo responder a requisições de DNS de usuários da rede;
- Esta função também pode ser usada para redirecionar usuários para um portal (captive portal);

▪ Suporte a 802.1x
- A solução deverá suportar o uso de 802.1x para autenticar usuários ou dispositivos na rede quando necessário;
- A solução deverá suportar PEAP e EAP-TLS;
- A solução deverá suportar as extensões de CoA (RFC 3576);
- A solução deverá funcionar em modo Proxy e também em modo Servidor;

▪ Integração com CheckPoint NGFW
- Permite a integração nativa com Firewall Checkpoint 77.20, 77.30 ou 80.10;
- Se integra com Identity Awareness do CheckPoint;
- A solução, uma vez identificado o usuário que está utilizando o dispositivo, repassa a informação de Usuário e endereço IP ao CheckPoint para que este possa aplicar políticas por usuário;
- A solução se torna um fornecedor de Identidade para o Firewall;
- A solução deverá permitir a integração de mais de um Firewall checkpoint simultaneamente;

▪ Integração com ServiceNow
- A solução deverá ser capaz de integrar-se nativamente com ServiceNow;
  - ♦ A solução deverá ser capaz de enviar dados ao CMDB do ServiceNOW
  - ♦ A solução deverá ser capaz de ler e consultar o CMDB para obter novos atributos sobre os dispositivos;
  - ♦ Estes atributos deverão poder fazer parte das políticas de visibilidade, classificação e Controle;
  - ♦ A solução deverá permitir que a base de dados do ServiceNow permaneça continuamente atualizada com mudanças nos dispositivos conectados à rede;
  - ♦ A solução deverá permitir que IT Incidents (jargão ServiceNow para tickets) sejam abertos automaticamente quando determinados eventos ou cenários forem encontrados;
- Integração com Mcafee EPO
  - ♦ A solução deverá ser capaz de integrar-se nativamente com Mcafee EPO

- ♦ A solução deverá consultar a base do ePO toda vez que encontrar um dispositivo sem o Agente ePO. Se o dispositivo não tiver registrado no ePO, a solução deverá automaticamente registrá-lo para que o ePO possa instalá-lo;
- ♦ A solução deverá ser capaz de ler e consultar o Mcafee ePO para obter novos atributos sobre os dispositivos;
- ♦ Estes atributos deverão poder fazer parte das políticas de visibilidade, classificação e Controle;

- Integração com Symantec Endpoint Protection Manager
  - ♦ A solução deverá ser capaz de integrar-se nativamente com Symantec Endpoint Protection Manager
  - ♦ A solução deverá permitir ser alertada quando a plataforma Symantec encontrar um malware e deverá ser capaz de tomar ações automatizadas de controle para remover o elemento da rede.
  - ♦ A solução deverá consultar a base do SEP Manager toda vez que encontrar um dispositivo sem o agente SEP. Se o dispositivo não tiver registrado no SEP Manager, a solução deverá automaticamente registrá-lo para que o SEP Manager possa instalá-lo;
  - ♦ A solução deverá avaliar os dispositivos e garantir que todas as políticas corporativas do SEP estão ativas no dispositivo, e deverá alertar ou remediar quando encontrar divergências;
  - ♦ A solução deverá receber o IOC de um malware detectado pelo SEP de dispositivo e deverá iniciar uma análise de todos os outros dispositivos gerenciados, com ou sem SEP, em busca desta mesma ameaça;
  - ♦ A solução deverá permitir o recebimento de um IOC detectado por outra ferramenta, como um scanner de vulnerabilidades, e disparar automaticamente um “scan” em todos os dispositivos que possuem SEP instalado.
- Integração com ferramentas de Análise de Vulnerabilidades marca Tenable,
  - ♦ A solução deverá ser capaz de interagir com as soluções de análise de vulnerabilidades para:
    - ➢ disparar automaticamente um scan de um dispositivo específico de acordo com uma política configurado na solução
  - ♦ A solução deverá ser capaz de ler e consultar a ferramenta de Análise de Vulnerabilidade para obter novos atributos sobre os dispositivos;
  - ♦ Estes atributos deverão poder fazer parte das políticas de visibilidade, classificação e Controle;
- Integração com ferramentas de Análise de Vulnerabilidades
  - ♦ A solução deve ser passível de integração nativa com SIEM;
  - ♦ As seguintes tecnologias devem ser suportadas:
    - ➢ Qradar
    - ➢ Splunk
    - ➢ ArcSight
    - ➢ Netwitness
  - ♦ A solução deverá ser capaz de interagir com as soluçoes de SIEM para:
    - ➢ disparar automaticamente ações de remediação ou controle em um dispositivo específico de acordo com uma política configurado na solução
  - ♦ A solução deverá ser capaz de ler e consultar a ferramenta de SIEM para obter novos atributos sobre os dispositivos;
  - ♦ Estes atributos deverão poder fazer parte das políticas de visibilidade, classificação e Controle;

➢ **Identificaçao de Dispositivos:**

- A solução deverá ser capaz de identificar onde cada dispositivo se conectou na rede
  - Qual controller e qual AP do Wifi;

- Qual o SSID usado para conexão;
- Qual Porta de Qual Switch;
- Características da Porta de Switch conectada – PoE, nome e número de VLAN, etc;

▪ A solução deverá usar múltiplos métodos para identificar a entrada de um novo dispositivo na rede:
- Tráfego espelhado gerado pelo dispositivo;
- Pacote DHCP gerado pelo dispositivo;
- Endereço do Dispositivo na tabela do switch ou default gateway;
- Trap SNMP da controller Wifi ou do Switch onde o dispositivo se conectou;
- Pacote 802.1x Auth, cuando a solução está se comportando como servidor 802.1x;
- Pacote 802.1x Accounting, mesmo quando a solução não está se comportando como servidor 802.1x;
- Informado via API, quando o dispositivo for uma máquina na núvem AWS ou Azure;

➢ **Classificação de Dispositivos;**
▪ Os dispositivos conectados à rede deverão ser classificados quanto a sua Função
▪ Os dispositivos conectados à rede deverão ser classificados quanto ao seu SO
▪ Os dispositivos conectados à rede deverão ser classificados quanto ao seu Fabricante
▪ A classificação deverá ser feita por múltiplos métodos. No mínimo os seguintes métodos deverão ser suportados pela solução:
- Fingerprint de DHCP
- Portas TCP abertas
- Cabeçalho HTTP visto ao acessar o portal (captive portal)
- Cabeçalho HTTP visto no tráfego espelhado ao acessar qualquer site
- Tráfego de Autenticação gerado pelo dispositivo
- Outros tráfegos gerados pelo dispositivo, vistos via NetFlow ou tráfego espelhado;
- Banner de NMAP;
- Dados obtidos pelo Switch;
- Domínio NetBIOS;
- Propriedades obtidas da nuvem privada ou pública, como SO da VM;
- Nome configurado no DNS;
- Endereços IPv4 e IPv6;
- Presença ou ausência de Agente da Solução instalado no dispositivo;
- Query SNMPv1, v2 e v3 ao próprio dispositivo;

➢ **Análise e Remediação de Postura;**
▪ A solução deverá ser capaz de analisar e remediar estações Windows sem o uso de agente instalado na máquina. As funções abaixo deverão ser suportadas sem agente:
- Suportar no mínimo Windows 7, 8 e 10;
- Suportar no mínimo Windows Server 2012, 2012R2 e 2016;
- A solução deverá determinar o nome do usuário que está com login feito no dispositivo;
- A solução deverá cruzar esta informação com a base de usuários listadas no item para obter dados do usuário como nome completo, e-mail e grupos a que pertence.
- Analisar se antivirus está instalado. No mínimo os seguintes antivirus deverão ser suportados nativamente:
  - ♦ AhnLab
  - ♦ Avast
  - ♦ AVG
  - ♦ Avira
  - ♦ BitDefender
  - ♦ E-Trust
  - ♦ ClamAV

- Comodo Antivirus
- eScan
- ESET Nod32
- F-Secure
- G Data
- Hauri
- Kaspersky
- KingSoft
- LightSpeed
- Mcafee
- Microsoft Security Essentials
- Microsoft Windows Defender
- Panda Antivirus
- Rising Antivirus
- Sophos Antivirus
- Symantec Antivirus
- Symantec Endpoint Protection
- Trend micro

- Para cada um dos antivirus listados acima, a solução deverá ser capaz de analisar a data da atualização;
- Para cada um dos antivirus listados acima, a solução deverá ser capaz de forçar que o dispositivo busque uma atualização (remediar o problema);
- Para cada um dos antivirus listados acima, a solução deverá ser capaz de analisar se o Antivirus está em execução
- Para cada um dos antivirus listados acima, a solução deverá ser capaz de forçar a execução de um antivirus parado (remediar o problema);
- Analisar se software Peer-to-Peer está instalado. No mínimo os seguintes softwares deverão ser suportados nativamente:
  - BearShare
  - BitComet
  - BitTorrent
  - Deluge
  - Kazaa
  - Spotify
  - Transmission
  - uTorrent
- Para cada um dos softwares listados acima, a solução deverá ser capaz de analisar se o Peer-to-Peer está em execução;
- Para cada um dos softwares listados acima, a solução deverá ser capaz de matar o processo de Peer-to-Peer rodando (remediar o problema);
- Analisar se Personal Firewall está instalado. No mínimo os seguintes antivirus deverão ser suportados nativamente:
  - Mcafee Endpoint Security
  - Windows Personal Firewall
  - Sophos Client Firewall
  - Symantec Client Firewall
  - Symantec Endpoint Prodtection
  - Zone Labs ZoneAlarm
- Para cada um dos softwares listados acima, a solução deverá ser capaz de analisar se o firewall está em execução;

- Para cada um dos softwares listados acima, a solução deverá ser capaz de iniciar a execução de um personal firewall parado (remediar o problema);
- Analisar se software de armazenamento na núvem está instalado. No mínimo os seguintes softwares deverão ser suportados nativamente:
  - Amazon Cloud Drive
  - Apple iCloud Drive
  - Box
  - Dropbox
- Para cada um dos softwares listados acima, a solução deverá ser capaz de analisar se o software está em execução;
- Para cada um dos softwares listados acima, a solução deverá ser capaz de matar o processo de armazenamento na nuvem que está rodando (remediar o problema);
- Analisar se software de armazenamento na núvem está instalado. No mínimo os seguintes softwares deverão ser suportados nativamente:
  - CheckPoint Full Disk Encryption
  - BitLocker
  - Symantec Endpoint Encryption
- A solução deverá ser capaz de analisar continuamente os processos que estão executando em cada dispositivo
- A solução deverá ser capaz de matar um processo nativamente, configurando apenas o nome do processo;
- A solução deverá ser capaz de analisar continuamente os serviços que estão sendo executados no SO;
- A solução deverá ser capaz de analisar os patches do windows que estão faltando no SO.
- A solução deverá ser capaz de disparar um processo de atualização de patches automaticamente (remediação);
  - Deve ser capaz de forçar que busque direto da internet;
  - Deve ser capaz de forçar que busque de um servidor WSUS configurado;
- A solução deverá ser capaz de ler qualquer chave de registry do SO
- A solução deverá ser capaz de escrever chaves de registry do SO
- A solução deverá ser capaz de executar scripts localmente no SO do dispositivo sendo gerenciado
- A solução deverá ser capaz de identificar periféricos conectados ao Windows e categorizá-los (impressora, iPhone, etc via USB)
- A solução deverá ser capaz de identificar o domínio NetBIOS e a participação do dispositivo Windows no domínio;
- A solução deverá ser capaz de identificar os compartilhamentos de disco habilitados no Windows do dispositivo sendo gerenciado;
- A solução deverá ser capaz de analisar um arquivo do SO, comparando data, tamanho, versão e hash MD5.
- A solução deverá determinar a versão exata do Windows

▪ A solução deverá ser capaz de analisar e remediar estações Linux sem o uso de agente instalado na máquina. As funções abaixo deverão ser suportadas sem agente:
- Suportar no mínimo CentOS 5, 6 e 7;
- Suportar no mínimo Debian 8 e 9;
- Suportar no mínimo Fedora 18,19,20,21,22 e 23;
- Suportar no mínimo Red Hat Enterprise Linux 5, 6 e 7;
- Suportar no mínimo Red Hat Enterprise Linux Desktop 7;
- Suportar no mínimo Ubuntu 12, 13, 14.0.4, 15, 16.0.4, 18.0.4;
- A solução deverá ser capaz de identificar a versão exata do SO instalado;

- A solução deverá ser capaz de analisar um arquivo do SO, comparando data, tamanho, versão e hash MD5;
- A solução deverá ser capaz de determinar o hostname configurado no SO;
- A solução deverá ser capaz de determinar o nome do usuário cujo login está feito no SO;
- A solução deverá ser capaz de analisar continuamente os processos que estão executando em cada dispositivo
- A solução deverá ser capaz de matar um processo nativamente, configurando apenas o nome do processo;
- A solução deverá ser capaz de executar scripts localmente no dispositivo sendo gerenciado;

▪ A solução deverá ser capaz de analisar e remediar estações MacOS sem o uso de agente instalado na máquina. As funções abaixo deverão ser suportadas sem agente:
- Suportar no mínimo MacOS 10.6 a 13;
- A solução deverá ser capaz de identificar a versão exata do SO instalado;
- A solução deverá ser capaz de analisar um arquivo do SO, comparando data, tamanho, versão e hash MD5;
- A solução deverá ser capaz de determinar o hostname configurado no SO;
- A solução deverá ser capaz de determinar o nome do usuário cujo login está feito no SO;
- A solução deverá ser capaz de analisar continuamente os processos que estão executando em cada dispositivo
- A solução deverá ser capaz de matar um processo nativamente, configurando apenas o nome do processo;
- A solução deverá ser capaz de determinar todos os softwares instalados no dispositivo sendo gerenciado;
- A solução deverá ser capaz de analisar os patches do MacOS que estão faltando no SO.
- A solução deverá ser capaz de disparar um processo de atualização de patches automaticamente (remediação);
- A solução deverá ser capaz de executar scripts localmente no dispositivo sendo gerenciado;

▪ A solução deverá ser capaz de analisar e dispositivos IoT. No mínimo as seguintes funções deverão ser suportadas:
- A solução deverá classificar o dispositivo IoT quanto a sua função na rede (impressora, camera, catraca, automação, televisão, etc)
- A solução deverá ter uma base de dispositivos IoT pré-configurada com os dispositivos mais comuns;
- A solução deverá atualizar esta base periodicamente e de maneira independente da atualização do SO;
- A solução deverá permitir customizar entradas, categorizando dispositivos novos, diferentes ou exclusivos do ambiente sendo instalado;
- A solução deverá permitir fazer query SNMP ao dispositivo SNMP para determinar detalhes;
- Analisar consumo de energia PoE do dispositivo, e monitorar mudanças no consumo;
- Fazer tentativas de login com usuários conhecidos via telnet e ssh para determinar segurança de dispositivos IoT;
  - ♦ A solução deve possuir uma lista de credenciais comumente usadas;
  - ♦ A solução deve permitir a adição de uma lista de credenciais típicas no ambiente;

➢ **Ações de Controle;**
- ▪ A solução deverá permitir diversos métodos de se implementar controle.
- ▪ A solução deverá permitir mudança de VLAN da porta dos switches através de SNMP e/ou CLI;
- ▪ A solução deverá permitir mudança de VLAN da porta dos switches através de 802.1x em modo Proxy;

- A solução deverá permitir mudança de VLAN da porta dos switches através de 802.1x em modo Server;
- A solução deverá permitir configuração de ACL nos switches através de SNMP e/ou CLI;
- A solução deverá permitir configuração de ACL nos switches através de 802.1x dACL
- A solução deverá permitir um shutdown da porta dos switches através de SNMP e/ou CLI;
- A solução deverá permitir a restrição de conectividade do dispositivo através de um Virtual Firewall implementado pela porta de tráfego espelhado, sem alteração em configuração de nenhum elemento de rede;
- A solução deverá permitir o redirecionamento do acesso web de um dispositivo a um portal (Captive Portal) usando tráfego espelhado;
- A solução deverá permitir o redirecionamento do acesso web de um dispositivo a um portal (Captive Portal) usando DNS;
- A solução deverá permitir a desconexão de um usuário do Wireless através de SNMP e/ou CLI;
- A solução deverá permitir a desconexão de um usuário do Wireless através de 802.1x;
- A solução deverá permitir a mudança no perfil de conectividade de um usuário do Wireless através de SNMP e/ou CLI;
- A solução deverá permitir a mudança no perfil de conectividade de um usuário do Wireless através de 802.1x;
- A solução deverá permitir a mudança no perfil de conectividade de uma Máquina Virtual no VMWare ESX através da mudança do Port Group configurado na VM
- A solução deverá permitir a mudança no perfil de conectividade de uma Máquina Virtual no VMWare NSX através da mudança do Security Group configurado na VM
- A solução deverá permitir a mudança no perfil de conectividade de uma Máquina Virtual no VMWare NSX através da mudança do Security TAG configurado na VM
- Além dos métodos que interagem com a infraestrutura, a solução deverá ser capaz de gerar alertas. Estas alertas devem ser no mínimo:
  - Syslog;
  - E-mail a um endereço pré-configurado para aquele tipo de incidente;
  - E-mail ao usuário que que está logado no dispositivo no momento;

➢ **Gestão da Plataforma;**

- A gestão da plataforma deve ser via interface gráfica;
- Toda a gestão da plataforma deverá ser feita em uma única Console;
- Toda a comunicação entre a console e os appliances virtuais deve ser criptografado;
- A console deverá apresentar todos os dispositivos conectados e as características descobertas de cada dispositivo. As colunas de informações apresentadas devem ser customizáveis;
- As políticas devem ser configuradas via esta mesma console gráfica;
- Os dispositivos que cairem em cada regra da política deverão ser apresentados na própria console;
- Os dispositivos deverão ser organizados em grupos baseado em qualquer característica;
- A console deverá apresentar um inventário de dispositivos, organizando-os por tipo, função, usuário, Sistema operacional;
- As credenciais para acesso à console devem ser locais ou integradas às bases de usuários como Active Directory;
- A console deverá ter diferentes níveis de acesso, customizável por usuário ou por Grupo do AD;
- A console deverá apresentar um Dashboard interativo. Neste dashboard deverá ser possível apresentar visões de:
  - Porcentagem de dispositivo por tipo
  - Porcentagem de dispositivo por nível de Compliance
  - Número de dispositivos conectados ao longo do tempo
  - Número de dispositivos no Wifi vs cabeado

- Porcentagem de usuários Corporativos vs Convidados

ITEM 5 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE PROTEÇÃO DE ENDPOINT

- Estar dimensionada para 2300 endpoints.
  - Funcionalidades e requisitos específicos:
  - Deverá realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 7(x86/x64); Windows 8.1 (x86/x64) e Windows 10 (x86/x64);
  - Deverá realizar a análise de dados automatizando a construção de modelos analíticos, identificando padrões de malwares desconhecidos possibilitando a tomada de decisões com o mínimo de intervenção humana, não apenas antes da execução, mas também durante o tempo de execução.
  - Deverá possuir tecnologia de capaz de detectar variantes de malwares desconhecidos por similaridade de código e analise por comportamento de criptografia realizando o bloqueio do artefato em casos suspeitos;
  - Deverá possuir motores específicos para detecção e bloqueio de ameaças do tipo ransomware e mineradores de criptomoeda;
  - Deverá detectar, analisar e excluir códigos maliciosos, tais como: adware, backdoor, MBR malware, browser exploits, HackTool, PUA (Potentially Unwanted Application), Rootkit, Spyware, Trojan, TrojanClicker, TrojanProxy e TrojanSpy.
  - Deverá analisar em tempo real programas maliciosos em:
  - Processos em execução em memória principal (RAM);
  - Arquivos executados, criados e modificados, inclusive em sessões de linha de comando (DOS ou Shell);
    - Arquivos compactados com análise em até 6 camadas de profundidade;
    - Objetos em OLE com análise em até 10 camadas de profundidade;
    - Detectar ameaças do tipo exploit dentro de arquivos OLE;
  - Deverá analisar setor de boot de dispositivos de armazenamentos após plugado;
  - Deverá possibilitar a configuração do consumo de CPU que será utilizada para uma varredura manual e agendada em três níveis;
  - Deverá possuir cache persistente dos arquivos que outrora foram escaneados, para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
  - Deverá permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a garantir a alta disponibilidade na análise e detecção de novas ameaças, sem utilização do servidor de gerenciamento;
  - Deverá possuir a capacidade de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;
  - Deverá permitir o agendamento das atualizações automáticas e/ou incremental das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência no mínimo diária, semanal, hora e minuto;
  - Deverá permitir o rollback das atualizações das listas de definições de vírus e engines;
  - Deverá permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações;
  - As funcionalidades de Endpoint Protection Platform-EPP, tais como antimalware, web reputation, controle de aplicação, host IPS, host Firewall e DLP deverão possuir um unico agente.
- **Funcionalidades de Controle de Dispositivos:**
  - Deverá possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e execução, apenas leitura, e bloqueio total;
  - Deverá possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM e DVD, com as seguintes opções: acesso total, leitura e execução, apenas leitura, e bloqueio total;

- Deverá possuir a capacidade de controlar drives mapeados com as seguintes opções: acesso total, leitura e execução, apenas leitura, e bloqueio total;
- Deverá permitir o bloqueio de bluetooth, portas COM e LPT, interface IEEE 1394, infravermelho, modems e Wireless NICs e Print screen;

❖ **Funcionalidades de Host IPS e Host Firewall:**

- Deverá permitir três níveis de configurações: permitir todo o tráfego de entrada e saída, bloquear o tráfego de entrada e permitir tráfego de saída e bloquear todo o tráfego de entrada e saída
- Deverá permitir que todas as regras das funcionalidades de firewall, IDS e IPS de host possam ser configuradas em modo detecção ou prevenção;
- Deverá realizar verificações de segurança automáticas que aponte vulnerabilidades de sistemas operacionais e aplicações e atribuir automaticamente as regras de Host IPS para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;
- Deverá bloquear explorações de vulnerabilidades conhecidas e desconhecidas em caso de aplicações desatualizadas;
- Deverá proteger em casos de fim do suporte dos sistemas operacionais legados;
- Deverá avaliar e recomendar automaticamente os patches virtuais necessários para os endpoints;
- Deverá aplicar filtros de controles para alertar e bloquear tráfego específico, como mensagens instantâneas e mídia transmissão.
- Deverá impedir que backdoors de rede entrem na rede corporativa;
- Deverá apresentar via console de gerenciamento as informações das vulnerabilidades protegidas, organizando as vulnerabilidades por números de boletins de segurança da Microsoft, números CVE ou outras informações importantes;
- Deverá possuir engine de detecção para ameaças do tipo remote access trojan (RAT);
- Deverá prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host IPS, tais como Microsoft Windows, Skype, Microsoft Office, Windows Services, DNS Client, Oracle, DCERPC Services , RTMP Client, Web Client, Shellcode, TFTP Client, Port Mapper, SQL, PostgreSQL, Intel AMT, adobe, java,
- Deverá permitir a emissão de alertas via SMTP, SNMP e Syslog;
- Deverá permitir criação de regras de firewall dos protocolos TCP/UDP
- Deverá permitir criação de regras de firewall por inbound, outbound, protocolo, portas (específicas ou range) e IP (específicos ou range).

❖ **Funcionalidades de Controle de Aplicação**:

- Deve prevenir danos potenciais de aplicativos indesejados ou desconhecidos (executáveis, DLLs,
- aplicativos da App Store do Windows, drivers de dispositivo, painéis de controle e outros executáveis portáveis (PE) arquivos).
- Deverá permitir a criação de políticas de segurança personalizadas;
- Deverá possiblitar permitir ou bloquear uma aplicação através do nome, caminho, expressão regular, hash ou certificado do aplicativo;
- Deverá possuir categorias de aplicações e permitir a utilização de múltiplas regras de controle de aplicações;
- Deverá permitir bloquear todas as aplicações do endpoint, exceto aqueles permitidos (lista branca);
- Deverá possuir atualização das categorias de maneira automatizada.
- Funcionalidades de Proteção contra Vazamento de Informações:
- Deverá permitir restrinjir o uso de drives USB, dispositivos móveis conectados via USB, gravadores de CD / DVD, armazenamento em nuvem e outras mídias removíveis com controle de dispositivo granular e políticas de prevenção de vazamento de dados;
- Deverá possuir a capacidade de detectar informações, com base em: palavras-chave, expressões regulares e atributos dos arquivos.
- Deve possuir a capacidade de detectar informações, em documentos nos formatos: Microsoft (.doc, .dot, .docx, .dotx, .docm, .dotm), Lotus Ami Pro (.sam), RTF (.rtf), WordStar (.wsd), Microsoft Write (.wri), Adobe PDF (.pdf), HTML (.htm), XML (.xml), Xerox DocuWorks (.xdw, .xbd), Ichitaro (.jtd), WordPerfect (.wp, .wpd), 7-Zip (.7z), ARJ (.arj), bzip2 (.bz2), compress (.Z), GZ (.gz), LHA

(.lzh), Microsoft Compiled HTML Help (.chm), Microsoft Outlook (.msg), Microsoft Outlook (.pst), Microsoft Outlook Express (.dbx), MIME (.eml), PAK/ARC (.arc), PGP Keyring (.pgp), RAR (.rar), TAR (.tar) e Zipped File (.zip), Quattro (.qpw, .wb3, .wb2, .wb1, .wq1), Lotus 1-2-3 (.123, .wk1, .wk3, .wk4, .wke, .wks), Microsoft Excel - (.xls, .xlw, .xlsx, .xltx, .xlsb, .xltm, .xlsm, .xlc, .xlam), Microsoft PowerPoint (.ppt, .pot, .pps, .pptx, .potx, .ppsx, .potm, .pptm, .ppsm) ,Microsoft Visio (.vdx, .vsd, .vss, .vst, .vsx, .vtx, .vdw)

- Deve possuir a capacidade de detectar arquivos multimédia nos formatos: AVI (.avi), MIDI (.mid), MPEG (.mpeg), Apple QuickTime (.mov), Adobe Flash (.swf) e Microsoft Wave (.wav);
- Deve possuir a capacidade de detectar arquivos compactados criptografados nos formatos .rar e .zip;
- Documentos criptografados (.accdb, .doc, .docx, .pdf, .ppt, .pptx, .wb1, .wb2, .wq1, .wpd, .xls, .xlsx)
- Deve possuir a capacidade de detectar documentos criptografados nos formatos: .accdb, .doc, .docx, .pdf, .ppt, .pptx, .wb1, .wb2, .wq1, .wpd, .xls e.xlsx
- Deverá permitir a criação de modelos personalizados para identificação de informações;
- Deverá possuir a capacidade de identificar e bloquear informações no mínimo para os seguintes meios de transmissão: Cliente de e-mail; Protocolos FTP, HTTP, HTTPS, aplicações de mensagens instantâneas, protocolo SMB, Webmails, CD / DVD, aplicações peer-to-peer, impressora, USB, software de sincronização (ActiveSync), área de transferência do Windows e serviço de armazenamento em nuvem;

❖ **Funcionalidades de Criptografia:**

- Possuir módulo de criptografia para endpoints (desktops e notebooks), permitindo criptografia para: disco total, pastas e arquivos e mídia removível.
- A funcionalidade de criptografia poderá ser entregue em outro agente.
- Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;
- Possuir a capacidade de exceções para criptografia automática;
- Possuir compatibilidade de autenticação por múltiplos fatores;
- Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;
- Possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;
- Possuir mecanismos para wipe (limpeza) remoto;
- Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);
- Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;
- O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);
- Permitir, em nível de política, a indicação de pastas a serem criptografadas;
- Possibilitar que cada política tenha uma chave de criptografia única;
- Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;
- Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;
- Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação.

❖ **Módulo para proteção de dispositivos móveis**

- O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais: iOS e Android;
- Deverá possuir gerenciamento de dispositivos móveis (MDM), gerenciamento de aplicações móveis e Serviços de Reputação de Aplicativos Móveis;
- Deverá detectar e bloqueiar aplicativos maliciosos e arquivos de dados nos dispositivos;
- Deverá fornecer visibilidade do número, tipos,e configuração de dispositivos acessando o ambiente corporativo;
- Deverá fornecer gerenciamento de inventário e relatórios possibilitando a visibilidade dos aplicativos usados entre dispositivos;

- Deverá permitir o gerenciamento e bloqueio de tipos específicos de aplicativos com base em categorias;
- Deverá permitir o bloqueio de conteúdos e sites da Web mal-intencionados usando serviços de reputação da Web;
- Deverá detectar ataques no dispositivo via aplicações de rede, portas e serviços, usando o firewall e IDS
- Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;
- Deverá monitorar, bloquear e registrar chamadas, SMS e MMS enviados;
- Deverá permitir o registro,provisionamento e desprovisionamento remotamente do dispositivos com a rede corporativa: VPN, Exchange ActiveSync e Wi-Fi;
- Deverá permitir o controle dos dispositivos e implantar políticas relevantes através do International
- Mobile Equipment Identity ou IMEI, Wi-Fi e endereço MAC;
- Deverá possuir proteção antimalware para Android;
- Deverá ser capaz de realizar escaneamento de malwares em tempo real;
- Deverá possuir a capacidade de detectar e bloquear de spam proveniente de SMS;
- Deverá possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;
- Deverá possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;
- Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;
    - Controle da política de segurança de senhas, com critérios mínimos de:
    - Bloqueio automático da tela;
    - Bloqueio por tentativas inválidas;
    - Quantidade de caracteres;
    - Quantidade de números;
- Deverá possibilitar o controle de acesso à seguinte lista de funções dos dispositivos Android: Bluetooth, camera, cartão de memória, Wlan/wifi, ancoragem e modo desenvolvedor;
- Deverá possibilitar o controle de acesso à seguinte lista de funções dos dispositivos IOS: camera, Facetime, Siri, jogos, discagem por voz, iCloud, emparelhamento Apple Watch,
- Deverá Permitir proteção dedicada contra vazamento de informações voltadas a clientes Microsoft Skype for Business e Microsoft Lync Server.
- Permitir proteção contra vazamento de informação em Office 365 em nuvem, Box, Dropbox, OneDrive for Business, Google Drive utilizando estruturas em nuvem para o gerenciamento do mesmo.

❖ **MÓDULO DE PROTEÇÃO WEB**

- Gerenciamento via console web
- Deve possuir a certificação da VmWare para Software Appliance ou a possibilidade de instalação no formato de Bare Metal, formato no qual depende da homologação do hardware por parte do fabricante;
- Virtual Appliance: Suportar VmWare ESX e ESXi 5.5 ou superior e Microsoft Hyper-v 2.0 Windows Server 2012 R2 ou superior.
- A solução Virtual appliance deve fornecer junto da sua ISO de instalação um banco de dados;
- Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e activex maliciosos, sem a necessidade de um agente ou software adicional;
- Toda a solução deverá ser do mesmo fabricante;
- Permitir criar políticas de verificação baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;
- Permitir um controle de quota em Megabytes ou por tempo para o acesso à internet, por usuário ou grupo de usuário, por dia, semana e mês;
- Permitir a utilização da ferramenta em modo Transparent Bridge, Forward Proxy, Proxy Reverso;
- Possuir suporte ao protocolo ICAP e WCCP,

- Utilizar os seguintes serviços de diretório: Microsoft Active Directory, Linux OpenLDAP Directory e Sun Java System Directory Server 5.2;
- Permitir configurar os usuários que terão acesso à internet, baseado em seus logins, endereço IP e range IP;
- Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;
- Permitir a geração de relatórios, de forma manual ou agendada, com todos os eventos da ferramenta: códigos maliciosos, paginas acessadas, URL's bloqueadas, atividade por período e spywares detectados;
- Atualização automática das vacinas de forma incremental e da versão do software;
- Gerenciamento centralizado com a mesma console que administra o resto da solução;
- Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;
- Possuir um tratamento especial para Java Applets, onde esse é verificado quanto à sua assinatura e certificado, podendo tomar ações distintas para cada combinação entre elas, podendo ainda configurar que operações um Applet pode executar na maquina do usuário e como seus certificados serão validados;
- A análise Antimalware da tecnologia deve ser realizada em Real Time, possibilitando uma ação imediata quando identificada uma ameaça;
- O tratamento da análise de tráfego da tecnologia quando detectado um vírus deve ser de limpar, deletar ou quarentenar;
- Possuir um tratamento especial para Activex, onde esse é verificado quanto à sua assinatura, e podendo tomar ações distintas para elas e como seus certificados serão validados;
- Permitir configurar os certificados digitais que são seguros, colocando também os não seguros em uma lista negra;
- A tecnologia deve ser capaz de identificar e bloquear conexões com redes zumbis (Botnets);
- Possuir banco de dados de URL categorizados em, no mínimo, 80 categorias e tomar as seguintes ações para o acesso a estas categorias: permitir, bloquear, monitorar, alertar, tempo de acesso e acesso com senha, este banco de dados deve estar hospedado na Internet para que se tenha uma atualização mais rápida das categorias.
- A tecnologia deve possuir integrado a mesma solução um Cache de páginas HTTP que visa a melhorar o desempenho da navegação.
- A configuração do tamanho dos objetos que serão armazenados no cache devem passíveis de modificação pelo Administrador da tecnologia;
- Possibilidade de permissão de acesso websites definidos nas categorias em períodos pré-determinados;
- Possuir integração com Safe Search do Google e do Yahoo
- Possuir análise de malware sobre o tráfego HTTPS;
- Possibilidade de permitir customizar notificações para o usuário de acordo com a política de acesso definida:
  - -HTTPS Access Denied
  - -HTTPS Certificate Failure
  - -HTTP/HTTPS Scanning
  - -HTTP/HTTPS Blocked File Type
  - -URL Blocking
  - -FTP Scanning
  - -FTP Blocked File Type
  - -IntelliTunnel (bloqueio de Instant Messaging)
  - -Applets and ActiveX Instrumentation
  - -Pattern File Updates
  - -URL Filtering and Scan Engines Update
- Possuir recurso para permitir / bloquear no mínimo 420 aplicações diferentes e este recurso deve funcionar no mínimo em dois modos de instalação (Forward Proxy e Bridge)

- Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey, ...)
- Possuir recurso de Web Reputation (reputação de HTTP), integrada com a solução de antivírus, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- Deve possuir a funcionalidade de replicar as configurações entre outros servidores de proteção do gateway HTTP através de uma tecnologia auxiliar de centralização de logs, reports e configurações.
- Deve possuir capacidade de criar os seguintes perfis de acesso a console de gerencia: Administrador, Auditor e Reports
- Possuir ferramenta integrada para Backup e restore das configurações da solução.
- A tecnologia deve contemplar a funcionalidade de Data Loss Prevention, afim, de evitar o vazamento de informações;
- A solução deve contemplar templates contra vazamento de informações que atendam regulamentações de compliance.
- A tecnologia deve possibilitar a criação de novos templates que visam a customização da tecnologia, afim, de proteger dados específicos;
- A tecnologia deve permitir o acesso a redes sociais restringindo jogos e a possibilidade de submeter posts;
- A geração dos relatórios pode ser realizada através de uma tecnologia Standalone, afim, de garantir base de dados diferentes entre reports e políticas de configurações de acesso à internet através do proxy;
- O relatórios deve permitir que a partir da sua console seja possível submeter configurações das políticas de acesso à internet entre diversas instâncias da tecnologia de WEB Gateway;
- O relatórios deve possuir no mínimo 50 tipos de relatórios pré-definidos, que tragam visibilidade de acesso: URLS mais acessadas, usuários que mais acessam a internet, acesso por categoria do web site, consumo de banda e violações de regra;
- O relatórios deve disponibilizar uma Dashboard de visualização dos acessos dos usuários ao WEB Gateway em tempo real;
- A tecnologia standalone de relatórios deve permitir que geração seja agendada e submetida por e-mail;

ITEM 6 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE GESTÃO DE VULNERABILIDADE E APLICAÇÕES

❖ **CARACTERÍSTICAS GERAIS**

- A solução deve ser licenciada para realizar varreduras (*scans*) de vulnerabilidades, avaliação de configuração e conformidade (*baseline* e *compliance*) e indícios e padrões de códigos maliciosos conhecidos (*malware*);
- A plataforma de gerenciamento deverá ser instalada nas dependências do cliente e deverá ser compatível para instalação nos seguintes sistemas operacionais:
  - Red Hat Enterprise Linux 6;
  - Red Hat Enterprise Linux 7;
  - CentOS 6, 64-bit;
  - CentOS 7, 64-bit;
- A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
- Deve ser licenciado para realizar o scan em 2048 IPs.

- A solução deve ser licenciada para no minímo 10 scanners ativos;
- A solução deve ser licenciada para o uso de no minímo 10 sensores passivos de rede para realizar o monitoramento em tempo real;
- A solução de gerenciamento deverá permitir hardening via controles SELinux para impedir explorações no servidor;
- Deve ter a possibilidade de armazenar localmente a base de dados de vulnerabilidades;
- Deve ser capaz de identificar no minímo 51.000 CVE´S;
- Deve permitir a autenticação com certificados SSL, smart cards, PIV (Personal identity verification) e common access cards (CAC);
- A solução deve fornecer, sem configuração adicional e em instalação padrão, pelo menos 90 dashboards diferentes para análise das informações coletadas em varreduras;
- Deve possibilitar, por meio da console central de gerenciamento, no mínimo 3 (três) métodos de escaneamento:
  - Scan ativo;
  - Scan com uso de agentes;
  - Scan passivo;
- Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv2 score;
- A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
- O algoritmo de priorização deve analisar vulnerabilidades presentes na National Vulnerability Database (NVD);
- A solução deve ser capaz de aplicar algoritimos de inteligência artificial(Machine learning) para analizar mais de 120 características relacionadas a vulnerabilidades;
- Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial;
- Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo;
- O sistema de pontuação e priorização de vulnerabilidades deve avaliar no minímo as seguintes características:
  - CVSSv3 Impact Score;
  - Idade da Vulnerabilidade;
  - Número de produtos afetados pela vulnerabilidade;
  - Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;
  - Lista de todas as fontes (canais de mídia social, dark web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;
- A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação);
- Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras;
- API exposta e disponível para integração com outras tecnologias, como por exemplo sistemas de controle de chamados de TI (BMC Remedy, ServiceNow, ServiceDesk Plus e afins);
- A solução deve ser capaz de integrar com soluções de gestão de acessos privilegiados (PAM),

tais como CyberArk, SEenha Segura, Centrify, BeyondTrust ou CA Technologies;

- A solução deve possuir sistema de alertas com ações definidas para cada alerta, entre elas:
  - Criação de Ticket no sistema de chamados interno da solução;
  - Envio de e-mail;
  - Envio de mensagem syslog;
  - Iniciar scan sob demanda com base em condições definidas;
  - Gerar relatório sob demanda filtrado nas condições do alerta;
- A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
- A solução deve ser licenciada para no minímo 2000 agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional.
- Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
- Os agentes devem realizar conexões para o sistema centralizado de gerenciamento de agentes e scanners, dentro do ambiente do órgão, sem a necessidade de acessar a Internet;
- A solução deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
- No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;
- A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan;
- Deve permitir a comunicação com instâncias de monitoramente de rede para a descoberta de vulnerabilidades de software em tempo real de maneira não intrusiva;
- A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- A solução deve possuir mecanismos de correlação de eventos observados em logs fornecidos de diferentes dispositivos de rede em conjunto com a monitoria passiva para detecção de comportamento malicioso e enriquecimento de resultados de varreduras;
- Deve ser possível determinar em tempo real (sem a necessidade de um scan ativo) quais portas estão abertas em determinado ativo;
- A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
  - Bancos de dados;
  - Hypervisors;
  - Dispositivos móveis;
  - Dispositivos de rede;
  - Endpoints;
  - Tablets;
  - Aplicações;
- Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;

- A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- Deve ter a capacidade de guardar em tempo real informações de GET,POST e Download que trafeguem na rede;
- A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;
- Deve identificar informações pessoais (Exemplo: CPF, Rg e etc) trafegando pela rede;
- A solução deve ser capaz de detectar o uso de serviços em nuvem como Dropbox, Salesforce e AmazonCloud;
- Deve fazer a enumeração passiva de arquivos compartilhados via FTP;
- Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente;
- A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
  - Sistema Operacional, Endereço IP, DNS, NetBIOS Host, NetBIOS Workgroup, MAC, SSH Fingerprint, Porta TCP e/ou UDP, Dias desde a descoberta do ativo, Exploit disponível, XREF, Hosts com Antivirus Desatualizado, Host com Browsers específicos (Opera, Chrome, Safari, Firefox), Hosts com Browser TOR instalado, Hosts com software VOIP instados e Hosts com clientes SQL instalados;
- A solução deve agrupar as informações encontrados no ambiente para no minímo:
  - Sumário de Ativos;
  - Sumário por CVE;
  - Sumário por Vulnerabilidade;
  - Sumário por protocolo;
  - Sumário por Boletins Microsoft;
  - Sumários por IP;
  - Sumário por nome DNS;
  - Lista de todos os sistemas operacionais encontrados;
  - Lista com todos os softwares encontrados;
  - Lista com todos os serviços;
  - Lista de Web Clients;
  - Lista de Web Servers;
- **Relatórios**
  - Deve ser capaz de executar relatórios manuais e periódicos de acordo com a frequencia estabelecida pelo administrador;
  - A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e RTF;
  - A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
  - Deve suportar a criação de relatórios criptografados(protegidos por senha configurável) ;
  - A solução deve suportar o envio automático de relatórios para destinatários específicos;
  - Deve ser possível definir a frequência na geração dos relatórios para no minímo: Diário,

Mensal, Semanal e Anual;

- Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- A solução deve possuir relatórios pré configurados com as seguintes informações:
  - Hosts verificados sem credenciais;
  - Top 100 Vulnerabilidades mais critícas;
  - Top 10 Hosts infectados por Malwares;
  - Hosts exploráveis por Malwares;
  - Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
  - Vulnerabilidades críticas e exploráveis;
  - Máquinas com vulnerabilidades que podem ser exploradas;
  - Relatório contendo um resumo geral de vulnerabilidades detectadas de forma passiva(Monitoramento passivo);
  - Relatório detalhando eventos com indicativos de intrusões na rede e vulnerabilidades que podem deixar a rede expostas a futuras invasões;
  - Informações sobre os hosts com maio número de vulnerabilidades contendo no minímo as seguintes informações: IP, Nome Netbios, DNS, Sistema Operacional e MAC Address;
  - Relatório de requisitos recomendados pelo NIST SP 800-171;
  - Relatório contendo indicadores de conformidade com o NIST 800-53;
  - Relatório detalhado contendo informações sobre logs de aviso e erro identificados no ambiente;
  - Lista dos principais hosts e sistemas operacionais com patches de segurança ausentes;
  - Relatório com informações sobre vulnerabilidades críticas e exploráveis que foram detectadas na rede;
  - Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um *exploit* disponível e informações do ativo.
- A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;
- Deve permitir a customização de relatórios podendo incluir no minímo as seguintes opções:
  - Marcad'agua customizada em cada página do relatório;
  - Customização de logo;
  - Header pré-definido;

❖ **Varreduras**

- ➢ A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- ➢ A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
- ➢ A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para

monitoramento contínuo de configurações e vulnerabilidades;

- A solução deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
- No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;
- A solução deve ser configurável para permitir a otimização das configurações de varredura;
- A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
- A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- A solução deve ser capaz de realizar pesquisas de dados confidenciais;

❖ **Auditoria de Configuração**

- A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
- A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
- A solução deve fornecer dashboards visuais, em formato de placar, contendo as verificações e controles de segurança verificados com indicação de sucesso ou falha, com base nos principais frameworks de segurança reconhecidos pela indústria, tais como:
  - SANS 20 Critical Security Controls;
  - ISO 27000;
  - NIST Cybersecurity Framework;
  - PCI Data Security Standard;
  - CIS Benchmark L1 e L2;
- A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;
- A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos sistemas operacionais Microsoft Windows e Linux;
- Deve suportar os seguintes Frameworks de segurança : ISO/IEC 27001/2, NIST Cybersecurity Framework (CSF), NIST 800-53, NIST 800-171, NERC CIP e GLBA.

❖ **VARREDURA DE APLICAÇÕES WEB**

- A solução deve realizar varreduras de vulnerabilidades em 10 FQDN em aplicações Web simultaneamente, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10;
- A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- A solução deverá capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

- Deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);
- Deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
  - Cookies, Headers, Formulários e Links;
  - Nomes e valores de parâmetros da aplicação;
  - Elementos JSON e XML;
  - Elementos DOM;
- Deverá também permitir somente a execução da função *crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação;
- Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
- Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
- Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
- Deve ser capaz de instituir no mínimo os seguintes limites:
  - Número máximo de URLs para crawl e navegação;
  - Número máximo de diretórios para varreduras;
  - Número máximo de elementos DOM;
  - Tamanho máximo de respostas;
  - Tempo máximo para a varredura;
  - Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
  - Número máximo de requisições HTTP por segundo;
- Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- Deve suportar o envio de noticações por email e SMS;
- Deverá ser compatível com avaliação de web services REST e SOAP;
- A solução deve suportar os seguintes esquemas de autenticação:
  - Autenticação Básica (Digest);
  - NTLM;
  - Autenticação de Cookies;
  - Autenticação através de Selenium;
- Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;
- Deve ser capaz de customizar parâmetros Selenium como: delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
- A solução deve ser capaz de exibir os resultados das varreduras de fprma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
- Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
- A solução deve ser capaz de realizar varreduras nos seguintes componentes:
  - WordpPess;
  - Blog Designer Plugin for Wordpress;

- Event Calendar Plugin for Wordpress;
- Convert Plus Plugin for Wordpress;
- AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts;
- Atlassian Confluence, Atlassian Crowd e Atlassian Jira;
- Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI

ITEM 7 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO COFRE DE SENHA E GESTÃO DE ALTAS CREDENCIAIS

- Suportar, no mínimo, 3.000 sessões simultâneas;
- Suportar, no mínimo, 650.000 horas de armazenamento de gravação de sessões.
- Os usuários geridos pela solução poderão estar conectados simultaneamente;
- Solução para armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux/Unix, Windows (Incluindo contas de serviço como COM+ e IIS), Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede, totalizando 150 usuários ou 5.400 dispositivos;
- Prover autenticação transparente no sistema-alvo ou dispositivo de rede. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso;
- Eliminar credenciais inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e invisíveis aos desenvolvedores e equipe de suporte de TI;
- Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;
- Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;
- Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;
- Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;
- Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;
- Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;
- Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução;
- Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;
- Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;
- Provisionamento de usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede;
- Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;
- Permitir o monitoramento on-line do uso das contas e desligamento da sessão;
- Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade;

- Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos e certificados;
- Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido;
- Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;
- Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;
- Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato ".csv";
- A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH, API REST HTTP/HTTPS;
- Caso seja necessária alguma integração com aplicações legadas e/ou integrações com o ambiente interno, o mesmo deverá ser customizado e desenvolvido pelo fabricante.
- Extrair informações do servidor localizado nos Data Centers remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas;
- Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução;
- No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades;
- Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local devem ser automaticamente replicadas para os outros servidores de redundância, de forma assíncrona e com delay máximo de 50ms;
- Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (Hash), Path e endereço IP do host ou conjunto de hosts a serem acessados pela solução;
- Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;
- Possibilidade de implementação SNMP sobre IPv6;
- Implementar a especificação IETF RFC 2460, referente ao protocolo IPv6;
- Possibilidade de implementar a MIB II, conforme RFC 1213;
- Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local;
- Controlar a elevação de privilégio em estações de trabalho (endpoints), a fim de executar aplicações autorizadas que necessitem deste privilégio (“Run As”);
- Possibilidade de mapear compartilhamentos de rede com um usuário administrador, diferente do usuário logado na máquina (“Mapear como”).
- Possibilidade de validação do acesso ao cofre apenas usuários com agente instalado no desktop para garantir e restringir o acesso de máquinas externas.
- Caso seja separado em componentes, nenhum deles deve conter senhas em texto claro para autenticação;
- Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH;
- Liberação de acesso para execução de tarefas específicas em plataforma SSH e TELNET.
- Tanto appliances quanto sistemas operacionais devem ser “hardenizados” e protegidos com firewall interno e detecção de intrusão;

❖ **Gestão de Usuários e Perfis**

- Cadastro de usuários com informações de nome, e-mail e departamento no mínimo.
- Cadastro de perfis de usuários;
- Segregação de funções por perfis de acesso;

- Flexibilidade para criação de quaisquer perfis novos, com diversas combinações de telas e funcionalidades de acordo com a necessidade do negócio sem intervenção do fornecedor;
- Importação automática de contas de usuários do AD;
- Importação automática de contas de usuários do LDAP;
- Gerenciamento de Grupos e Perfis de acesso integrados aos grupos de AD.

❖ **Autenticação de Usuários**
- Autenticação local através de usuários e senha;
- Autenticação centralizada integrada com LDAP, LDAPS para MS AD com múltiplos DCS;
- Autenticação centralizada integrada com TACACS;
- Autenticação centralizada integrada com RADIUS;
- Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;
- Duplo fator de autenticação nativo para acesso web ou através de client;
- Gestão de autenticação com múltiplos autenticadores simultaneamente.

❖ **Cadastro de Ativos**
- Cadastro de equipamentos parametrizado manualmente;
- Atributos como Marca, Modelo, Fabricante, Localidade, Grupo abertos para configuração do administrador da ferramenta independente do fabricante.
- Cofre de Credenciais
- Sistema seguro de armazenamento de credenciais e senhas;
- Armazenamento de senhas criptografadas com padrões de criptografias fortes como AES 256 ou superior;
- Consolidação periódica de senhas para identificar senhas que foram alterados em sistema gerenciados;
- Envio de alerta por SIEM de senhas que não estejam iguais ao cofre.

❖ **Cofre de Informações privilegiadas**
- Armazenamento de certificados digitais;
- Armazenamento de senhas pessoais;
- Alerta de vencimento de informações armazenadas;
- Logs de alteração de informações privilegiadas;
- Permissão para compartilhamento de informações com outros usuários.

❖ **Gravação de logs (Vídeos e Comandos)**
- Gravação de Vídeo das sessões realizadas através de webproxy ou proxy transparente em formato otimizado;
- Gravação de comandos digitados em ambientes RDP e SSH;
- Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;
- Exportação de sessão em formato vídeo;
- Busca de registro de sessão por usuário, sistema alvo, ip alvo, data e hora;
- Busca por comandos e entradas de teclado digitados em plataforma Linux;
- Busca de comandos e entradas de teclado em plataforma Windows;
- Gravação de Logs de Input e Output de comandos;
- Sem necessidade de agentes locais para gravação de sessão;
- Armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:
- Identificação do usuário que realizou determinado acesso a um dispositivo;
- Identificação de quem aprovou o acesso do usuário;
- Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto.
- Prover, ao menos, os seguintes filtros para a recuperação de logs: Usuário; Sistema-alvo acessado, Tipo de atividade, Intervalo de tempo (data/hora/minuto inicial e final);
- Permitir o acompanhamento on-line de sessões remotas pelo administrador e desligamento da sessão remotamente;

❖ **Bloqueio de Comandos e Controle de Privilégios**

- Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - Baseado em blacklist;
- Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - Baseado em whitelist;
- Possibilidade de bloqueio e auditoria de comandos específicos;
- Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;
- Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;
- Marcação de pontuação de comandos de acordo com nível de risco de cada comando.

❖ **Rotação de senhas**

- Troca automática de senhas para Servidores (Unix, Linux, Windows), Bancos de Dados (MS SQL, ORACLE, MYSQL, PostgreSQL), Aplicações Web, Dispositivos de Rede, Mainframe;
- Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;
- Flexibilidade para configuração de força de senha gerada;
- Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;
- Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;
- Armazenamento de histórico de senhas por equipamento;
- Registro de troca executadas;
- Relatório de acompanhamento de trocas;
- Relatório de erros de trocas;
- Alertas de falha ou sucesso de trocas;
- Possibilidade de reconfiguração de scripts de troca por configuração;
- Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca;
- Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;
- Templates com linguagem acessível e fácil interpretação;
- Fluxo de aprovação de alteração de Template para evitar fraudes;
- Rastreabilidade de Alteração de Template;
- Troca de senhas em aplicações HTTP/HTTPS com templates.

❖ **Análise de Comportamento**

- Análise de sessão de usuário baseado em histórico de comportamento. Análise mínima das variáveis de estações origem, estações destino, credenciais, horários, duração de sessão;
- Identificação de comportamento diferenciados com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG;
- Análise de sessão de usuários com pontuação de comando críticos com alertas de anormalidade em relatórios em tela ou alertas para SIEM/SYSLOG;
- Dashboards gráficos com informações sobre riscos e ameaças.

❖ **Dashboards e Relatórios**

- Relatórios de operação com lista e usuários cadastrados, equipamentos cadastros, credenciais cadastradas;
- Relatórios PCI;
- Relatórios de Gestão de Evidências;
- Relatórios de Auditoria;
- Relatórios de Alertas;
- Exportação para Excel (.csv);
- Dashboard de utilização;
- Dashboard de conexões;
- Dashboard de utilização de sessões;
- Dashboard de sessão;

- Dashboard de usuário;
- Dashboard de servidor;
- DashBoard de estação de acesso.
- Controle de Elevação de Privilégios em Endpoint (Windows)
- Para plataforma Windows possui a possibilidade de um agente local capaz de iniciar aplicações injetando credenciais automaticamente;
- Permite a função e “Run As” para elevação de privilégio para executar aplicações que requerem privilégios;
- Mapeamento de compartilhamento de rede com usuário diferente do usuário logado na máquina (“Mapear como”);
- As aplicações fazem parte da lista de uma lista autorizada;
- Este tipo de acesso não revela senha ao usuário;
- Não faz a gravação de sessão;
- Faz a gravação de logs no cofre.

❖ **Central Gerenciamento**

- Console central de gerenciamento de aplicação com capacidade para:
- Criação de usuários;
- Busca de sessão gravada;
- Busca de Consulta de senhas;
- Gestão de políticas de acesso centralizadas;
- Cadastro de dispositivos centralizados.

❖ **Ambiente de instalação**

- A solução deve ser baseada em appliance virtual ou físico, atendendo as seguintes especificações:
- Caso o banco de dados e/ou Sistema Operacional utilizado seja de terceiros (exemplo: ORACLE/SQL ou Windows), a solução deverá ser entregue com licenças de software e garantia que a compatibilize com a solução;
- Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação, sem custos adicionais para a CONTRATANTE;
- Não haver necessidade de utilização de ferramentas de terceiros para completar a solução, ou seja, um fabricante único que atenda todas as necessidades de um Cofre de Senhas.
- Da Arquitetura de Implantação da Solução
- A solução deve ser licenciada e implantada de modo a atender, no mínimo, aos seguintes requisitos de arquitetura: Ser instalada em 02 (duas) localidades;
- Para as soluções ofertadas em virtual appliance ou máquina virtual, os recursos de hardware serão fornecidos pela CONTRATANTE;
- Para que a solução continue funcionando localmente mesmo com a falha de um nó de cada elemento, em cada uma das 02 (duas) localidades, no mínimo os seguintes elementos devem ser instalados em regime de alta disponibilidade:
  - Cofre de senhas (entendido como o elemento da solução que controla as credenciais de acesso, incluindo a interface de acesso dos usuários à solução);
  - Gateway/Proxy de Sessão (elemento que provê e controla o acesso privilegiado monitorado aos ativos de TI);
  - A solução deve replicar as configurações nas 02 (duas) localidades, de modo que, no evento de falha total de seus elementos instalados em uma localidade, a solução continue disponível via uso dos elementos da outra localidade;
- O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é:
  - Site principal: Ativo;
  - Site secundário: Ativo;
- O acesso primário (em situação normal) dos usuários à solução deve ser sempre via os elementos instalados em sua rede local.
- Caso a solução fornecida do tipo appliance (hardware), devem ser fornecidos pela CONTRATADA, no quantitativo necessário para atender aos requisitos de arquitetura e alta disponibilidade

apresentados, com todas as licenças válidas, com garantia igual ao do objeto desta contratação e sem custos adicionais para a CONTRATANTE.

- Embora não esteja previsto no projeto inicial da solução, a composição do objeto deverá suportar, arquitetura redundante de alta disponibilidade em nuvem, conectada por meio de interface Ethernet, em modo Warm Standby.

ITEM 8 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE CRIAÇÃO DE CORREÇÃO TEMPORÁRIA PARA NOVAS VULNERABILIDADE

- Estar dimensionada para 300 servidores.
  - Funcionalidades de Gerenciamento:
  - Permitir o envio de notificações via SMTP;
  - Permitir o envio de registros de logs a um servidor remoto;
  - Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;
  - Permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;
  - Permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
  - Permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;
  - Armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados: PostgreSQL, Microsoft SQL Server e Oracle Database;
  - Permitir a definição de permissionamento, no mínimo, para os modos de visualização e edição de políticas;
  - Permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;
  - Possuir dashboards para facilidade de monitoração, as quais poderão ser customizados pelo usuário;
  - Possuir a capacidade de criar políticas de forma global para todas as máquinas virtuais, por perfis e individualmente para cada host;
  - Permitir a criação/utilização de tags pré-definidas para o agrupamento e aplicação de políticas aos hosts segundo características comuns;
  - Permitir o envio de eventos da console via SNMP;
  - Permitir o rollback de atualização de regras pela console de gerenciamento;
  - Gerar pacote de auto-diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
  - Possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;
  - Possuir a capacidade de classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.
  - A solução deverá permitir o seu gerenciamento agrupando os hosts gerenciados em pastas inteligentes, possibilitando organização de grupos de hosts para a aplicação de políticas;
  - O agrupamento de hosts deverá ser no mínimo pelos seguintes parâmetros:
  - Hostname;
  - Sistema Operacional;
  - Docker Host;
  - Politica de Configurações;
  - Active Directory Name/Folder.
  - Requisitos mínimos:
  - Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware, e HyperV;

- A solução deverá permitir gerenciar políticas de segurança em múltiplas plataformas e sistemas operacionais, para hosts físicos, virtuais ou em nuvem (Vcloud, AWS ou Azure), todos em uma única console centralizada e do mesmo fabricante;
- Para cada plataforma de virtualização haverá uma forma diferente de integração, com ou sem agente, preservando a capacidade de implementação das funcionalidades da solução.
- Conter os seguintes módulos para a proteção de Servidores físicos, virtuais ou em nuvem:
  - Módulo Antimalware contendo as funcionalidades de:
    - Anti-malware;
    - Reputação Web;
    - Behaviour Analysis;
    - Módulo de segurança de rede, contendo as funcionalidades de:
    - Firewall;
    - Inspeção de Pacotes com virtual Patching (HIPS/HIDS);
- Módulo de segurança e integridade do sistema, contendo as funcionalidades de:
  - Controle de Aplicações;
  - Monitoramento de Integridade;
  - Inspeção de Log's;
- Para hosts gerenciados de Docker container deverá permitir a aplicação de regras de IPS/IDS e Anti-malware;
- Permitir a implantação dos módulos de segurança supracitados, no mínimo para os seguintes sistemas operacionais: Windows Server 2003, 2008, 2012 e Windows 2016;
- Sistemas Operacionais Linux, no mínimo para as distribuições: Red Hat, Oracle Linux, Suse, CentOs, Ubunto e Debian.
- Deverá possuir integração nativa com os módulos Amazon SNS, e Amazon Identity and Access Management (IAM);
- Deverá possuir gerenciamento de todos os eventos relativos aos hosts gerenciados possibilitando, além do armazenamento dos eventos na própria solução, o seu encaminhamento para uma solução de SIEM;
- A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs de mercado, no mínimo com: IBMQradar, Splunk e ArcSight de modo a permitir enviar os seus logs para essas soluções;
- A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
- A solução deverá suportar o uso de REST API's para permitir a integração com outras aplicações;
- O uso das REST API's deve suportar no mínimo as seguintes funcionalidades:
  - Autenticação – Log in e Log out;
  - Administração de Contas - Criação, edição e exclusão de contas de acesso;
  - Eventos – Acesso à lista de eventos dos módulos de Antimalware e Reputação Web;
  - Monitoração de Status - Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks;
  - Monitoração de uso – recuperação de estatísticas sobre as operações da solução em cada tenant.
- A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

❖ **Funcionalidades do Módulo de antimalware**

- O módulo de Antimalware deverá efetuar a proteção contra códigos maliciosos através da instalação ou não de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
- O módulo de Antimalware deverá suportar a análise de comportamento (Behavior Monitoring) para a detecção avançada de ameaças;

- A funcionalidade de análise de comportamento deverá permitir o bloqueio de atividades suspeita de criptografia de arquivos visando impedir a propagação de malwares do tipo ransomware.
- Possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
- A funcionalidade de análise de comportamento deverá permitir o backup de arquivos que estiverem sendo criptografados, fazendo a restauração dos mesmos em caso de bloqueio do processo de criptografia;
- O módulo Antimalware deverá incluir técnicas de Inteligência artificial baseada em algoritmo de Machine Learning para análise preditiva de malwares;
- Executar rastreamento nas máquinas virtuais e fornecer lista de todas as recomendações de segurança para os softwares que estiverem instalados nessas máquinas virtuais, bem como do sistema operacional;
- Implementar a proteção contra acesso a websites ou URL's consideradas maliciosas, de baixa reputação ou não categorizadas;
- Deve permitir a proteção contra acesso a websites ou url consideradas maliciosas ou de baixa reputação;
- A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
- Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

❖ **Funcionalidades do Módulo de segurança de rede;**

- Proteger de forma automática e transparente contra brechas de segurança descobertas, interrompendo somente o tráfego de rede malicioso;
- Operar como firewall de host stateful bidirecional, monitorando as comunicações nos servidores protegidos;
- Possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
- Possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
- Permitir que regras de Firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
- Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, by-pass, force allow, deny;
- Permitir realizar pseudo stateful em tráfego UDP;
- Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem;
- Permitir a criação de novas regras utilizando templates padrão;
- Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas;
- Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
- Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do SO e demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações (virtual Patching);
- Permitir execução de varreduras sob demanda ou agendada;
- Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras;
- Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais e aplicações: Windows 2003, 2008 e 2012; Linux Red Hat, Suse, CentOS e Debian;
- Aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.

- Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- Possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting;
- Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- Permitir configuração de regras de IDS/IPS diferenciadas de acordo com horário ou dia da semana;
- Implementar a inspeção de tráfego incoming SSL;
- Apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo links com referências externas, quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- Bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de um determinado web browser ou aplicação de backup;
- Permitir habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- Permitir que as regras de IPS atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa decidir qual ação deva ser tomada;
- Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

❖ **Funcionalidades do Módulo de segurança e integridade do sistema**

- Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
- Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux;
- Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;
- Possuir a capacidade de monitorar mudanças efetuadas no registro do Windows;
- Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização de XML para criação de regras avançadas;
- Permitir execução destas varreduras sob demanda ou agendada;
- Rastrear arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;
- Gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;
- Registrar em relatório todas as modificações que ocorram nos objetos monitorados;
- Classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- Possibilitar a escolha do diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- Possuir capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
- Permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- Implementar inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor;
- Permitir modificar as regras por severidade de ocorrência de eventos;
- Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do SO;

- A solução deverá permitir a implantação do módulo de controle de aplicações nas plataformas Linux e Microsoft Windows anteriormente descritas;
- O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- A solução deverá permitir o escaneamento de um host gerando uma imagem de baseline, a partir da qual qualquer mudança ou aplicação nova deverá ser bloqueada;
- O agrupamento dos eventos deverá ser realizado pelo menos por hash ou por máquina;
- Deverá possuir funcionalidade de janela de manutenção desabilitando a funcionalidade de controle de aplicação por um tempo pré-determinado reativando a sua funcionalidade após o termino da janela;
- A solução deverá possuir no mínimo as funcionalidades de bloquear tudo o que não for permitido explicitamente (whitelist) e permitir tudo o que não for bloqueado explicitamente (blacklist).

❖ **Gerenciamento centralizado para todos os itens**

- A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de endpoint,mobile, antispam, filtro web e solução de proteção para servidores.
- Instalação do servidor na plataforma Windows 2008 Server ou superior, seja o servidor físico ou virtual;
- Suportar base de dados Microsoft SQL;
- Deve gerenciar logs das atividades e eventos gerados pela solução;
- Deve possuir integração com Microsoft Active Directory;
- Deve permitir níveis de administração por usuários ou grupos de usuários;
- Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;
- Deve disponibilizar sua interface através dos protocolos http e https;
- Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;
- Deve permitir diferentes níveis de administração, de maneira independente do login da rede;
- Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;
- Deve permitir criação de modelos de relatórios customizados;
- Deve permitir logon via single sign-on com os demais produtos da solução;
- Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;
- Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;
- Deve permitir o controle individual de cada componente a ser atualizado;
- Deve permitir a definição de exceções por dias e horas para não realização de atualizações;
- Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;
- Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;
- Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;
- Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;
- Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;
- Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;
- Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);
- Deve permitir o controle do intervalo de expiração de comandos administrativos;
- Deve possuir a configuração do tempo de expiração da sessão dos usuários;
- Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;
- Deve permitir a configuração da duração do bloqueio;
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias
- Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

- Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;
- Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;
- Deve de permitir a criação de políticas de segurança personalizadas;
- As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:
  - Nome parcial ou completo das estações de trabalho, permitindo a utilização de caracteres coringa para identificação do nome parcial da máquina;
  - Range de endereços IPS;
  - Sistema operacional;
  - Agrupamento lógicos dos módulos;
- As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;
- Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;
- Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;
- Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
- Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;
- A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;
- Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;
- Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

ITEM 9 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE FILTRAGEM DE CONTEÚDO DE E-MAIL

- **Deverá ser licenciada para 2000 (dois mil) usuários da Plataforma:**
  - A solução Antispam deve possuir controle de caixas postais e fluxo de análise de mensagens/dia ilimitadas, de acordo com os recursos de hardware disponíveis;
  - Deve ser uma solução MTA (Mail Transfer Agent) completa com suporte ao protocolo SMTP, que controla o envio e o recebimento de todas as mensagens da empresa, com registro de logs das atividades do MTA;
  - A licença de uso deve atingir um número de 2000 (duas mil) caixas postais.
  - Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, spyware, worms, trojans, SPAM, phishing, e-mail marketing, e-mail adulto ou qualquer outra forma de ameaça virtual.
  - Deve permitir alta disponibilidade das funções de filtragem, de maneira assegurar que o serviço de correio nunca pare por falha da solução.
  - A solução deve suportar o processamento de no mínimo 10.000 (dez mil) conexões simultâneas e 160.000 (cento e sessenta mil) mensagens por hora.
  - Deve ser capaz de efetuar implementação em virtual appliance, compatível com os principais sistemas de virtualização do mercado, entre eles:
    - VMWare;
    - Citrix;
    - Microsoft Hyper-V.
- **Pontos Gerais:**
  - A licença de uso do software base possuir 12 (dozes) meses de atualização do fabricante compreendendo os seguintes módulos:

- Atualização das assinaturas de segurança disponibilizadas automaticamente como por exemplo: assinaturas de vírus, malwares e outras ameaças, serviços de reputação de websites, IPs e assinaturas de Websites e aplicativos web;
- Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante bom como atualizações de recursos melhorias dentro da mesma versão;
- Acesso a base de inteligência global do fabricante para análise online de ameaças;

- Analisar mensagens, no mínimo, por meio dos seguintes métodos:
- Proteção dinâmica por reputação;
- Assinaturas de spam;
- Filtros de Vírus;
  - A verificação de vírus, além da técnica tradicional (por assinatura), também deve ser feito através de BigData do fabricante, bem como utilização de método Fuzzy Hash ou Similar para detecção de similaridades e detecção de possível variante de malware;
  - Possuir dois módulos de antivírus, sendo um do próprio fabricante, já devidamente licenciado para uso simultâneo;
- Filtros de anexos;
- Filtros de phishing;
- Análise heurística;
- Análise do cabeçalho, corpo e anexo das mensagens;
- E-mail bounce;
- Dicionários pré-definidos e customizados com palavras e expressões regulares;
  - Já deve vir com dicionários pré-estabelecidos, para posterior utilização, tais como:
    - Número de cartão de crédito;
    - CNPJ;
    - RG e CPF;
- Deve possuir mecanismo de backup e recuperação da configuração da solução;
- Deve possuir capacidade de envio de backup via FTP e SFTP, sendo configurado diretamente na interface gráfica da solução (sem necessidade de qualquer configuração em linha de comando).
- Os manuais necessários à instalação e administração da solução, devem constar no seguinte idioma: Português do Brasil ou Inglês;
- A interface de administração do sistema deve ter suporte a no mínimo um dos seguintes idiomas:
  - Português do Brasil;
  - Inglês;
- A interface do usuário deve suportar o idioma Português do Brasil ;
- Deve possuir banco de dados relacional para armazenamento dos registros de acesso, logs de sistema e configurações. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante. Não serão aceitas soluções baseadas em armazenamento de Logs em formato Texto;
- Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino;
- Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;
- Ter a capacidade de processar o tráfego de entrada e de saída de mensagens no mesmo appliance, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido;
- A solução deve ser capaz de efetuar a saída de e-mails indicando um IP específico para a saída de mensagens, isto é, possuir a capacidade de redirecionar as mensagens de saída por IP's diferentes para cada domínio cadastrado no appliance se o administrador assim desejar;
- A solução deve permitir criação de regras por:
  - Grupos de usuários;
  - Domínios;
  - Range de IP;

- IP/Rede;
- Remetentes específicos;
- Destinatários específicos;
- Grupos de LDAP;

- Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;
- Possibilidade de permitir relay autenticado para clientes externos da corporação;
- Deve possuir ferramenta de auditoria de email, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”;
- A console de gerenciamento deve permitir a transferência de arquivos (SCP/FTP) e ser acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:
  - Administração centralizada de todas as regras e filtros integrantes da solução;
  - Status da versão das assinaturas do antivírus em uso;
  - Controle de acesso de usuários, com diferentes privilégios de configuração;
  - Criação de relatórios, gráficos e estatísticas, com suporte a múltiplos domínios;
  - Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.
- Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;
- Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF;
- Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:
  - Conteúdo do anexo;
  - Mime-Type do anexo;
  - Extensão do anexo;
  - Nome completo do anexo;
  - Nome parcial do anexo;
  - Expressão regular;
  - Tamanho do anexo;
  - Anexos compactados com senha;
  - Quantidade de níveis de compactação no mesmo anexo;
- Possuir “Zimlet” de integração com o sistema de correio eletrônico Zimbra, permitindo que através da interface Web do Zimbra seja possível marcar uma mensagem como “Spam” ou “Não Spam”, atualizando o sistema de filtragem e gerando uma nova regra para autoaprendizagem do sistema;
- Deve possuir um sistema de Disaster e Recover, ao qual com um só botão é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente.
- Possuir a função de abertura de relay automático para empresas que usam Microsoft Office 365, sem necessidade de cadastro de IP´s ou DNS da Microsoft para abertura de relay.
- Deve possuir sistema de diagnóstico via interface WEB, com no mínimo de execução nos seguintes testes:
  - Teste de Conectividade TCP – Bastando informar o Host e Porta a ser testado;
  - Teste de Conectividade ICMP – Bastando Informar o Host a ser testado;
  - Teste de DNS – Bastando informar Host ou Domínio a ser testado;
  - Teste de Envio de E-mail;
  - Teste de Lookup de E-mail via LDAP;
  - Teste de Conectividade com o fabricante (para isso, testa-se as portas necessárias de comunicação junto ao fabricante);
  - Teste de TRACEROUTE;
  - Teste de DNS Reverso;

- Teste de SPF, para checar se tem registro para um determinado domínio;
- Teste de DKIM, para checar se tem registro para um domínio;
- Teste de DMARC, para checar se tem registro para um domínio;
- Teste de portas de Saída utilizadas pelo sistema.

- Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:
  - Serviço de antivírus;
  - Serviço de MTA;
  - Serviço de Banco de Dados;
  - Serviço de DKIM;
  - Serviço de DLP;
  - Serviço de SMNP;
- Deve permitir a instalação de agentes/plug-ins (tanto no appliance de gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, tais como:
  - Zabbix;
  - Nagios;

- **Da alta disponibilidade:**
  - Suportar Cluster de Alta Disponibilidade na forma de Cluster Ativo-Ativo e Ativo-Passivo e Load Balance através do registro MX e/ou sistemas de balanceamento proprietário, assegurando as funções de filtragem que o serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução;
  - Deve permitir a configuração em Cluster com appliances virtualizados em DataCenters distintos;
  - O cluster deve poder ser formado por appliances físicos e appliaces virtuais, de forma mista.
  - Administração centralizada de múltiplos nodos de filtragem em uma única interface web, independente se estiver em modo cluster de alta disponibilidade ou load balance de forma que o gerenciamento e a replicação de políticas do cluster também seja feita de forma centralizada;
  - A administração de todo cluster deve ser feita através de um único IP de destino, não sendo permitido a gestão de regras de forma descentralizada.
  - Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único Virtual IP.

- **Do Gerenciamento:**
  - O acesso à interface de administração deve possuir diferentes níveis de acesso de forma granular, permitindo que sejam configurados perfis diferentes de administradores, por endereços de e-mail e domínio permitidos;
  - O sistema deve permitir criar usuário do tipo Auditor que tenha permissão de visualizar através da interface web os e-mails que forem colocados para auditoria, sendo possível definir quais endereços de e-mails ou domínios ele poderá auditar;
  - O sistema deve possuir ainda no mínimo quatro perfis de administrador pré-definidos:
    - Administrador: Com acesso total às configurações da solução;
    - Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;
    - Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;
    - Operador: Com acesso à administração da quarentena e gerenciamento da “Black e White List”;
    - Usuário: Possui a capacidade de administrar sua “Black e White List”, individualmente, bem como sua área de quarentena individual;
  - Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:
    - Emails;
    - Domínios;
    - IP’s;
    - Range de IP;

- Expressão Regular;
- Usuários;
- Listas de distribuição;
- Grupos de LDAP;

- **Alertas e logs da solução:**
  - Deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso;
  - A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável;
  - Possuir registro de log de TODAS as ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso e para obtenção do mesmo, não sendo necessário acionamento da fabricante da solução;
  - Possuir mecanismo de feedback por email ao administrador sobre recursos e atualizações do sistema;
  - Deve possuir capacidade de envio dos logs de um nodo específico ou de todo o cluster para um servidor de syslog. Também deve ser possível selecionar os logs a serem enviados, bastando selecionar conforme opções indicados:
    - Emergency
    - Alert
    - Critical
    - Error
    - Warning
    - Notice
    - Informational
    - Debug
  - Deve ser possível enviar email caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio do email podem ser:
    - Espeço em disco;
    - Filas de email;
    - Memória;
    - Processador;
    - Serviço de Filtragem;
    - Atualização do sistema de segurança;
    - Antivirus e Antispam;
    - Ponto de acesso indisponível;

- **Das Funcionalidades para o Usuário Final:**
  - Possuir interface web de administração segura HTTPS para que o usuário final possa administrar suas opções pessoais, sem que estas opções interfiram na filtragem dos demais usuários.
  - A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo os seguintes idiomas:
    - Português do Brasil;
    - Inglês;
  - O usuário final deve poder incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails.
  - O usuário final deve poder visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que as mesmas sejam consideradas somente como “possível spam” ou “spam”.
  - O usuário final deve poder solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer ao qual não permita que o usuário final a libere.
  - O usuário deverá poder selecionar qual o idioma utilizado sua interface, sendo no mínimo os seguintes idiomas:
    - Português do Brasil;

- Inglês;

- **Da quarentena:**
  - Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio appliance, sem necessidade de nenhum hardware adicional;
  - Deve possibilitar a gestão de quarentena pelos administrados de forma que o mesmo possa visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host destinatário, a mensagem original, tamanho da mensagem original e permitindo no mínimo as ações liberar e/ou excluir;
  - Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;
  - A interface deve permitir identificar quais Regras do Modulo de AntiSpam foram ativadas e qual sua pontuação, afim de permitir ao administrador a elaboração de regras granulares;
  - A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos;
  - Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas no próprio appliance, seja ele virtual ou físico.
  - Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena;
  - Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens;
  - O sistema de quarentena de e-mails deve criptografar automaticamente as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails armazenados em quarentena, assim aumentando a confiabilidade e segurança da solução.
  - Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, por exemplo: manter as mensagens das últimas 72 horas, dessa forma ao ultrapassar esse limite, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos.
  - O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo “indeterminado”.
  - Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena, por exemplo limitar uma quarentena a 100GB, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos.
  - O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela.
  - Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

- **Dos Usuários e Grupos:**
  - Possuir integração com serviço de diretórios LDAP, Microsoft Active Directory e Zimbra para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack”) sem que haja necessidade de modificar os parâmetros “default” do serviço de diretórios.
  - Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory.
  - Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas.
  - Permitir a utilização de mais de um servidor de LDAP, para autenticação dos usuários em outro servidor LDAP, caso ocorra indisponibilidade do servidor primário de LDAP.
  - Integração nativa com os principais sistemas de colaboração do mercado, entre eles:
  - Microsoft Exchange®;
  - Zimbra Collaboration Suite®;

- IBM Lotus Domino®;
- Possibilitar a customização de regras e políticas por usuários ou grupos;
- A solução deverá permitir a configuração do intervalo de sincronismo entre a solução anti-spam e o serviço de diretório.
- Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de anti-vírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

- **Dos relatórios:**
  - Deve permitir a geração de relatórios de todos os appliances de um cluster de forma centralizada através de uma única interface web no console de gerenciamento;
  - Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;
  - Permitir a seleção de dados para a formulação de relatórios por data ou por um intervalo de tempo específico;
  - Deve permitir a configuração de um período para a retenção de dados para a formulação de relatórios;
  - Capacidade de criar relatórios globais e por domínio contendo no mínimo as seguintes informações:
  - Sumário de mensagens;
  - Quantidade de mensagens processadas;
  - Principais origens de spam por domínio, endereço de e-mail;
  - Principais destinos de spam por domínio, endereço de e-mail;
  - Principais origens de vírus;
  - Principais fontes de ataque;
  - Estatísticas da quarentena;
  - Conexões completadas X bloqueadas;
  - Relatório de tráfego;
  - Principais destinatários de Spam
  - Principais destinatários de e-mail;
  - TOP Attachments;
  - TOP SPF Violations;
  - TOP Ataques por fraude de email / tentativa de spoof;
  - Permitir filtros de relatórios com definição de origem e destinos específico;
  - Possuir relatórios estatísticos de conexões, ameaças, quarentena, SPAM;
  - Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
  - Capacidade de remoção automática das mensagens em quarentena de acordo com as configurações definidas pelo administrador do sistema;
  - Os relatórios no mínimo devem poder ser filtrados por:
    - Período de tempo;
    - Ponto de Filtragem que o email passou;
    - De;
    - Para;
    - Qual a classificação que a mensagem atingiu, dentre eles no mínimo:
      - DLP;
      - Provável SPAM;
      - SPAM;
      - Vírus;
      - Conteúdo Bloqueado;
      - Whitelist;
      - Blacklist;
      - Tamanho Excedido;

- Phishing
- Relatório para um único usuário ou Domínio

- Para evitar agendamento de múltiplos relatórios, dessa forma consumindo recursos desnecessários do sistema, o appliance deve possuir um sistema de relatório integrado e com isso, em um único relatório agendado agrupa-se no mínimo os seguintes os relatórios:
  - Relatório de Volume de Mensagens por Data;
  - Relatório dos Principais Destinatários de SPAM;
  - Relatório dos Principais Remetentes de SPAM;
  - Relatório de Top E-mail Relays;
  - Relatório de Top Remetentes por Quantidade;
  - Relatório de Top Remetentes por Volume;
  - Relatório de Top Destinatário por Quantidade;
  - Relatório de Top Destinatário por Volume;
  - Relatório de Vírus;
  - Relatório de Estatísticas da Quarentena;

- **Rastreamento das mensagens:**
  - Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando).
  - O rastreamento deve ser possível através de qualquer um dos seguintes campos:
    - ID da mensagem;
    - Email do Remente;
    - Email do Destinatário;
    - Domínio do Remetente;
    - Domínio do Destinatário;
    - Assunto da mensagem;
    - Nome do anexo;
    - Palavra contida no conteúdo do corpo da mensagem;
    - IP de Origem da mensagem;
    - Tamanho da mensagem;
    - Regra de SPAM;
    - Regra de DLP;
    - Se a mensagem foi entregue ou não;
    - Regras personalizadas aplicadas na mensagem;
    - Nome da ameaça encontrada.
  - A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
  - Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando como filtro o assunto, o remetente, o destinatário, regra de bloqueio, conteúdo do corpo da mensagem, data, status, hora de entrega da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”.
  - O rastreamento deve ser a partir de uma única interface de gerenciamento independente de qual appliance filtrou a mensagem, não sendo aceito pesquisa via linha de comando;
  - O rastreamento deverá ter a opção de ser efetuado de todos os pontos de filtragem, sem a obrigatoriedade de separação de um único ponto de filtragem por vez;
  - Deve apresentar como resultado as seguintes informações:
    - Remetente da mensagem;
    - Destinatários da mensagem;
    - Servidor de origem;
    - Se foi armazenada em quarentena;
    - Se continha vírus
    - A regra que atuou;

- O servidor de origem;
- O tamanho da mensagem;
- Se foi entregue ou não;
- Qual ponto de filtragem utilizado (qual appliance processou a mensagem);

- No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue;
- Se o email tiver sido bloqueado por ser considerado spam ou possível spam, deve apresentar os filtros aplicados, bem como a pontuação apresentada por cada filtro e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador);
- Deve ser capaz de visualizar a fila de e-mails em tempo real, bem como o sentido do email na fila (se é fila de entrada de email ou saída de email), indicando total de emails na fila de saída, total de emails na fila de entrada e total de emails com erros na entrega.
- Rastrear emails à partir de uma determinada ameaça.
- Apresentar na interface gráfica as fontes de ataque e através delas, apresentar quais emails recebidos, originários dessa fonte de ataque.
- Apresentar em mapa geográfico da localização das fontes de ataque.

- **Proteção contra ataques:**
  - A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service).
  - Ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com Suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS/ SSL, permitindo configurar domínios onde o TLS é mandatório;
  - A solução deverá possuir a capacidade de executar as seguintes ações:
    - Limitar o número de conexões TCP permitidas através de um valor configurável.
    - Rejeitar a conexão SMTP que se caracterize como "flooding".
  - Deve ser capaz de efetuar a filtragem do trafego de correio eletrônico bloqueando a entrada de:
  - Vírus;
  - Spyware;
  - Worms;
  - Trojans;
  - Spam;
  - Phishing;
  - e-mail Marketing, ou qualquer outra forma de ameaça virtual;
  - Deve possuir controle total da comunicação permitindo restringir:
  - IP reverso mal configurado;
  - Domínios inexistentes;
  - Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados;
  - Enforce RFC821;
  - Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador. A frequência de atualização desta consulta deve ser de no mínimo 15 minutos, sem necessidade de interrupção do serviço;
  - A solução deve ser capaz de filtrar contra vírus as mensagens tanto de entrada quanto de saída de e-mails;
  - Permitir criação de políticas diferenciadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;
  - Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:
  - Aceitar;
  - Colocar em quarentena;
  - Inserir tag personalizada no assunto;
  - Marcar o cabeçalho;
  - A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:
  - Alterar o assunto da mensagem;

- Adicionar cabeçalhos para rastreamento;
- Descartar a mensagem;
- Colocar em uma determinada área de quarentena definida pelo administrador;
- Deve permitir também a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, Inglês e espanhol, ou a aplicação de regras por país;
- Possuir a capacidade de criar filtros personalizados usando expressões regulares;
- Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;
- Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);
- Capacidade de limitar o número máximo de mensagens enviadas por remetente a cada hora, com opção de bloqueio automático do remetente, caso esse limite seja excedido.
- Permite criar regras customizáveis contra spammers, possibilitando um controle avançado em todo conteúdo do e-mail efetuando buscas por Expressões Regulares presentes em todo conteúdo do e-mail (SMTP HEADER, BODY, URL, ANEXOS), sendo possível criar regras compostas utilizando os operadores lógicos “E” e “OU”;
- O fabricante da solução deve possuir consulta de reputação de IP de remetentes de e-mail. Esta consulta deve retornar os dados do remetente, com informações referentes à:
- Infraestrutura de rede;
- Registro em blacklists mundiais;
- Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.
- Capacidade de efetuar consultas externas para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de Spams e phishings recebidos e outros tipos de ameaças;
- Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de email;
- Deve possuir suporte ao bloqueio de conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento do Appliance, em especial baseado em lista local de bloqueio de conexão (IP’s, email e domínio do remetente ou email e domínio do destinatário), RBL’s e SPF;
- Deve permitir que o administrador do sistema cadastre novas RBL’s para serem utilizadas a nível de conexão SMTP;
- Possibilidade de restringir o processamento de mensagens (relay) endereço IP;
- Deve ter capacidade de proteção a spoofing de email (tanto Spoofing de emails na entrada – quando o hacker utiliza o domínio do órgão como remetente, como Spoofing de emails na saída – quando tem algum email de saída que não esteja com o domínio do órgão como remetente), já incrementado na solução, bastando o administrador ativar a regra, sem necessidade de customizar uma regra para isso;
- Possuir capacidade de criar cotas de envio e recebimento de e-mails em um prazo determinado de tempo, limitando o fluxo e prevenindo ataque do tipo DOS ou distribuição de spam através de um computador infectado na rede interna;
- Possuir mecanismo de “Engargalamento de Email” (Spam Throttling) permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;
- Deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem;
- Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
- Possuir controle de surtos, penalizando o remetente por um tempo configurável pelo administrador ao detectar:
  - Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de email;
  - Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de email;

- Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de email;

- Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:
  - Fontes de ataque;
  - Ameaças encontradas;
  - Ameaças Identificadas;

- **Da proteção contra SPAM e PHISHING:**
  - Possuir filtro de anti-spam para detecção de spams usando no mínimo as seguintes tecnologias:
  - FingerPrint: Filtro por assinatura de spam;
  - Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;
  - Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);
  - Análise de Imagens: Filtragem de spam em imagens;
  - Filtro de URL: Filtragem por URL mal-intencionada contidas na no corpo da mensagem, dessa forma combatendo possível email Phishing;
  - Filtro de URL contidas no Emails com Categorização – Permitir ao administrador definir através de categorias, com no mínimo 30 categorias, divididas por assunto, possibilitando ao administrador definir uma pontuação. Categorias mínimas contidas na solução:
  - Conteúdo pornográfico;
  - Abuso infantil;
  - Redes sociais;
  - Racismo e ódio;
  - Pesquisa de empregos;
  - Streaming de áudio;
  - Streaming de vídeo;
  - Esportes;
  - Notícias;
  - Compras On Line.
  - Deve possuir tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;
  - Deve possuir tecnologia capaz de avaliar um link "URL" recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivos (Tipo Zip, EXE, RAR, etc), na tentativa de enganar o usuário , efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;
  - Deve permitir que o administrador cadastre novas RBL's a serem utilizadas a nível de cálculo de SPAM. O administrador deverá ter a autonomia para selecionar quais RBL's serão utilizadas a nível de conexão SMTP e quais serão utilizadas a nível de cálculo de SPAM;
  - Possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:
  - Recurso de Grey List;
  - Recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para "fail" e "soft fail", conforme descrito pelo Comitê Gestor da Internet no Brasil em seu website oficial (HTTP://www.antispam.br/admin/spf);
  - Recurso de checagem por DMARC;
  - Recurso de checagem por assinatura DKIM;

- Recurso de checagem de DNS Reverso;
- Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;
- Análise de reputação de IP;
- Reputação de Mensagens;
- Filtros de URL;
- Filtro de anti-phishing;
- Consulta de RBL´s (real-time blackhole list);
- Machine Learning utilizando tecnologia Bayes Databases ou similar.
- Classificar a reputação de novas origens de spam com tecnologia de classificação dinâmica. O sistema de reputação deve utilizar dados de redes globais de monitoramento de tráfego web e de e-mail, não restringindo ao fluxo de mensagens do ambiente instalado;
- Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:
- Origens das mensagens;
- Destino das mensagens;
- Domínios;
- Endereços de e-mails;
- Expressões regulares (dicionário de palavras);
- Fluxo;
- Quantidade de mensagens;
- Tamanho de anexo;
- Número máximo de destinatários em uma única mensagem;
- Tipo de arquivos em anexo;
- Extensões de arquivos em anexo, identificados por Mime-Type;
- Anexos criptografados;
- Anexos compactados;
- Níveis de compactação dos arquivos anexos;
- Quantidade de anexos na mensagem;
- Conteúdo HTML no corpo da mensagem.
- Possuir mecanismo de análise de conteúdo HTML no corpo da mensagem mensagens, permitindo ao administrador desarmar as tags HTML possivelmente perigosas e bloquear as mensagens, possuindo no mínimo a identificação das seguintes Tags:
- “<form>”;
- “<script>”;
- “<iframe>”
- Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas Confiáveis e Spams permitindo ao administrador configurar nesses casos as seguintes ações:
- Entregar direto o e-mail;
- Colocar em quarentena;
- Remover mensagem;
- Auditar mensagem;
- Encaminhar a mensagem;
- Notificar o destinatário;
- Adicionar header na mensagem;
- Transformar HTML em texto simples
- Possuir sistema de detecção de ataque de diretórios (DHA – Directory Harvest Attack), capaz de recusar novas conexões SMTP de uma fonte emissora, caso ela tenha enviado, em um período de tempo, mensagens a usuários inválidos/inexistentes no domínio;
- Deve permitir regras internas para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos da contratante, permitindo definir no mínimo: país de origem, endereço de domínio e IP do remetente;

- A solução deve permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório:
    - Microsoft Active Directory;
    - LDAP;
    - Esteja integrado com a solução e administre suas próprias mensagens categorizadas como spam;
- Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory;
- Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o dialogo SMTP (tratar Non-Delivery Report Attack);
- Possuir proteção contra bounce email attack através “Bounce Address Tag Verification”;
- Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas;
- Deve permitir que mensagens de Falso Negativo sejam reportadas através da interface gráfica para o laboratório de pesquisa do fabricante ou oferecer um caminho para que mensagens de falso negativo sejam reportadas diretamente ao laboratório do fabricante;
- Deve possuir mecanismo que permita a adição de Cabeçalho de identificação da classificação das mensagens como SPAM, a fim de integrar com sistemas de correio eletrônicos tais como:
- Microsoft Exchange;
- Zimbra Collaboration Suite;
- Lotus Domino e outros.
- Deve possuir mecanismo de análise e detecção de imagens pornográficas e/ou nudez, permitindo ao administrador definir a sensibilidade da detecção e a criação de regras por usuários e/ou grupos de usuários e permitindo a tomada de ações de bloquear ou liberar a mensagem;

- **Da proteção contra VÍRUS:**
    - Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente;
    - Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de email);
    - Possuir módulo de detecção “Hora Zero” para a identificação de novas ameaças desconhecidas pelo antivírus, colocando em determinada área da quarentena por período de tempo, até nova verificação pelo antivírus.
    - Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .rar, .zip, .tar, .arj, .cab, .lha, .exe, .lzh, .tgz e .gzip;
    - A solução deve possuir um motor antivírus e Antimalware do próprio fabricante da solução, além de um motor Antivírus e AntiMalware de terceiro já integrado a solução sem custo adicional;
    - Proteção contra Vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional:
    - Dia-zero (zero-day);
    - Vírus outbreak;
    - Hora-zero (Zero-hour);
    - Targeted Attack protection;
    - Tomar no mínimo as seguintes ações:
        - Descartar a mensagem;
        - Colocar em uma determinada área da quarentena definida pelo administrador;

- **Das notificações de quarentena individual do usuário:**
    - A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (Digest) em períodos de tempo pré-configuráveis por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste Digest, dispensando a instalação de agentes e acesso a quarentena individual do usuário.
    - Grupos diferentes de usuários devem poder receber a notificação em horários diferentes.

- O digest deve ser enviado em Língua portuguesa do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários;
- Deve ser possível a customização do digest com as seguintes características alteráveis:
  - Email de origem;
  - Título/Assunto do email;
  - Mensagem do digest, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor;
  - Logomarca do digest;
- O digest deve permitir ao usuário final tomar no mínimo as ações de:
  - Liberar uma mensagem bloqueada;
  - Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens do mesmo já sejam barradas;
  - Marcar o remetente como confiável (whitelist), para que as futuras mensagens do mesmo não sejam pontuadas como spam;
  - Reportar o bloqueio indevido;
  - Solicitar envio de novo resumo;
  - Acessar sua área de quarentena;
- Deve permitir que o administrador escolha qual quarentena a ser incluída no Digest do usuário final, por exemplo incluir no Digest os e-mails quarentenados que foram considerados conteúdos maliciosos (VÍRUS);
- A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final poder selecionar, no mínimo dentre elas:
- Liberar email;
- Reportar Falso Positivo;
- Incluir o remetente do email em blacklist individual (do próprio usuário);
- Incluir o remetente do email em whitelist individual (do próprio usuário);
- Visualizar o email;

- **Do disclaimer:**
  - Capacidade de incluir “disclaimers” nas mensagens enviadas;
  - A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP.
  - A solução deverá suportar a configuração dos “disclaimers” em formato html e texto.

- **Prevenção a roubo de informação (DLP) e Compliance:**
  - Deve possuir módulo DLP (Data Loss Prevention) do próprio fabricante, já integrado na solução sem a necessidade de licenciamento adicional ou outro appliance.
  - O módulo de DLP deve analisar todo conteúdo da mensagem a fim garantir a confiabilidade das mensagens que saem da empresa, permitindo ao administrador configurar diversas ações a fim de restringir, controlar ou auditar as mensagens e informações sensíveis da empresa;
  - Deve permitir criar regras de compliance “Auditoria/Aderência” através de filtros avançados de análise da mensagem, permitindo identificar através de Dicionários (Conjunto de Palavras e Expressões Regulares) personalizados pelo administrador ou já existentes na ferramenta, dentre eles:
  - Identificação de CPF;
  - Número de cartão de crédito;
  - CNPJ.
  - Deve permitir a busca a partir dos dicionários de palavras dentro dos arquivos em anexo nos e-mails com suporte a no mínimo aos formatos .doc, .xls, .ppt, .pdf;
  - As regras de compliance podem ser criadas utilizando os Dicionários definidos nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:
  - Cabeçalho;
  - URL (contidas no e-mail);

- Corpo do email;
- Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT.
- Permitir ao administrador criar regras de compliance para arquivos criptografados, possibilitando ao administrador configurar a ação a ser tomada quando um anexo criptografado é identificado. A ferramenta deve ter no mínimo três algoritmos de detecção: Mecanismo Heurístico, Myme-Type e Extensão;
- Todos os itens do DLP devem permitir configurações através de regras que permitam ao administrador definir, no mínimo, as seguintes ações:
- Entregar a mensagem;
- Não entregar a mensagem;
- Armazenar a mensagem para auditoria;
- Notificar remetente e destinatário da mensagem;
- Encaminhar a mensagem para outro destinatário.
- Todos os itens do DLP devem permitir configurações que permitam ao administrador criar regras complexas através de operadores lógicos “E” e “OU”;
- Deve permitir ao administrador gerar notificação (se assim desejar) ao remetente do email, indicando que o email enviado não condiz com as normas da empresa. Essa notificação poderá ser customizada de acordo com a necessidade do administrador;

- **Criptografia de Email**
  - Deve possuir módulo de criptografia do próprio fabricante, já integrado na solução sem a necessidade de licenciamento adicional ou outro appliance.
  - A criptografia deve atuar na saída de e-mails que trabalhe de maneira transparente ao usuário final, sem a necessidade de plugins, agentes ou outro tipo de software e com uma interface para o destinatário das mensagens, customizável pelo administrador;
  - A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional;
  - Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base em no mínimo:
  - Assunto;
  - Destinatário;
  - Email do Remetente;
  - Nome do Anexo;
  - A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente;
  - Deve impossibilitar o uso de Cache de Browser para acesso as mensagens criptografadas;
  - Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada;
  - Deve possibilitar ao administrador indicar se o destinatário poderá responder o email;
  - Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o email;

- **Do Sistema de Proteção Contra Ataques Dirigidos (Targeted Attack Protection - TAP):**
  - Deverá prover proteção contra ataques dirigidos tais como:
    - Spear-phishing;
    - Ataques Zero-Day;
    - Ameaças avançadas persistentes (APTs)
  - Deve possuir técnica para construção de modelos estatísticos com Big Data;
  - Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:
    - Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;
    - Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;
    - Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.
  - Possuir acesso ao Dashboard do módulo de Segurança contra-ataques dirigidos;
  - O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:

- Detecção - A análise de email deve verificar variáveis em tempo real incluindo as propriedades da mensagem, bem como, o histórico de e-mail do destinatário para identificar anomalias que indiquem uma ameaça potencial.
- Proteção - Deve assegurar que links para URLs suspeitas são dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto o serviço verifica se o destino é seguro.
- Ação - Deve demonstrar aos administradores e gestores de segurança em tempo real e de forma interativa uma visão dos ataques sofridos e das ameaças que posam sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle on-line.

- Não será aceita solução baseada apenas em reputação de URL.
- A solução deve conter engine para detecção de Anomalias, não podendo se limitar a analise com definições baseadas em ataques já conhecidos.
- A solução deve ser proativa e ter capacidade de detecção por heurística, utilizando técnicas de análise de grande volume de dados, desta forma definindo um modelo de padrão de mensagens da corporação, levando em conta remetentes, destinatários, volume de mensagens e vários outros fatores, dessa forma modelando os e-mails “Normais” da corporação e barrando “Anomalias”, fazendo essa análise e definição de padrão por caixa posta.
- Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:
  - Email do Destinatário;
  - Email do Remetente;
  - Domínio de Origem;
  - Domínio de Destino;
  - IP/Rede;
  - Range de IP;
  - Expressão Regular;
  - Usuários;
  - Listas de distribuição;
  - Grupo de LDAP;
- A proteção de URL deverá reescrever os links do e-mail e a cada clique o sistema deverá analisar a URL e somente depois de passar por todos os testes, sendo constatado que não é malicioso, deve redirecionar para a URL original. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site será bloqueado no navegador.
- O sistema deverá ser capaz varrer anexos no mínimo nas extensões PDF, Microsoft Office, arquivos em Flash para payloads maliciosos, Microsoft Office com as seguintes extensões a serem verificadas:
  - .swf;
  - .pdf;
  - .doc;
  - .xls;
  - .xlsx;
  - .ppt;
  - .ppt;
  - .pptx;
  - .rtf.
    - Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para descartar e salvar uma cópia na quarentena.
- A solução deverá dispor de Dashboard alertando aos administradores de ataques por e-mail e deverá fornecer detalhes sobre o ataque direcionado, fará triagem para reduzir potenciais danos, reportando ao fabricante criando relatórios detalhados para o departamento de segurança e executivo.

- Deverá ser capaz de efetuar a verificação da reputação de anexos e caso a reputação do anexo não conste no banco de dados, a solução deverá ter a opção de enviar automaticamente o anexo para a nuvem do fabricante para análise em tempo real em sistema de SandBox do próprio fabricante caso o administrador opte por este serviço. Este sistema de SandBox deve conter tecnologia de detecção usando "Analise Comportamental" do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas.
- Deve possuir tecnologia SandBox local, isto é, efetuar o SandBox sem enviar o arquivo ao fabricante ou a terceiros, efetuando toda a análise de anexos dos emails localmente, atendendo dessa forma a legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais).
- A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita e os usuários que ignoraram através do Dashboard.
- A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS e FPT, URL's que comecem com "www" independente do protocolo.
- A solução deverá permitir que o administrador configure o sistema de proteção URL reescrevendo todas as mensagens que contiverem URL e enviado ao sandbox para testes garantindo um alto nível de segurança.
- A solução deverá prover lista de exceções de URL para que não sejam reescritas.
- O Dashboard deverá exibir o número de cliques em cada ameaça.
- O Dashboard deverá exibir qual usuário clicou na URL detectada como ameaça.
- O Dashboard deverá exibir informações atualizadas sobre as ameaças detectadas, deverá exibir a classificação da mensagem e deverá exibir status atualizado e detalhado sobre as ameaça no mínimo com as seguintes informações:
  - Clicado – Número de vezes que uma URL reescrita foi clicada por um usuário, inclusive se a mensagem for encaminhada para outro usuário e também for clicada.
  - Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso.
  - Permitida – Número de vezes que o modulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.
- O Dashboard deverá exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada.
- No Dashboard deverá ser possível filtrar uma URL em um campo de busca para analisar todas as ocorrências com aquela URL, bem como verificar o status atual dela e preview da página web.
- O Dashboard deverá possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta.
- No Dashboard deverá ser possível filtrar um IP em um campo de busca para analisar todas as ocorrências com aquele IP, bem como verificar o status atual dele e preview da página web.
- O Dashboard deverá disponibilizar sistema de coleta (report) de amostra do IP para a engenharia do fabricante analisar.
- O Dashboard deverá possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta.
- No Dashboard deverá ser possível analisar um arquivo, sendo enviado pelo administrador como amostra e retornar todas as ocorrências do arquivo enviado.
- O Dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta.
- A ferramenta de segurança contra ataques dirigidos, deve possuir o sistema colaborativo, ao qual o administrador poderá configurar que o usuário final possa indicar liberação e bloqueio de URL's, mesmo analisados pelo sistema e dessa forma reportando falsos positivos e falsos negativos. Deve prover também um Dashboard onde o Administrador poderá verificar todos reportes enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo.

- Deve possuir módulo de CDR “Content Disarm and Reconstruction”, que quando ativado irá remover conteúdos possivelmente perigoso, em no mínimo para os seguintes tipos:
  - JavaScript;
  - Links;
  - Executáveis;
  - VB Script;
    - De dentro de documentos, em no mínimo para os seguintes tipos:
- PDF;
- DOC;
- DOCX;
- PPT;
- PPTX;
- XLS;
- XLSX;
- Deve possuir capacidade de ignorar reescrita de algumas URL’s e não envio de arquivos para análise no SandBox do fabricante;
- O SandBox do fabricante deve ter a capacidade de analisar arquivos do tipo:
  - .swf;
  - .pdf;
  - .doc;
  - .xls;
  - .xlsx;
  - .ppt;
  - .ppt;
  - .pptx;
  - .rtf.

  Que estejam inseridos dentro de arquivos compactados.
- Deve ter a opção de não fazer reescrita de URL’s em casos de mensagens criptografadas, no mínimo com os sistemas de criptografia:
  - PGP;
  - S/MIME;
  - DKIM.
- Deve ter a opção de não fazer reescrita de URL’s em casos de mensagens oriundas de determinados países, por exemplo: Mensagens oriundas da China, Austrália e Belize;
- Deve poder desativar a reescrita de URL’s se a mensagem atingir uma pontuação de mínima de SPAM definida pelo administrador;
- Possibilidade do administrador de incluir URL’s, arquivos e IP’s em uma lista de bloqueio (Blacklist) no sistema de detecção;
- Possibilidade do administrador de incluir URL’s, arquivos e IP’s em uma lista segura (Whitelist) no sistema de detecção;

- **Do Sistema de Proteção a Fraudes de E-mail:**
  - A solução deverá ter a capacidade de detectar domínios recém adquiridos (tempo de considerado como recém adquirido deverá ser configurável pelo administrador) e indicar o que deve ser feito neste caso:
    - Pontuar;
    - Ignorar;
    - Bloquear.
  - Deve possuir capacidade de detecção de Spoofing de emails externos, isto é, ter a capacidade de comparar o domínio do cabeçalho do email (Header do Email/Envelope SMTP), com o domínio apresentado como remetente para o usuário final (Cabeçalho From) e indicar o que deve ser feito se forem diferentes:
    - Pontuar;

- Ignorar;
- Bloquear.

- O sistema deve possuir a opção de configurar regras para detectar emails que estejam utilizando ataques do tipo Look-A-Like Domain, isto é, detectar emails com domínios similares aos domínios utilizados pelo órgão.
- Deve possuir sistema de detecção de emails oriundos de servidores de emails gratuitos (free emails), tais como Google, Yahoo, Hotmail, etc, para serem usado em regras personalizadas de filtragem.
- Nativamente deve possuir sistema de detecção de emails externos (emails de entrada) que tentem utilizar o(s) domínio(s) da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

SUPORTE TÉCNICO DA CONTRATADA

- A garantia inclui as atualizações corretivas e evolutivas, disponibilizadas por meio de repositório personalizado para a **CONTRATANTE**, além do suporte técnico;

- O Suporte Técnico deve ser prestado durante os 12 meses de contrato, sob demanda e ativo, deverão ser executados por profissional com Certificado de Capacitação Oficial do Fabricante, que deverá emitir relatórios a respeito de eventuais incidentes específicos / apurações especiais, sob demanda da **CONTRATANTE**;

- O suporte técnico deve ter o regime de funcionamento 24x7, com chamados ilimitados e atendimento na língua portuguesa. Deve oferecer atendimento por telefone, *e-mail*, *web*, *Whatsapp* e/ou videoconferência. Deve incluir a resolução de incidentes e apoio operacional por meio de acesso remoto (VNC ou similar). Deverão ser realizadas visitas presenciais de suporte técnico quando não possível resolução nas formas informadas anteriormente;

INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO, COM A CORRESPONDENTE DOCUMENTAÇÃO

- A implantação do *software* será realizada em ambiente de produção acompanhada de repasse de conhecimento que se dará na modalidade presencial, com fornecimento de documentação técnica produzida pela **CONTRATADA**;

- A implantação deverá ser executada por profissional com Certificado de Capacitação Oficial do Fabricante;

- Engenharia da solução:

elaborar os documentos de planejamento do projeto e o desenho detalhado do projeto e sua implementação;

fornecer a garantia da melhor implementação da solução através do trabalho dos profissionais da **CONTRATANTE** junto com os especialistas da **CONTRATADA**;

detalhar em conjunto com a **CONTRATADA** o uso pretendido do equipamento e software, as características de uso das aplicações, dos dados, sistemas, requisitos de alta disponibilidade e desempenho;

definir a maneira de configurar o ambiente baseado nas expectativas e premissas;

realizar o planejamento inicial de implementação voltado para oferecer o melhor desempenho às aplicações, através do uso dos recursos disponíveis;

iniciar o trabalho de consultoria com a avaliação do ambiente atual, prosseguindo com o estudo do ambiente para o cenário final, confrontando a implementação com as melhores práticas recomendadas para o tipo de aplicação;

contemplar o plano de implementação do projeto com as configurações necessárias para a instalação e parametrização dos equipamentos;

avaliar do cenário inicial indicará ajustes e lacunas que devem ser endereçados para que a implementação seja bem-sucedida;

- Planejamento:

mapear e analisar a infraestrutura da **CONTRATANTE**;

avaliar incialmente a matriz de compatibilidade de todos os produtos de hardware e software que comporão a solução de modo a assegurar a compatibilidade e funcionalidade da implementação;

elaborar um projeto de implementação de cada componente e também do conjunto, considerando todos os elementos novos e existentes da **CONTRATANTE**, com respectivo cronograma de execução;

gerar a documentação extensiva e abrangente e será usada diretamente para a implementação do projeto.

incluir nesta fase as seguintes atividades, dependendo da disponibilidade de funcionalidades no hardware e na infraestrutura:

analisar o ambiente atual, através de coleta de informações, sejam elas fornecidas pela **CONTRATANTE** ou coletadas diretamente pela **CONTRATADA** para avaliar os tipos de dados a serem armazenados no ambiente;

planejar a configuração do ambiente de destino;

planejar os métodos de consolidação e migração quando necessários;

documentar a implementação geral em um documento de projeto;

documentar os detalhes do processo (configuração do ambiente e métodos de implementação) em um documento chamado “Documento de Especificação de Projeto – DEP” que será usado pelos engenheiros de sistema;

poderá ser elaborado documentos adicionais ao longo do projeto, em formato resumido, para facilitar a compreensão das diversas áreas envolvidas no projeto;

elaborar um programa de testes, na forma de um documento chamado “Caderno de Testes” (CT), que comprove o sucesso de cada atividade técnica realizada e que toda a implementação foi realizada de acordo com o projeto;

detalhar o DEP toda a configuração que será implementada baseado no desenho do projeto de hardware e software definidos. Toda a parametrização é documentada;

entender que o DEP permite que caso ocorra alguma falha ou problema toda a implementação possa ser refeita;

entender que o DEP não é uma documentação estática, havendo a necessidade, pode ser atualizado durante a execução do projeto;

os seguintes instrumentos de projeto serão gerados nesta fase:

documento de Especificação de Projeto que conterá as configurações de *hardware* e *software*, relevantes à implementação em questão, de todos os servidores, tais como:

diagrama Geral da Solução;

diagramas de Equipamentos;

definição de parametrizações e customizações pertinentes a solução;

lista de *patches* a serem instalados;

plano de Testes para a demonstração do serviço:

testes de *power-on e power-off* do ambiente;

teste das redundâncias implementadas;

REPASSE DE CONHECIMENTO

- Ao término da implantação, será realizado repasse de conhecimento na modalidade *hands-on* para 4 (quatro) empregados, com carga horária de 40 horas, a ser executado no período de duas semanas, com informações acerca dos produtos implementados, com o seguinte conteúdo:

informações gerais acerca do projeto;

informações gerais acerca dos produtos instalados;

arquitetura da solução;

parametrizações aplicadas nos produtos;

procedimentos de inicialização e parada do ambiente;

procedimentos de administração básica, relativos aos serviços configurados.

- O conteúdo explícito do *hands-on* será informado logo após a fase de engenharia da solução e deve ser validado e aceito pela **CONTRATANTE**.

5 – DEVERES E RESPONSABILIDADES DA CONTRATANTE

Nº	Descrição
1	A CONTRATANTE deverá fornecer a infraestrutura, os dados necessários para a implantação da solução e a equipe técnica para acompanhamento das atividades, devendo garantir o sigilo das informações.
2	A CONTRATANTE deverá fornecer a infraestrutura para necessária para realização do repasse de conhecimento contratada.
3	Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, e emitir o TERMO DE RECEBIMENTO PROVISÓRIO e TERMO DE RECEBIMENTO DEFINITIVO.

6 – DEVERES E RESPONSABILIDADES DA CONTRATADA

Nº	Descrição
1	Os serviços prestados pela CONTRATADA deverão obedecer aos requisitos estabelecidos no item 3 – DESCRIÇÃO DA SOLUÇÃO e 4 – ESPECIFICAÇÃO DA SOLUÇÃO. Os requisitos contemplados neste documento não esgotam todas as possibilidades de mensuração, ficando ressaltado que alterações, exclusões ou inclusões de novos itens serão possíveis, mediante acordo entre CONTRATADA e CONTRATANTE.
2	Propiciar à CONTRATANTE os meios e facilidades necessárias à fiscalização dos serviços, por meio de relatórios e *dashboards*, observando as penalidades cabíveis.
3	Comunicar à CONTRATANTE por escrito e em tempo hábil, qualquer dificuldade que esteja impedindo a execução do objeto, prestando os esclarecimentos necessários.
4	Fornecer à CONTRATANTE todas as informações solicitadas, no prazo de 5 (cinco) dias úteis.
5	Cumprir os prazos das atividades referentes a implantação das soluções, definidos no cronograma de execução elaborado na fase de planejamento.

7 – MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução		
Prazos	Assinatura do contrato	-

	Reunião de alinhamento do contrato	Em até 5 (cinco) dias úteis a partir da assinatura do contrato.
	Entrega do hardware	Até 30 dias após a assinatura do contrato.
	Entrega da licença do ambiente de software	Até 30 dias após a assinatura do contrato.
	Implantação (instalação, configuração, integração e documentação) das soluções	Em até 30 (trinta) dias úteis a partir da data de recebimento, pela **CONTRATADA**, da Ordem de Serviço. As fases de engenharia da solução e planejamento deverão ocorrer nos primeiros 9 (nove) dias úteis.
	Repasse de conhecimento presencial	A ser realizada logo após da conclusão da fase de implantação da solução.
	Suporte	A partir da concessão das licenças, pelo período de 12 (doze) meses.
	Vigência contratual	Até o fim do prazo do suporte contratado.
Horários	As atividades deverão estar compreendidas no período de 8h às 18h (horário de Brasília). Casos excepcionais serão avaliados pontualmente.	
Locais de Entrega	As atividades de implantação da solução de segurança cibernética, entrega de material e repasse de conhecimento serão na Sede da Instituição, situada na Avenida Duque de Caxias s/n Parte A - Setor Militar Urbano (SMU), em Brasília/DF.	

Quantidade mínima de bens ou serviços para comparação e controle

Os serviços serão controlados conforme item “8 - MODELO DE GESTÃO DO CONTRATO”.

Mecanismos Formais de Comunicação entre a Contratada e a Administração

A comunicação formal entre as partes deverá ser realizada através de sistema indicado pela CONTRATANTE.

Forma de Pagamento em Função dos Resultados

Pela implantação da solução, entrega de material e repasse de conhecimento, a CONTRATANTE pagará à CONTRATADA, após a implantação das soluções e Termo de Recebimento Provisório, a ser emitido após a execução parcial dos serviços, até o 10º (décimo) dia do mês subsequente ao da prestação do serviço, mediante atesto na Nota Fiscal a ser apresentada com 10 (dez) dias de antecedência do vencimento.

Etapa	Descrição da Etapa	Entregáveis	Valor em R$
1	Implantação	Instalação, entrega de material e integração da solução de segurança cibernética.	R$

8 – MODELO DE GESTÃO DO CONTRATO

Acompanhamento e fiscalização (incluindo a indicação de gestor e fiscais)

A execução deste contrato será acompanhada e fiscalizada por representantes da CONTRATANTE, credenciados no ato da assinatura do contrato.

A comunicação formal deverá ser realizada através de sistema indicado pela CONTRATANTE.

O representante designado deverá acompanhar a prestação de serviços, registrar as ocorrências e determinar as medidas necessárias ao fiel cumprimento do contrato, inclusive, poderá sustar a prestação de serviços parcialmente sempre que considerar a medida necessária.

O pagamento das notas fiscais está condicionado ao atesto da CONTRATANTE dos serviços prestados pela CONTRATADA.

Acordo de níveis de serviço – ANS

- O intervalo de tempo para início de atendimento do chamado, de acordo com a severidade, deve observar os critérios seguintes:

  severidade 1 (um): 2 (duas) horas;

  severidade 2 (dois): 4 (quatro) horas;

  severidade 3 (três): 8 (oito) horas;

  severidade 4 (quatro): 24 (quatro) horas.

- A severidade varia de 1 (um) a 4 (quatro), sendo 1 (um) a mais crítica e 4 (quatro) a menos crítica.

- A severidade é descrita da seguinte forma em um rol não taxativo:

  Severidade 1 (um) - Interrupção de serviço crítico:

  um serviço crítico em ambiente de produção está indisponível e nenhuma solução de contingência está disponível;

  um serviço crítico em ambiente de produção, como realização de *backup*, está parado ou não responde e não está sendo possível estabilizá-lo ou reiniciá-lo;

  Severidade 02 (dois) - Funcionalidades principais:

  uma ou mais funcionalidades estão severamente prejudicadas;

o uso da ferramenta pode continuar de forma restrita, apesar da produtividade em longo prazo poder ser afetada;

possíveis problemas críticos antes de uma atualização;

Existe uma solução de contorno temporária para o problema.

Severidade 03 (três) - Funcionalidades menores:

Uma ou mais funcionalidades não críticas não estão funcionando, existindo solução de contorno disponível;

Perda parcial, não crítica, de funcionalidade;

Funcionamento de alguns componentes prejudicados, permitindo a continuidade de uso;

Possíveis problemas não críticos antes de uma atualização.

Severidade 04 (quatro) - Perguntas gerais de utilização:

Questões referentes à aparência do produto, incluindo erros na documentação;

Dúvidas quanto à configuração geral ou quanto ao uso do produto;

Notificações sobre upgrade, grandes mudanças e migração;

Pedidos de melhorias.

Considerações gerais

As cláusulas contratuais de cunho administrativos e legais serão incluídas conforme modelo estabelecido pela Gerência de Compras e Contratos.

Em especial deverão ser atendidas as disposições da Lei nº 13.709/2018.

Critério de aceitação – Métrica e periodicidade

Métrica 1	
Indicador de Qualidade	Cumprimento das etapas definidas no item 7 – Modelo de Execução do Contrato, subitem Rotinas de Execução
Mínimo aceitável	100% da etapa
Métrica	Verificação dos entregáveis
Ferramentas	De acordo com os entregáveis da implantação
Periodicidade Aferição	Definida na reunião de alinhamento

Métrica 2	
Indicador de Qualidade	Cumprimento dos Acordos de Nível de Serviços - ANS
Mínimo aceitável	Conforme previsto nos ANS
Métrica	Conforme previsto nos ANS
Ferramentas	Conforme previsto nos ANS
Periodicidade Aferição	Mensal por meio dos *dashboards*

Metodologia / formas de avaliação da qualidade e adequação da solução às especificações funcionais e tecnológicas

Nos recebimentos provisório e definitivo da solução de segurança cibernética será verificada a aderência da solução implantada às especificações técnicas e às necessidades da instituição.

Sanções

O não cumprimento total ou parcial das obrigações assumidas, na forma e nos prazos estabelecidos, sujeitará a **CONTRATADA** às penalidades seguintes.

1. Advertência, em casos de inexecução total ou parcial do contrato, conforme a gravidade;
2. Multas Contratuais:
    - de 25% do valor global do contrato, em caso de atraso superior a 7 (sete) dias no prazo de execução da implantação (instalação, configuração,integração e documentação) e repasse de conhecimento das soluções;
    - de 1% ao dia, respeitando o limite de 25% do valor global do contrato, até que a CONTRATADA dê solução à inexecução do avançado ou até a rescisão contratual nos casos de inexecução parcial do contrato;
    - de 40% do valor global do contrato nos casos de inexecução total do contrato; e
    - até 20% (vinte por cento) do valor global do contrato, no caso de infringência por parte da CONTRATADA de disposições constantes na legislação e que não estejam abarcadas pelos demais itens desta cláusula.
3. Rescisão unilateral pela CONTRATANTE, em casos de inexecução total ou parcial do contrato, conforme a gravidade, sem prejuízo da aplicação das multas contratuais.

Os casos de descumprimento dos Acordos de Nível de Serviço (ANS), conforme definido nesta Especificação Técnica de Solução de TI, serão enquadrados, conforme a gravidade, como inexecução total ou parcial do contrato.

Em todas as situações, independentemente da aplicação de multas, poderá ser aplicada a pena de advertência, caso a CONTRATANTE julgue mais conveniente em face das circunstancias do caso específico.

As multas poderão ser aplicadas de forma isolada ou cumulativamente com qualquer das demais multas e/ou penalidades.

Não há necessidade de primeiro serem aplicadas penalidades mais brandas, podendo a CONTRATANTE, dependendo do ocorrido, aplicar diretamente as penalidades mais graves.

As penalidades poderão ser relevadas, no todo ou em parte, a critério da CONTRATANTE, desde que justificado e comprovado que o inadimplemento decorreu de caso fortuito ou de força maior.

Sendo rescindido o presente contrato, o pagamento devido será proporcional às etapas cumpridas até a data da resolução.

Para se ressarcir de eventuais prejuízos causados pela CONTRATADA e cobrar o valor da(s) multa(s) porventura aplicada(s), a CONTRATANTE poderá descontar o valor do prejuízo e da multa do pagamento decorrente deste contrato, dos valores devidos à CONTRATADA.

Caso o procedimento previsto no item anterior não baste para o pagamento do valor devido pela CONTRATADA, a CONTRATANTE ajuizará a cobrança judicial e ou a competente ação para reparação de danos, independentemente de prévia notificação (judicial ou extrajudicial), à CONTRATADA.

No processo de aplicação de penalidades, será sempre assegurado o direito ao contraditório e à ampla defesa.

9 – CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

ADJUDICAÇÃO DO OBJETO **x Preço global** **☐ Por lote** **☐ Por item**

Proposta Técnica

A proposta deverá ser entregue em papel timbrado da empresa e conter os itens abaixo:

Dados da empresa (CNPJ, razão social e contato do responsável);

- Valor unitário;
- Valor de implantação;
- Dados bancários da empresa (conta jurídica);
- Prazo de fornecimento e execução dos serviços;
- Data da proposta atualizada;
- Cronograma de implantação;
- Concordância com a forma de faturamento estabelecido no item 7 – Modelo de Execução do Contrato, subitem **Forma de Pagamento em Função dos Resultados**;
- Validade da proposta de pelo menos 60 (sessenta) dias;
- Estar devidamente assinada pelo responsável.

Id	Qualificação Técnica e Operacional (inclusive critério de sustentabilidade)	Descrição
1	Atestado de Capacidade Técnica	Para fins de qualificação técnica a **CONTRATADA** deverá apresentar à **CONTRATANTE** atestado ou declaração de capacidade técnica emitido por

		pessoa jurídica que comprove a prestação satisfatória de serviços, compatíveis em no mínimo 50 % da solução em características, quantidades e prazos com o objeto desta Especificação de Solução de TI.
2	Atestado de parceria do fabricante	Para fins de qualificação técnica a **CONTRATADA** deverá apresentar à **CONTRATANTE** atestado ou declaração de parceria, que comprove a autorização em revender e comercializar, prestar serviços e suporte técnico nos produtos descritos nesta Especificação de Solução de TI.
3	Declaração sobre Plano de Continuidade	A **CONTRATADA** deverá apresentar declaração sobre a existência de plano de continuidade de negócios, garantindo a prestação de serviços conforme estabelecido no item 3 – DESCRIÇÃO DA SOLUÇÃO e 4 – ESPECIFICAÇÃO DA SOLUÇÃO, se responsabilizando pela veracidade das informações prestadas.
4	Declaração sobre Auditoria	A **CONTRATADA** deverá declarar se é acompanhada por auditoria interna ou externa, se responsabilizando pela veracidade das informações prestadas, estando sujeita a sanções na forma da lei.
5	Certidão negativa de débitos trabalhistas	Certidão Negativa de débitos trabalhistas emitida pelo TST – Tribunal Superior do Trabalho.
6	Declaração de trabalho escravo	Declaração de que a empresa não consta no cadastro de empregadores que tenham submetidos trabalhadores à condição análoga de escrava, do Ministério do Trabalho e Emprego – MTE.
7	Caderno técnico	Caderno técnico (especificação técnica) oficial do fabricante de cada solução entregue

Critérios de julgamento

Conforme descrito no Item 2 – JUSTIFICATIVA DA CONTRATAÇÃO.

Id	Critérios	Justificativa

1	O menor preço ofertado	Buscar a proposta mais vantajosa para instituição desde que atendidos os critérios identificados.