EDITAL

CONTRATAÇÃO DIRETA: DISPENSA DE LICITAÇÃO nº 28/2024

Torna-se público que a Câmara Municipal de Monte Alegre do Sul/SP realizará contratação de pessoa jurídica de direito privado especializada em gerenciamento de central de operações de segurança (SOC), zelando pela proteção, monitoramento, suporte técnico e auditorias de conformidade em relação à Governança de TI e de Segurança da Informação.

I – DO OBJETO

Contratação de empresa especializada em gerenciamento de central de operações de segurança (SOC), zelando pela proteção, monitoramento, suporte técnico e auditorias de conformidade em relação à Governança de TI e de Segurança da Informação, utilizando ferramentas de segurança e monitoramento embarcadas no equipamento do tipo "appliance" (dispositivo especificamente dedicado e otimizado para executar funções relacionadas ao serviço, com alta confiabilidade e desempenho), o qual deverá ser fornecido em regime de comodato, pela empresa Contratada.

II – DA APRESENTAÇÃO DE ORÇAMENTO

Os interessados poderão, após visita técnica a ser agendada através do telefone 3899-1515, encaminhar os orçamentos aos seguintes endereços eletrônicos: a) administrativo@cmmontealegredosul.sp.gov.br ou b) compras@cmmontealegredosul.sp.gov.br, ou apresentar fisicamente no prédio-sede da Câmara Municipal de Monte Alegre do Sul/SP, localizado na Praça Coronel João Ferras, nº 45, Centro – Monte Alegre do Sul/SP.

III – DO PRAZO

O presente edital terá vigência de 03 (três) dias úteis a parte da publicação no sítio eletrônico oficial e mural de avisos deste Poder Legislativo

IV – DA CONTRATAÇÃO

Transcorrido o referido prazo de vigência deste Edital, a contratação se dará conforme o Termo de Referência anexo.

V – DAS DISPOSIÇÕES FINAIS

A) A apresentação de orçamento não implicará, de ofício, na contratação

B) Integram este Edital, para todos os fins e efeitos, o Termo de Referência em anexo.

Monte Alegre do Sul/SP, 04 de dezembro de 2024.

Atenciosamente,

LUIZ FABIANO FERREIRA
PRESIDENTE DA CÂMARA MUNICIPAL DE MONTE ALEGRE DO SUL/SP

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa especializada em gerenciamento de central de operações de segurança (SOC), zelando pela proteção, monitoramento, suporte técnico e auditorias de conformidade em relação à Governança de TI e de Segurança da Informação, utilizando ferramentas de segurança e monitoramento embarcadas no equipamento do tipo "appliance" (dispositivo especificamente dedicado e otimizado para executar funções relacionadas ao serviço, com alta confiabilidade e desempenho), o qual deverá ser fornecido em regime de comodato, pela empresa Contratada.

2. CONDIÇÕES GERAIS DA SOLUÇÃO

A Contratada deverá prestar serviços de gerenciamento de central de operações de segurança (SOC), zelando pela proteção, monitoramento, suporte técnico e auditorias de conformidade em relação à Governança de TI e de Segurança da Informação, utilizando ferramentas de segurança e monitoramento embarcadas no equipamento do tipo "appliance" (dispositivo especificamente dedicado e otimizado para executar funções relacionadas ao serviço, com alta confiabilidade e desempenho), o qual deverá ser fornecido em regime de comodato, pela empresa Contratada.

1. O equipamento deverá conter todas as soluções "embarcadas", ou seja, instaladas e prontas para uso centralizado.
2. O "appliance" deverá ser fornecido com todas as soluções embarcadas, tais como o sistema de monitoramento de redes e infraestrutura, o sistema centralizador de logs e o sistema para gestão de vulnerabilidades- fornecendo toda a observabilidade e proteção contínuas exigidas neste Termo de Referência em uma única interface, dispensando a necessidade de o operador alternar entre dispositivos ou aplicações distintas.
3. A Contratada deverá fornecer serviços continuados de auditoria técnica, para levantar as inconformidades e necessidades do ambiente, por meio de diagnósticos e processos, identificar soluções e, então, recomendar ações de melhoria bem direcionadas, tanto durante a instalação e implantação da solução quanto pelo período em que o contrato estiver vigente.
4. No que tange ao hardware e software componente da solução, a Contratada deverá fornecer suporte técnico e manutenção preventiva, corretiva, evolutiva, para identificação de problemas, falhas, instabilidades, comportamentos anômalos, queda de desempenho, dúvidas durante a vigência do contrato.

5. A Contratada, por virtude de suas atividades, pode apontar não conformidades na estrutura de TI da Contratante e como definido no item auditoria deve sugerir soluções para as não conformidades- incluindo orientações e especificações adicionais caso as soluções extrapolam a capacidade técnica ou operacional da equipe interna de TI.

6. O protocolo descrito no item anterior também deve ocorrer se nas auditorias periódicas forem detectadas inconformidades em serviços e ferramentas fornecidos por empresas privadas terceirizadas pela Contratante. Neste caso, a Contratada deverá recomendar correções ao departamento de TI mediante apresentação do relatório, documentando objeto da não conformidade, para fins de demonstração e resolução junto à empresa responsável.

7. A Contratante fornecerá um endereço de IP fixo para o equipamento dentro da infraestrutura de rede e TI que se pretende monitorar- provendo à contratada a conectividade necessária para o bom funcionamento das aplicações e serviços.

8. Possuir agentes compatíveis com os principais Sistemas Operacionais do mercado (Windows, MacOS e Linux) viabilizando o monitoramento de todos os itens especificados anteriormente sem qualquer prejuízo ou restrição na qualidade do monitoramento e proteção.

9. Permitir monitoramento e proteção contínua de ativos de rede sem a necessidade de configuração adicional por parte da equipe técnica da Contratante, devendo todos os itens mencionados neste Termo de Referência serem prontamente monitorados e exibidos na interface centralizada a partir do momento da efetivação de seu onboarding no sistema fornecido pela Contratada. Esta especificação tem por objetivo garantir a viabilidade técnica e fluidez da implantação do appliance.

10. Os operadores do sistema serão designados pela Contratante, tendo como atribuição a observação do sistema e tomada de ações imediatas de resposta, exceto quando fora do horário de expediente. Período no qual essa responsabilidade é totalmente atribuída à equipe de Analistas da contratada.

11. Todo procedimento de configuração e atualização contínua dos módulos e serviços "back-end" é de inteira responsabilidade da Contratada- de modo que os operadores possam manter seu foco no monitoramento e tomada de ações corretivas, por meio da interface "front-end" do appliance.

12. O monitoramento deve ocorrer ininterruptamente 7 dias por semana, com a Contratada sendo responsável por monitorar principalmente aos finais de semana e feriados os alertas da ferramenta de monitoramento- haja visto que nesta faixa horária os operadores e técnicos do staff interno da Contratante não estão em serviço.

3. CONDIÇÕES DO SERVIÇO DE NOC

A Contratada deverá ser responsável pelo monitoramento da infraestrutura interna de redes, servidores, endpoints e serviços, operando continuamente através de seu Centro de Operações com apoio de seu "appliance" instalado na estrutura, oferecendo no mínimo os seguintes recursos:

1. Detecção de problemas e instalação de software em dispositivos conectados à rede
2. Detecção de problemas e instalação de hardware em dispositivos conectados à rede
3. Gerenciamento de status e desempenho de infraestrutura e equipamentos de TI, incluindo, no mínimo o status em tempo real e dados históricos acerca de:
    a. Uso de memória RAM
    b. Uso de CPU
    c. Uso de disco (tanto a taxa de escrita/leitura quanto o volume de armazenamento ocupado).
    d. Status da(s) interface(s) de rede, tanto no contexto da rede local quanto da conectividade a internet.
    e. Monitoramento de uso da rede (volume histórico de dados enviados/recebidos por cada dispositivo monitorado) via NOC.
4. Monitoramento de status de serviços de firewall
5. Monitoramento de status de aplicações e protocolos essenciais ao funcionamento da rede (DHCP, DNS, etc).
6. Monitoramento e registro histórico do tempo de funcionamento (uptime) dos dispositivos.
7. Monitoramento de rede, incluindo análise do funcionamento e desempenho, relatórios técnicos voltados para correção e otimização da rede de modo geral ou em pontos específicos, com base nos dados coletados pelo NOC ao longo de toda a vigência do contrato.
8. Comunicar, através de canal especificado pela contratante, eventos de relevância ocorridos na rede (tanto no contexto de disponibilidade e desempenho quanto de conformidade técnica e segurança).
9. Viabilizar, através de veículo de comunicação de fácil acesso, a solicitação de relatórios personalizados acerca dos dados coletados e armazenados pelo NOC, para atender a qualquer demanda que possa surgir da Contratante no contexto de documentação, diagnóstico e controle de sua infraestrutura de T.I.
10. Comunicar à contratante sobre indisponibilidades de serviços incluídos no sistema de monitoramento e gerenciamento de logs- zelando para que o comunicado seja claro e objetivo acerca das especificações do problema, o ponto de origem e impacto para a infraestrutura.

11. Ainda no contexto de incidentes e problemas, a Contratada deve ser capaz de validar correções aplicadas pela Contratante, apresentando evidências técnicas de que o problema foi devidamente sanado.

12. Permitir conferir em tempo real o desempenho e disponibilidade de ativos de rede, incluindo servidores, endpoints e aplicações.

13. Possuir a possibilidade de monitoramento de infraestrutura com suporte ao protocolo SNMP para consulta e captura (polling e trapping).

14. Permitir a criação de checagens customizáveis (filtrando os dados pelo dispositivo de origem, o período analisado, entre outras formas de filtragem demandadas pela Contratante conforme as particularidades de sua infraestrutura).

15. Exibir os dados desejados em intervalos customizáveis.

16. O monitoramento poderá ser realizado por servidores/proxy e/ou clientes (agentes).

17. Permitir a definição de gatilhos de eventos sob demanda, com recursos de automação de alertas e notificações para a equipe ou profissional designado pela Contratante. As notificações devem ocorrer por qualquer meio comum e acessível de comunicação, não podendo gerar quaisquer custos adicionais para a Contratante.

18. A interface de NOC deve fornecer Gráficos em tempo real, que facilitem e otimizem a observabilidade da infraestrutura por meio de recursos visuais, sem necessidade de configuração por parte dos operadores.

19. Capacidade de monitoramento de aplicações web e sites.

20. Dados armazenados em banco de dados seguro inteiramente gerenciado pela Contratada- sendo de sua responsabilidade a manutenção, atualização e proteção deste componente.

21. Possuir Histórico configurável, incluindo a possibilidade de a Contratante definir uma política de retenção específica ainda na fase de implantação- viabilizando assim o estabelecimento de parâmetros de rotação de logs de NOC coerente com sua necessidade.

22. Permitir o registro/cadastro automatizado e simplificado de dispositivos no sistema de monitoramento, por meio de comunicação com "agentes" de fácil instalação e configuração- de modo que novos dispositivos possam ser facilmente incorporados sob o monitoramento em qualquer período durante a vigência do contrato.

23. A Contratada deve fornecer instruções claras e todo o suporte técnico necessário para o processo de inclusão de novos endpoints na infraestrutura monitorada.

24. Permitir a autenticação segura de usuário na interface de monitoramento, evitando que pessoal não autorizado tenha acesso a dados técnicos e restritos acerca da infraestrutura de T.I.

25. Permitir monitoramento com agente ou sem agente, viabilizando o monitoramento de dispositivos onde por algum motivo não se fez possível a instalação das aplicações "client side" (agentes) fornecidas pela contratada.

4. SISTEMA DE GERENCIAMENTO CENTRALIZADO DE INFORMAÇÕES DE SEGURANÇA (SIEM)

O Sistema deverá:

1. Permitir coleta e armazenamento eficiente e abrangente de logs de eventos.
2. Apresentar todos os logs de modo categorizado conforme o "nível" de criticidade do evento- permitindo a distinção clara de eventos altamente relevantes para o time técnico.
3. Oferecer redundância nos mecanismos de coleta de logs, utilizando dois ou mais agentes de coleta - de modo que se um dos agentes falhar o outro será capaz de manter a observabilidade do sistema.
4. Oferecer os dados de log consolidados por meio de representações gráficas claras e objetivas, os quais serão úteis para obter uma indicação visual clara de seus problemas, bem como apresentar suas descobertas para avaliação à alta administração em um formato que seja mais conveniente ao seu contexto.
5. Deve possibilitar a filtragem rápida e fácil dos dados apresentados pela interface gráfica, de modo que os logs exibidos possam ser limitados conforme o período monitorado e o dispositivo de origem, viabilizando análises precisas dos eventos.
6. Deve mostrar de forma clara o volume de eventos total registrado, tanto em tempo real quanto o volume histórico, distinguindo cada contagem pelo dispositivo de origem- necessários para identificação de picos de atividade e sua origem.
7. Arquivamento de seus registros por períodos prolongados ou predeterminados de tempo (semanas / meses / anos)- obedecendo à política de retenção de logs definida pela Contratante.
8. Permitir o monitoramento em tempo real de eventos sem restrições quanto ao volume de dispositivos monitorados, com a finalidade de agilizar a resposta quando ameaças, erros ou omissões são detectados.
9. Possuir sistema de análise de tendência para correlação de eventos e gerar seus próprios modelos e filtros personalizados que especificam se alguma atividade suspeita foi encontrada ou se outros problemas foram identificados pelo sistema e precisam ser corrigidos.
10. Opções de pesquisa avançada para rápida localização e classificação de dados pertinentes.
11. Permitir a coleta de registros de várias fontes, que podem ser unificados em um único recurso de registro e consulta universal.

12. As notificações devem permitir ser ajustadas de forma a serem ativadas somente quando determinados critérios (geralmente questões importantes) forem atendidos, reduzindo o tempo gasto na navegação por questões irrelevantes.

13. A contratada deve se responsabilizar por toda a parametrização dos gatilhos e alertas, incluindo sua atualização constante, visando manter o sistema de monitoramento sempre alinhado aos eventos relevantes e críticos no contexto atual de cibersegurança e conformidade.

14. Para garantir que o alerta seja visto por todas as partes envolvidas, o software de gerenciamento de log deve ser configurado para enviar notificações e resumos por e-mail.

5. SISTEMA DE SCANNER DE VULNERABILIDADES

5.1 - A Contratada deverá fornecer um sistema de scanner de vulnerabilidade com as seguintes características:

1. Disponibilizar cobertura aos "CVEs" (Common Vulnerabilities and Exposures).
2. Criar políticas de varreduras.
3. Possibilitar alta precisão de verificação, apresentando baixas taxas de falso positivo.
4. Possibilitar o agendamento de scans.
5. Disponibilizar verificação de vulnerabilidades em até 48 horas após a divulgação de nova vulnerabilidade.
6. Escaneamento sem agentes, facilitando um scan eventual.
7. Disponibilizar modelos pré-criados para análise de vulnerabilidades importantes e amplamente conhecidas.
8. Programação de scans para execução uma única vez ou de forma recorrente.
9. Apresentar o resultado das análises em tempo real.
10. Realizar análise de vulnerabilidades em ampla variedade de sistemas.
11. Possibilitar, via sistema, a visualização agrupada por vulnerabilidades semelhantes, facilitando o gerenciamento.
12. Classificar as vulnerabilidades por nível de criticidade.
13. Possuir interface WEB
14. Permitir que as varreduras sejam realizadas de maneira passiva (sem agente no endpoint) ou com agente de maneira ativa.

5.2- Os relatórios disponíveis no sistema de scanner de vulnerabilidade, deverão conter no mínimo, as seguintes características:

1. Apresentar a descrição da vulnerabilidade, seu impacto e sua correção.
2. Apresentar incidentes por categoria.
3. Ser exportados em diversos padrões do mercado, sendo eles CSV, PDF e XML.
4. Disponibilizar o resultado das análises de vulnerabilidades com recomendações de tratamentos para os incidentes.
5. Distribuir relatórios por e-mail automaticamente após finalização das análises.
6. O sistema deve permitir a avaliação de tendências entre os relatórios e alertar por e-mail em caso de alteração no nível de segurança de cada host.

5.3- Em relação aos recursos de gestão, operação e interface do usuário, implementação e suporte, estes deverão:

1. Permitir administração via interface GUI (Graphical User Interface).
2. Ter compatibilidade com sistemas operacionais Linux (Debian, Kali, Mint, Ubuntu, Fedora, Red HaEL, CentOS), Windows 10 e/ou 11, Windows Server (2012, 2012 R2 e 2016).
3. Implementar a solução por instalação embarcada em "appliance".
4. Possuir número ilimitado de IPs para análise de vulnerabilidade.
5. Fornecer relatórios mensais de todas as vulnerabilidades encontradas, assim como as ações a serem executadas para mitigar tais vulnerabilidades.

6. SISTEMA DE GESTÃO DE VULNERABILIDADES

1. Deve fornecer especificações claras acerca dos sistemas e versões de software vulneráveis- verificando automaticamente e alertando sobre versões e configurações que representam falhas na segurança do ambiente monitorado.
2. Deve proporcionar à Contratante uma visão de "inventário" das vulnerabilidades ativas no ambiente- com indicadores de criticidade, risco e ameaça.
3. O inventário de vulnerabilidades deve ser mantido e atualizado com base nas políticas de verificação e retenção acertadas junto ao time técnico da Contratante.
4. A interface deve ser intuitiva, no sentido de que a origem e criticidade de cada ameaça possa ser

compreendida sem exigir nenhuma análise técnica/complexa. Para isso, é padrão se utilizar de recursos gráficos como mapas de calor, formatação condicional, escalas de cores, entre outros.

5. Deve fornecer informações claras e precisas acerca das vulnerabilidades identificadas no ambiente, especificando o código de referência CVE associado- garantindo a identificação da brecha com base no padrão global.

6. Deve realizar o escaneamento, registro e alerta de vulnerabilidades de forma abrangente e passiva, de modo que os operadores internos nomeados pela Contratante não precisem em momento algum realizar configurações complexas para conseguir avaliar o nível de segurança do ambiente, suas falhas e pontos vulneráveis.

7. Deve permitir, através da interface centralizada do appliance, a filtragem de vulnerabilidades pela origem- tanto com base no software quanto no dispositivo vulnerável- agilizando a visualização e mitigação da ameaça por parte dos operadores.

8. Deve apontar a versão do software vulnerável, garantindo que os operadores possam identificar a correção necessária, atualizando para uma versão segura com facilidade e rapidez.

9. Dado seu caráter altamente técnico e volátil, a elaboração, configuração e atualização do sistema de gestão de vulnerabilidades fica sob inteira responsabilidade da Contratada- cabendo aos operadores apenas seu monitoramento e eventual tomada de ações corretivas.

7. SISTEMA DE DETECÇÃO DE INTRUSOS (IDS)

A Contratada deverá fornecer um sistema de detecção de intrusos com as seguintes características:

1. Interface de acesso web através de navegador- acessível através das mesmas credenciais dos demais módulos do appliance- não exigindo dos operadores o recadastramento e utilização de vários usuários/senhas.

2. Agir em modo passivo, capturando continuamente logs de todos os endpoints apontados pela Contratante.

3. Monitor de tráfego em tempo real, que deverá ser usado para monitorar o tráfego que entra e sai de uma rede em tempo real e emitirá alertas aos usuários quando detectar pacotes potencialmente maliciosos ou ameaças em redes de protocolo de internet (IP).

4. Logging e classificação automatizada de eventos críticos, para permitir o registro de atividades essenciais às técnicas de detecção de intrusão.

5. Análise do protocolo, processo de detecção de rede que captura dados em camadas de protocolo para análise adicional. Isso permite que o administrador de rede examine mais detalhadamente pacotes de dados potencialmente maliciosos, o que é crucial, por exemplo, na especificação da pilha de Protocolo de controle de transmissão (Transmission Control Protocol/IP, TCP/IP) .

6. Impressão digital do sistema operacional (SO), usa o conceito de que todas as plataformas têm uma pilha TCP/IP exclusiva. Por meio desse processo, pode ser usado para determinar a plataforma do sistema operacional que está sendo usada por um sistema que acessa uma rede.

7. Ser capaz de identificar e alertar em tempo real eventos característicos de invasões cibernéticas, com representações visuais claras e diretas acerca da origem, horário e natureza da ocorrência.

8. Possibilitar a inclusão, mediante solicitação formal da Contratante, de alertas e indicadores gráficos focados em eventos específicos.

9. Possibilitar o monitoramento de diretórios críticos do sistema operacional, cujo mapeamento é de inteira responsabilidade da Contratada. Por "críticos" deve-se entender todo e qualquer arquivo e pasta cujas operações de escrita, leitura e gravação podem representar indicadores de compromisso (IOC).

8. SISTEMA DE RESPOSTA ESTENDIDA A INCIDENTES (EDR/XDR).

O sistema de EDR/XDR é crucial para detectar e responder a ameaças avançadas em tempo real, aumentando a resiliência cibernética da instituição. Ao monitorar comportamentos suspeitos, responder automaticamente a incidentes e fornecer análises forenses detalhadas, o sistema impede que ataques causem maiores prejuízos. A integração desses dois sistemas cria uma abordagem robusta, que não só assegura a conformidade, mas também protege proativamente os ativos críticos contra ameaças em constante evolução.

1. Identificação automática de ameaças e ações imediatas para contê-las.
2. Coleta e análise constantes de dados de dispositivos para identificar atividades suspeitas.
3. Mecanismos de mitigação automatizados para conter ameaças assim que detectadas.
4. Monitoramento de padrões de comportamento para identificar atividades maliciosas.
5. Ferramentas para análise proativa de ameaças ocultas nos sistemas.
6. Integração de informações de fontes externas para atualizar a detecção de ameaças.
7. Capacidade de desconectar dispositivos infectados para limitar o impacto.
8. Console unificado para gerenciar e monitorar todos os endpoints.
9. Ferramentas de investigação para entender a origem e a trajetória da ameaça.

10. Detecção e bloqueio de tentativas de explorar vulnerabilidades.

11. Capacidade de integrar com sistemas de monitoramento e resposta centralizados (demais componentes descritos neste Termo de Referência).

12. Recebimento de atualizações constantes para se adaptar a novas ameaças.

13. Configurações específicas para diferentes grupos de dispositivos e usuários.

14. Compatibilidade com vários sistemas operacionais, como Windows, Linux e macOS.

15. Geração de relatórios e dashboards para análise e auditoria.

16. Capacidade de expandir a cobertura de endpoints sem perder desempenho.

9. SISTEMA DE CONFORMIDADE E GOVERNANÇA.

A implementação de um sistema de Conformidade e Governança é fundamental para que as instituições garantam o cumprimento de normas e políticas internas e externas, minimizando riscos legais e operacionais. Esse sistema possibilita a conformidade contínua ao monitorar, auditar e gerar relatórios de práticas de segurança, o que fortalece a postura regulatória e a confiança em auditorias. Com um controle completo sobre os ativos e políticas, a instituição reduz significativamente vulnerabilidades e acessos não autorizados. Para tanto, deve oferecer as seguintes funcionalidades:

1. Monitoramento Contínuo de Conformidade. Verificação constante de conformidade com normas regulatórias e políticas internas.

2. Inventário e Gestão de Ativos Catalogação automática de dispositivos, serviços e aplicações na infraestrutura.

3. Controle de Acesso. Gerenciamento e monitoramento de permissões para prevenir acessos não autorizados.

4. Auditoria de Logs e Atividades. Coleta e análise detalhada de registros de eventos e atividades em tempo real.

5. Análise de Integridade de Arquivos (FIM): Monitoramento de alterações em arquivos críticos para identificar atividades suspeitas.

6. Detecção de Vulnerabilidades. Identificação e alerta sobre fraquezas e falhas de segurança em sistemas e aplicações.

7. Verificação de Configuração. Avaliação de configurações dos sistemas e dispositivos para alinhamento com práticas de segurança.

8. Automação de Relatórios de Conformidade. Geração automática de relatórios que atendem a requisitos de auditoria e regulamentação.

9. Gerenciamento de Políticas de Segurança: Implementação e monitoramento de políticas de segurança para os ativos monitorados.

10. Integração com os demais módulos de segurança: Compatibilidade com NOC, SIEM, EDR e outras ferramentas para viabilizar o cruzamento entre os dados técnicos de e as regras compliance.

11. Alertas de Segurança em Tempo Real. Notificação imediata de incidentes que afetam a conformidade e a segurança.

12. Conformidade com Múltiplas Normas. Verificação automatizada com relação a normas que representam o alto padrão do mercado global de cibersegurança.

13. Análise de Riscos. Avaliação contínua do ambiente para identificar, medir e gerenciar riscos de segurança.

14. Gestão de Patches e Atualizações. Identificação de falhas corrigíveis por atualização e suporte para gestão de patches.

15. Suporte Multi-OS. Monitoramento de conformidade em múltiplos sistemas operacionais homologados pelo *National Vulnerability Database* (NVD), incluindo as distribuições oficiais Windows (sem restrição de versão), Linux e macOS.

16. Políticas Adaptativas de Controle de Acesso: Ajuste automático das permissões de acesso com base em mudanças nas políticas de segurança- a ser definido e atualizado continuamente pela Contratante mediante orientação técnica da Contratada.

17. Controle visual de Alterações de Configuração. Monitoramento de alterações nos sistemas que podem afetar a conformidade.

18. Os controles devem ser configurados pela Contratada, haja visto que o volume de regras jurídicas e detalhes técnicos a serem considerados para tanto são altamente complexos e evoluem continuamente.

19. Escalabilidade. Capacidade de suportar quantidades adicionais de ativos cuja conformidade técnica e jurídica é monitorada- sem impacto na performance de monitoramento e análise.

10. SUPORTE EM SEGURANÇA DA INFORMAÇÃO

Os serviços de suporte em segurança da informação consistem em inventariar e avaliar vulnerabilidades encontradas nos sistemas e recursos de TI e na solução de segurança fornecida, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas, obrigando-se a Contratada a auxiliar a contratante na mitigação das

vulnerabilidades encontradas, propondo ativamente as soluções e, em casos onde a solução for impossível, deverá administrar e documentar o "override" ou substituir as vulnerabilidades por host.

11. AUDITORIA CONTÍNUA EM SEGURANÇA DA INFORMAÇÃO E COMPLIANCE.

1. A Contratada deverá monitorar o sistema de detecção de intrusos identificando se o tipo de alerta é real ou falso positivo. Nos casos de alerta real deverá informar aos gestores do ambiente de TI.
2. O sistema de detecção de intrusos deverá emitir o alerta automaticamente e a Contratada definirá a gravidade e a severidade da ameaça.
3. A Contratada deverá realizar auditorias mensais nos servidores e entradas de DNS dos domínios utilizados pela Contratante e apresentar relatório das inconformidades encontradas incluindo entradas relativas à segurança de tráfego de e- mails tais como SPF, DKIM e DMARC.
4. A Contratada deverá realizar periodicamente testes de Phishing enviando e- mails para usuários aleatórios da Contratante e, em seguida apresentar relatório contendo os usuários que clicaram nos links enviados, para que seja possível treiná-los a fim de aumentar a consciência de segurança em todo o ambiente.

12. SERVIÇOS CONTINUADOS

A Contratada deverá realizar os serviços descritos abaixo, durante toda a vigência do contrato:

1. Manutenção preventiva de todos os módulos buscando melhor performance e diminuir a possibilidade de falha com interrupção dos serviços, lembrando que o centralizador de logs e o sistema de detecção de intrusos devem possuir um uptime (tempo de funcionamento total por mês) de 99% devido a importância de suas ações de segurança.
2. Manutenção corretiva de todos os módulos e do hardware do "appliance", sendo a Contratada responsável por toda manutenção corretiva necessária ao funcionamento do equipamento, incluindo substituição de peças e componentes além de substituição do equipamento em casos onde a manutenção cause uma interrupção maior do que o estabelecido no SLA.
3. Reconfiguração quando houver mudança de ambiente tecnológico.
4. Reconfiguração quando for necessário ações de segurança.
5. Reconfiguração quando a CONTRATANTE definir novas regras.

6. Acompanhamento dos relatórios de segurança auxiliando o departamento de TI na solução dos problemas encontrados.

7. SOC (security operations center) com monitoramento 24 horas, com ações pré definidas pela Contratante em casos de indisponibilidade de serviços e ativos de rede monitorados.

8. Realocação e reconfiguração do "appliance" se solicitado.

9. Os serviços devem ser prestados no local de instalação não sendo permitidos serviços de maneira remota.

10. Os serviços de centralização de operações de segurança devem ocorrer ininterruptamente 7 dias por semana, com a Contratada sendo responsável por monitorar principalmente aos finais de semana os alertas das ferramentas de segurança.