ANEXO I - ESPECIFICAÇÃO TÉCNICA

Contratação de solução de gestão e correlação de eventos de segurança da informação (SIEM) e gestão da resposta a incidentes de segurança da informação (SOAR), e demais serviços associados

1. ITEM 01 – SOLUÇÃO DE GESTÃO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO (SIEM) E GESTÃO DA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (SOAR).

1.1. REQUISITOS GERAIS DA SOLUÇÃO:

1.1.1. A solução deve ser composta pelos seguintes grupos de funcionalidades:

1.1.1.1. Gestão e correlação de eventos de segurança da informação SIEM (Security Event Manager) com suporte a análise comportamental e;

1.1.1.2. Gestão da resposta a incidentes de segurança da informação SOAR (Security Orchestration, Automation and Response).

1.1.2. Todos os equipamentos, produtos, peças ou softwares necessários à implementação da solução devem ser novos e de primeiro uso, não deverão constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Os produtos utilizados devem possuir licenciamento, garantia do fabricante e atualização de versão **pelo período de 5 anos**.

1.1.3. Os produtos utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a respectiva garantia.

1.1.4. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.

1.1.4.1. Caso a solução não possua licenciamento perpétuo, deverá permanecer com todas as funcionalidades ativas por pelo menos seis meses após o término da garantia.

1.1.5. As funcionalidades de gestão e correlação de eventos de segurança da informação SIEM (Security Event Manager) e gestão da resposta a incidentes de segurança da informação SOAR (Security Orchestration, Automation and Response) podem ser de fabricantes distintos desde que a integração entre as duas soluções sejam suportadas pelos respectivos fabricantes.

1.1.6. Todos os módulos que compõem a solução deverão se integrar visando constituir um ambiente homogêneo de análise, investigação, inteligência, defesa cibernética e resposta a incidentes.

1.1.7. Deverá ser entregue comprovação ponto a ponto de atendimento das características técnicas dos produtos aos requisitos exigidos neste Termo de Referência por meio da **transcrição de trecho** do documento oficial do fabricante que **comprove expressamente o atendimento da funcionalidade,** informando:

1.1.7.1. Qual é o documento;

1.1.7.2. Onde encontrar o documento;

1.1.7.3. Qual a página do documento;

1.1.7.4. Qual o parágrafo do documento.

1.1.8. Assume-se que todos os itens descritos abaixo estarão contemplados na solução independente de qual módulo da solução implementa a funcionalidade e do verbo aplicado ao item.

1.2. REQUISITOS GERAIS DAS FUNCIONALIDADES DE GESTÃO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO (SIEM):

1.2.1. A solução deve ser composta pelos seguintes grupos de funcionalidades:

1.2.1.1. Coleta de eventos de segurança (logs, eventos ou registros de auditoria)

1.2.1.2. Armazenamento de eventos e registros processados;

1.2.1.3. Analisar, processar e correlacionar eventos de segurança;

1.2.1.4. Análise de Comportamento de Usuários e dispositivos (User and entity behavior analytics (UEBA))

1.2.1.5. Contextualização e enriquecimento de dados com inteligência de ameaças;

1.2.1.6. Monitoramento de Tráfego de Rede com coletores especializados responsáveis pela extração de dados de segurança e captura de pacotes em tráfego de rede;

1.2.2. Deve implementar o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório Microsoft Active Directory e LDAP;

1.2.3. A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos padrões de mercado, de padrão aberto e reconhecidamente seguros garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP.

1.2.4. Juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, a contratada deverá prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento.

1.2.5. As funcionalidades de gestão e correlação de eventos de segurança da informação (SIEM) devem ser do mesmo fabricante.

1.2.5.1. Como exceção, as funcionalidades de Monitoramento de Tráfego de Rede com coletores especializados responsáveis pela extração de dados de segurança e captura de pacotes em tráfego de rede podem ser de fabricantes distintos desde que a integração entre as soluções seja suportada pelos respectivos fabricantes;

1.2.6. Todos os módulos que compõem a solução de SIEM deverão se integrar visando constituir um ambiente homogêneo de análise, investigação, inteligência, defesa cibernética e resposta a incidentes.

1.2.7. A solução de SIEM, bem como os softwares necessários para o funcionamento deverão ser instalados e executados **na infraestrutura do MPDFT**, com fornecimento de **todos os softwares necessários** para operação, incluindo todas as licenças necessárias para operação do software.

1.2.7.1. A Instalação deverá ser em **appliance virtual**, com todo software integrado pelo fabricante em formato compatível com a plataforma Vmware;

1.2.7.2. A CONTRATANTE irá fornecer os recursos de armazenamento e processamento necessários para a implantação da solução no ambiente de virtualização VMware.

1.2.7.3. Caso a solução necessite de outros softwares para seu funcionamento, como Sistema Gerenciador de Banco de Dados, Geradores de Relatórios etc., as licenças desses softwares deverão ser fornecidas no bojo da solução, sem ônus para o CONTRATANTE.

1.2.8. A solução deverá ser capaz de receber, interpretar, processar e correlacionar todos os eventos de segurança (logs, eventos ou registros de auditoria) e informações coletadas pelo monitoramento de tráfego de rede.

1.2.8.1. É importante que a integração e correlação de logs e eventos não sofra perdas de registros em eventuais casos de pico, devendo enfileirar os registros para processamento futuro nesses casos.

1.2.9. O SIEM deverá ser capaz de trazer contextualização e enriquecimento de dados para análises que serão realizadas pelo time de reposta a incidentes.

1.2.10. Deverá ser fornecido em arquitetura tolerante a falhas

1.3. REQUISITOS DAS FUNCIONALIDADES DE SIEM - INTERFACE DE GERENCIAMENTO, VISUALIZAÇÃO E RELATÓRIOS:

1.3.1. A solução deve implementar o gerenciamento dos componentes através de uma interface de gerência central;

1.3.2. A solução deve implementar a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

1.3.3. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.

1.3.4. Possuir interface web em HTML5;

1.3.5. Possuir a capacidade de efetuar o controle de acesso e a segregação de funções dos usuários da solução com base em papéis e perfis de usuário, de maneira que seja possível limitar os recursos da solução a grupos de usuários, conforme critério definidos;

1.3.6. A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;

1.3.7. Ofuscar os campos sensíveis dos eventos nas visualizações e relatórios gerados (senhas, identidade funcional, números de cartões de crédito e outros similares);

1.3.8. A solução deve ser capaz de integrar em uma única console de visualização, dados e metadados de eventos (logs e fluxos de rede), alertas e incidentes de segurança de modo que permita identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;

1.3.9. Deverá implementar visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário;

1.3.10. Deve ter capacidade de sumarizar múltiplos alertas idênticos automaticamente;

1.3.11. Deverá implementar a procura por texto, campos pré-definidos, palavras chaves, operações booleanas e expressões regulares em todo o conteúdo dos dados e metadados capturados;

1.3.12. Deverá implementar buscas complexas através do encadeamento de comandos de consulta (pipeline forma ou Lucene ou similar a SQL) para geração de relatórios e visualizações;

1.3.13. Deverá implementar a gravação da query de procura em formato de filtro

para utilização futura;

1.3.14. Deverá implementar a gravação dos resultados da pesquisa em arquivo ou na própria plataforma;

1.3.15. Deverá implementar funcionalidade assistente ou possuir textos informativos para facilitar a criação das queries;

1.3.16. Deverá implementar funcionalidade de listagem das queries realizadas ou salvas para facilitar o reuso em pesquisas;

1.3.17. A solução deve possuir a capacidade de navegação continua sobre os dados em formato "*drill down*" e pivoteamento, podendo realizar pesquisas avançadas para melhor correlação de eventos;

1.3.18. Deverá implementar a criação de *dashboards* customizados de tal modo que cada caso de uso implementado possa ter seu *dashboard*.

1.3.19. Deverá implementar dashboards para fins de monitoramento da solução, com visualização de métricas de volumetria de eventos (GB/dia) e utilização de CPU;

1.3.19.1. Caso a ferramenta utilize outra métrica, como EPS, a visualização acima deverá ser do licenciamento padrão da solução;

1.3.20. Deverá implementar a livre customização da interface, definindo página inicial por usuário e dashboards customizados;

1.3.21. Deve ser capaz de criar dashboards customizados, contendo apenas gráficos e tabelas escolhidas pelo usuário.

1.3.22. Deverá ser fornecido com dashboards pré-configurados e permitir a criação de novos dashboards;

1.3.23. Deverá permitir a fácil criação de uma vasta gama de efeitos visuais:

1.3.23.1. Tabelas;

1.3.23.2. Gráficos com agrupamento em período;

1.3.23.3. Linhas;

1.3.23.4. Barras;

1.3.23.5. Múltiplas áreas;

1.3.23.6. Pizza;

1.3.23.7. Elemento único (métrica ou contador simples);

1.3.23.8. Mapas Geo – IP.

1.3.24. Deverá implementar para todos os gráficos, capacidade de mudar títulos, legendas e rótulos do eixo e as configurações na própria interface;

1.3.25. A partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e fazer drill-down do mesmo para efetiva investigação e identificação de causa raiz;

1.3.26. Deve implementar a geração de relatórios gerenciais relativo aos eventos de todas as fontes de dados usadas para alimentar a solução.

1.3.27. Implementar a criação de novos relatórios e alteração dos existentes;

1.3.28. Deverá possuir relatórios pré-configurados separados em categorias;

1.3.29. Apresentar relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de serem gerados em pdf e csv;

1.3.30. Deverá implementar o agendamento de geração de relatórios periódicos, notificar ou enviar automaticamente os relatórios gerados para os destinatários;

1.4. REQUISITOS DAS FUNCIONALIDADES DE SIEM - DA COLETA DE EVENTOS DE SEGURANÇA:

1.4.1. A solução deverá estar dimensionada e licenciada para coleta, processamento e retenção de uma volumetria diária média **estimada** de **200 GB/dia ou 5.000 EPS** (Eventos por Segundo).

1.4.1.1. Caso não seja possível o licenciamento por GB/dia, será aceita métrica equivalente ao **GB/dia**, como por exemplo o *Message per Second* (MPS) ou Volume por Segundo (VPS), mas a CONTRATADA ao apresentar a proposta deverá converter a métrica utilizada para **GB/dia** de forma que todas as propostas estarão em conformidade com a métrica **GB/dia**.

1.4.1.2. Caso não seja possível o licenciamento por GB/dia, será aceito licenciamento por usuários (3500 usuários), mas a CONTRATADA ao apresentar a proposta deverá converter a métrica utilizada para **GB/dia** de forma que todas as propostas estarão em conformidade com a métrica **GB/dia**. Para essa conversão considerar a quantidade de usuários de **3500.**

1.4.2. A solução deverá suportar, em episódios de ataque ou sobrecarga de eventos, duas vezes seu volume licenciado durante 6 horas consecutivas, sem limites de ocorrências, mantendo o funcionamento da solução, sem perda de

eventos ou restrições de funcionalidades.

1.4.3. A solução deverá estar dimensionada para coleta de eventos de 500 fontes simultâneas.

1.4.4. Ser capaz de normalizar e categorizar os eventos em um padrão único que será usado pela solução;

1.4.5. O SIEM deverá ser capaz de receber, interpretar, processar e correlacionar todos os eventos de segurança (logs, eventos ou registros de auditoria) recebidos dos serviços de TI providos pelo MPDFT, que englobam os seguintes produtos e tecnologias, mas não limitados a:

1.4.5.1. Sophos XG Firewall: registros de firewall, IDS/IPS, filtro web, filtro de e-mail e VPN.

1.4.5.2. F5 Big IP: logs de requisições;

1.4.5.3. F5 Big IP DNS;

1.4.5.4. F5 Big IP WAF;

1.4.5.5. Office 365;

1.4.5.6. Microsft OneDrive e Sharepoint;

1.4.5.7. Microsft Exchange Local e em Nuvem (Microsft Exchange Online);

1.4.5.8. Mcafee Endpoit Security e Mcafee EPO: logs de segurança de endpoint, EDR e DLP.

1.4.5.9. VMWare;

1.4.5.10. Switches;

1.4.5.11. Roteadores;

1.4.5.12. Access points;

1.4.5.13. FreeRadius;

1.4.5.14. Logs de servidores Linux;

1.4.5.15. Logs e registros de servidores Windows Server;

1.4.5.16. Logs e registros de Windows Server Active Directory;

1.4.5.17. Logs de servidores Web como Apache e IIS;

1.4.5.18. Logs de servidores de aplicação como Tomcat e Jboss;

1.4.5.19. Logs e registros de Serviço de Gestão de Vulnerabilidades: Tenable SC;

1.4.5.20. Logs e registros de Solução de PAM (Privileged Access Management);

1.4.5.21. Logs de Banco de Dados como: SQL Server, Mysql, Postgres, Redis e MongoDB.

1.4.6. Caso a solução não implemente nativamente a coleta e processamento de algum tipo de evento produzido por algum elemento da estrutura de TI da CONTRATADA, deverá implementar a integração por configuração manual de conectores customizados. Tal integração devera ser feita e configurada durante a implantação da solução ou por abertura de chamado no suporte.

1.4.7. A solução deverá suportar a coleta dos logs de outros sistemas e ativos que venham a ser incorporados pelo MPDFT durante a vigência do contrato, mesmo que não conste inicialmente no Termo de Referência. Nesse caso, a contratada poderá implementar conectores customizados, caso a solução não tenha capacidade de recebimento do log nativamente.

1.4.8. Caso a fonte geradora de eventos não possuir capacidade de gerar eventos com riqueza de detalhes ou uteis para o processamento do SIEM, a CONTRATADA deverá disponibilizar módulos para coleta de eventos em endpoint.

1.4.9. Deverá coletar dados de feeds externos com no mínimo, os seguintes formatos/protocolos/fontes:

1.4.9.1. LDAP;

1.4.9.2. Bases de ameaças conhecidas (Threat Intelligence);

1.4.9.3. Bases de reputação de endereços IP e URLs;

1.4.9.4. Bases de Indicadores de comprometimento (IOC);

1.4.9.5. Base de Táticas, Técnicas e Procedimentos (TTPs – “Tactics, Techniques, and Procedures”) do framework MITRE ATT&CK;

1.4.9.6. Base de CVE;

1.4.9.7. WHOIS;

1.4.9.8. DNS Lookup;

1.4.10. Para coletar eventos de segurança deve implementar, no mínimo, os seguintes métodos/protocolos/formatos:

1.4.10.1. Syslog (TCP, UDP e TLS);

1.4.10.2. MySQL;

1.4.10.3. MS SQL;

1.4.10.4. Postgres;

1.4.10.5. Microsoft Windows Event Logging, coletados remotamente sem uso de agente de coleta (Por exemplo WMI, Windows Remote Management ou API);

1.4.10.6. API, coletados via requisições HTTP/HTTPS;

1.4.10.7. Logs armazenados em formato texto, compactados ou não;

1.4.10.8. Logs armazenados em SQL Database;

1.4.10.9. Arquivo texto;

1.4.10.10. Arquivo texto compactado;

1.4.10.11. Dados de segurança ou capturas de pacotes coletados pelos agentes de monitoramento de tráfego de rede;

1.4.10.12. Agente de coleta;

1.4.11. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de personalização de coletores, ou solução similar.

1.4.12. 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 neste edital;

1.4.13. A solução deve prover agentes coletores que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução.

1.4.14. Os coletores da solução deverão ser capazes de armazenar os dados localmente (*cache*) em caso de indisponibilidade da comunicação com os destinos dos eventos.

1.4.14.1. O envio dos dados em *cache* deve ocorrer imediatamente após a disponibilização do destino do evento.

1.4.15. A distribuição dos módulos, conectores ou agentes - o que for aplicável ao correto funcionamento da solução - no ambiente tecnológico deve ser livre, no sentido de permitir a conexão com os ativos do CONTRATANTE sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados;

1.4.16. Rotular eventos por zonas diferentes mesmo que estejam em redes com

mesmo endereçamento IP;

1.4.17. A solução deverá ajustar o horário dos eventos, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de sincronização de NTP (*Network Time Protocol*) com os servidores locais.

1.4.18. Deve ser capaz de acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;

1.4.19. Marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento;

1.4.20. Filtrar e selecionar os eventos que serão inseridos na solução e permitir a criação e alteração de filtros.

1.4.21. A camada de coleta deverá permitir ser instalada em modo distribuído, possibilitando a implementação de seus elementos o mais próximo possível dos dispositivos e softwares monitorados.

1.4.22. A solução deve ser capaz de enviar o evento bruto (raw) para o armazenamento e consulta futura;

1.4.23. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos

1.4.24. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução;

1.4.25. De forma a evitar a perda de eventos por sobrecarga ou indisponibilidade, a contratada deverá fornecer solução em arquitetura redundante e tolerante a falhas.

1.5. REQUISITOS DAS FUNCIONALIDADES DE SIEM - DO ARMAZENAMENTO:

1.5.1. Componente da solução responsável pela retenção dos dados coletados.

1.5.2. A solução deverá estar dimensionada e licenciada para armazenar, pesquisar e gerenciar os eventos de segurança por no **mínimo 90 dias** para fins de análise e resposta a incidentes.

1.5.2.1. Nesse modo de armazenamento as consultas ao SIEM deverão ser respondidas em no máximo 30 segundos, com exceção de relatórios.

1.5.2.1.1. Esse requisito será validado durante o Período de Funcionamento Experimental (PFE) previsto nos requisitos da contratação, dispensando sua comprovação com base em documentação exigida nos requisitos desse edital.

1.5.3. A solução deverá estar dimensionada e licenciada para armazenar, pesquisar e gerenciar os eventos de segurança por no **mínimo por 5 anos** para fins de auditoria.

1.5.3.1. Deverá ser capaz de configurar quais eventos de segurança serão armazenados por longos períodos para fins de auditoria.

1.5.4. A solução deve possuir a capacidade de gerenciar o armazenamento de longo prazo de eventos de auditoria em um repositório central (mínimo de 5 anos);

1.5.5. A solução deve possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.

1.5.6. Deverá ter capacidade de definir política de retenção dos dados;

1.5.7. Ter a capacidade de definir política de retenção dos dados on-line, ou seja, dados mantidos no banco de dados da solução, disponíveis para consulta imediata;

1.5.8. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão;

1.5.9. Deverá ter capacidade de armazenar os eventos em formato original (raw);

1.5.10. Deverá ter a capacidade de guardar eventos brutos em forma comprimida;

1.5.11. Deverá ter a capacidade de recuperar, sob demanda, registros sem modificação para preservação de evidência com qualidade forense;

1.5.12. De forma a permitir seu uso em auditorias e processos forenses, não deverá ser possível, a seleção e exclusão de eventos individuais. Deve ser possível apenas a exclusão de eventos conforme a política de retenção - ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros - ou por meio de tarefas administrativas;

1.5.13. Implementar o expurgo dos dados de forma automática com a personalização do período de tempo do expurgo

1.5.14. Deverá ser capaz de configurar a utilização de volumes de armazenamento locais e externos.

1.5.15. Deverá ser capaz de exportar eventos para formato texto ou csv ou JSON em estruturas NFS, SAN e localmente;

1.5.16. Implementar: políticas de controle de acesso aos dados, auditoria e tráfego dos dados criptografados com algoritmos padrões de mercado reconhecidamente seguros;

1.5.17. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.

1.5.18. A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;

1.6. REQUISITOS DAS FUNCIONALIDADES DE SIEM - DA ANÁLISE, PROCESSAMENTO E CORRELAÇÃO DE EVENTOS:

1.6.1. Componente da solução responsável pelo processamento, análise e correlação dos eventos coletados;

1.6.2. A solução deverá estar dimensionada e licenciada para efetuar a análise e correlação dos eventos em tempo próximo ao real (near real-time) de todos os dados recebidos;

1.6.2.1. Esse requisito será validado durante o Período de Funcionamento Experimental (PFE) previsto nos requisitos da contratação, dispensando sua comprovação com base em documentação exigida nos requisitos desse edital.

1.6.3. Deve ser capaz de criar novas regras de correlação e editar as já existentes.

1.6.4. Deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido;

1.6.5. Deve implementar a correlação de eventos e alertas com dados existentes em listas (watchlist). Deve implementar também a criação de novas listas e a personalização das existentes

1.6.6. Deve implementar a execução das regras de correlação em eventos passados para análise histórica de atividades suspeitas;

1.6.7. Deve implementar correlação de metadados dos eventos de segurança com as informações coletadas nas bases de ameaças conhecidas (Threat Intelligence);

1.6.8. Deve ter a capacidade de fazer a correlação de quaisquer tipos de eventos armazenados, incluído eventos de seguranças e informações coletadas pelo monitoramento de tráfego de rede;

1.6.9. Deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:

1.6.9.1. Severidade do evento;

1.6.9.2. Criticidade do ativo;

1.6.9.3. Existência de vulnerabilidade no ativo;

1.6.10. Possuir a funcionalidade de definição de prioridade para os eventos, alerta e incidente.

1.6.11. Como resultado da aplicação de regras de correlação a solução deve ser capaz de executar ações automáticas como: enviar e-mail; enviar mensagem para o usuário conectado ao console; executar comando; abrir, alterar e fechar casos na ferramenta de incidentes (SOAR); alterar dados de uma watchlist; gerar relatórios e alertas.

1.6.12. Implementar a criação de alarmes customizados pelo usuário, utilizando qualquer metadado armazenado como parâmetro para envio de alertas;

1.6.13. Implementar o envio dos alertas para tratamento dos incidentes em sistema de SOAR.

1.6.14. Deverá se integrar nativamente com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente.

1.6.15. Deve ser capaz de integrar com plataforma de chamados para abertura automática de ticket de acordo com o tipo e a gravidade dos alertas gerados.

1.6.15.1. Implementar integração com sistema SOAR utilizado no ITEM 04 - Serviço de gestão, descoberta e resposta a incidentes de segurança da informação (SIEM/SOAR)

1.6.15.2. Implementar integração via e-mail com plataforma de chamados OTRS (community versão 6) utilizada no MPDFT

1.6.16. Deverá implementar alertas por syslog e e-mail;

1.6.17. Fornecer a informação sobre os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.

1.6.18. Deverá prover a cadeia de eventos que culminaram no alerta.

1.6.19. Correlacionar os eventos coletados de forma a evidenciar incidentes que caracterizem um ataque.

1.6.20. A correlação de eventos deve possuir uma linha de base (baseline)

comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal;

1.6.21. Deverá possuir recurso de workflow automatizado, de forma que ações de criação, alteração e fechamento de casos possam ser realizadas automaticamente, como ações resultantes das regras de correlacionamento;

1.6.22. Deverá analisar o contexto do alerta para priorização de seu tratamento e redução de falso-positivo.

1.6.23. Deverá classificar os alertas identificados em função do risco.

1.6.24. As regras de correlação devem ser exportáveis usando formato padrão de mercado (JSON, XML, TXT ou CSV) ou padrão proprietário da solução.

1.6.25. Deverá utilizar técnicas de *machine learning* e inteligência artificial para detectar anomalias e para análise de eventos e alertas gerados.

1.6.25.1. Deve permitir ao administrador do sistema confirmar ou rejeitar eventuais comportamentos, com posterior inclusão de tal classificação no aprendizado.

1.6.26. Implementar detecção das seguintes atividades maliciosas:

1.6.26.1. Acesso a endereços IP e URLs conhecidamente maliciosas;

1.6.26.1.1. As informações sobre a reputação dos recursos acessados devem ser fornecidas por entidades especializadas em inteligência;

1.6.26.2. Acessos a aplicações realizados por mecanismos automatizados(bots).

1.6.26.3. Inundações de pacotes (floods);

1.6.26.4. Ataques a usuários e senhas de aplicações mediante tentativas sucessivas (força bruta ou ataques de dicionário);

1.6.26.5. Varreduras de redes para mapeamento de ativos e descoberta de vulnerabilidades;

1.6.26.6. Anomalias em comportamentos de usuário da rede interna para identificação de ameaças internas;

1.6.26.7. Injeções de comandos em aplicações;

1.6.26.8. Movimento lateral;

1.6.26.9. Uso indevido da rede, como tentativa de acessar arquivos que o usuário não tenha permissão;

1.6.26.10. Comprometimento de credenciais.

1.6.26.11. Comportamentos anômalos como acesso a domínios externos, acesso remoto a ativos que necessitam de acesso privilegiado e duração de login não usual ou fora de horário e local rotineiros.

1.6.26.12. Outros tipos de atividades maliciosas: deve permitir personalizar as correlações e detecções para atender necessidades específicas no MPDFT;

1.6.27. Implementar mapeamento das detecções de atividades maliciosas com as Táticas, Técnicas e Procedimentos (TTPs – "*Tactics, Techniques, and Procedures"*) do framework MITRE ATT&CK.

1.7. REQUISITOS DAS FUNCIONALIDADES DE SIEM - DA CONTEXTUALIZAÇÃO E ENRIQUECIMENTO DE DADOS COM INTELIGÊNCIA DE AMEAÇAS:

1.7.1. Deve incluir subscrição, durante o período do contrato de suporte e garantia, a base (via API) de ameaças conhecidas (Threat Intelligence), totalmente compatível com a solução ofertada.

1.7.2. A subscrição deverá prover acesso às seguintes informações:

1.7.2.1. Lista de endereços IP identificados como maliciosos;

1.7.2.2. Lista de URLs classificadas como maliciosas;

1.7.2.3. Lista de Indicadores de comprometimento (IOCs);

1.7.2.4. Reputação de sites;

1.7.2.5. Classificação de conteúdo de serviços Web;

1.7.2.6. Táticas, Técnicas e Procedimentos (TTPs – "Tactics, Techniques, and Procedures") do framework MITRE ATT&CK;

1.7.2.7. CVE;

1.7.2.8. WHOIS;

1.7.2.9. DNS Lookup;

1.7.3. As informações providas devem ser atualizadas dinamicamente, à medida que novas ameaças são detectadas na Internet;

1.7.4. O acesso aos dados da subscrição deve ser feito via HTTP REST API, de forma totalmente integrada e orquestrada pelo sistema;

1.7.5. A subscrição a base de ameaças conhecidas deve estar dimensionada e licenciada para correlação automatizada de metadados do volume de eventos processados pela solução;

1.7.6. Deve fornecer informações de Whois e Geolocalização para endereços IP e URL classificadas como ameaças;

1.7.7. As informações sobre endereços IP devem incluir quais tipos de ameaças foram identificadas, com pelo menos cinco das seguintes classificações ou equivalentes: exploits, phishing, botnet, DoS, scanners, proxies anônimos, malware, ransomware, DGA (Domain Generation Algorithm) ou origens de spam;

1.7.8. O provedor desses serviços deve possuir ciclo contínuo de tratamento das informações, utilizando fontes de detecção espalhadas por todo o mundo.

1.7.9. Além da subscrição a base de ameaças conhecidas, a solução deverá ser capaz de ter acesso a pelo menos três das seguintes fontes de informações via HTTP REST API em suas versões abertas e gratuitas: Shodan; Censys.io; Virus Total; Grey Noise e MISP - Open Source Threat Intelligence Platform;

1.7.9.1. Esse requisito será validado durante o Período de Funcionamento Experimental (PFE) previsto nos requisitos da contratação, dispensando sua comprovação com base em documentação exigida nos requisitos desse edital.

1.8. **REQUISITOS DAS FUNCIONALIDADES DE SIEM - REQUISITOS DE ANÁLISE DE COMPORTAMENTO DE USUÁRIOS E DISPOSITIVOS (USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)):**

1.8.1. Deverá implementar Análise de Comportamento de Usuários e dispositivos (User and entity behavior analytics (UEBA)) integrado ao SIEM, licenciado para análise de no mínimo **3.500 (três mil e quinhentos)** usuários simultâneos.

1.8.2. Deverá utilizar técnicas de *machine learning*, modelos estatísticos e inteligência artificial.

1.8.2.1. Deverá criar uma linha de base (*baseline*) de comportamento para usuários de forma que possa detectar desvios de comportamento, incluindo ameaças conhecidas, desconhecidas e ocultas.

1.8.2.2. O *baseline* deverá levar em consideração o grupo de segurança (por ex. grupo do Active Directory integrado) ao qual o usuário pertence.

1.8.3. Deverá atribuir um *score* (pontuação) de risco para cada usuário e para cada anomalia detectada de acordo com a gravidade/intensidade do desvio em

relação ao *baseline* de comportamento

1.8.3.1. Deverá ser possível analisar em detalhes a atividade de cada usuário ao longo do tempo.

1.8.3.2. Deverá ser possível monitorar usuários específicos.

1.8.3.3. Deverá ser possível relacionar várias formas de identificar um usuário, de forma que ele seja identificado como apenas um dentro da solução.

1.8.3.3.1. Deverá implementar a integração com LDAP e Active Directory para identificação de usuários e grupos.

1.8.3.4. Deverá ser possível determinar a lista de usuários privilegiados para um monitoramento rigoroso.

1.8.4. Deverá mostrar tendências de anomalias.

1.8.5. As anomalias detectadas devem ter um *score* (pontuação) de risco e devem ser analisadas levando em conta outros eventos detectados pelo SIEM para que ameaças maiores sejam relacionadas.

1.8.6. Os modelos de anomalias usados pelo UEBA devem permitir ao administrador do sistema confirmar ou rejeitar eventuais comportamentos, com posterior inclusão de tal classificação no aprendizado no intuito de diminuir os falsos-positivos.

1.8.7. Deverá ser capaz de aglutinar diversas anomalias relacionadas em apenas um ou poucos itens para análise e resolução mais rápida.

1.8.8. A funcionalidade de UEBA deverá dar suporte a detecção de no mínimo os seguintes tipos de ameaças:

1.8.8.1. Abuso de conta privilegiada.

1.8.8.2. Escalação de privilégios.

1.8.8.3. Exfiltração de dados (transferência não autorizada de dados).

1.8.8.4. Comprometimento de credenciais.

1.9. REQUISITOS DAS FUNCIONALIDADES DE SIEM - REQUISITOS DE MONITORAMENTO TRÁFEGO DE REDE:

1.9.1. Deverá fornecer Análise de Tráfego de Rede (Network Traffic Analysis (NTA)) integrado ao SIEM, tendo como insumo captura de pacotes em tráfego de rede;

1.9.2. Deverá fornecer coletores especializados responsáveis pela extração de dados de segurança e captura de pacotes em tráfego de rede;

1.9.3. A solução deve funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;

1.9.4. A solução deverá estar dimensionada e licenciada para análise de tráfego Ethernet com throughput contínuo de **1 Gbps (um gigabit por segundo);**

1.9.5. Realizar análises, aprendizado de máquina e detecções de eventos de segurança com base no tráfego monitorado;

1.9.6. Executar Deep Packet Inspection (DPI) em todo tráfego que chega às interfaces de coleta, identificando aplicações através de assinaturas, e não depender somente das portas (TPC/UDP) utilizadas para a identificação.

1.9.7. Deve realizar o parse de metadados em tempo real dos seguintes protocolos ou aplicações:

1.9.7.1. HTTP 1.0 e 1.1;

1.9.7.2. Domain Name System (DNS);

1.9.7.3. Bancos de dados: SQL Server, PostgreSQL (pgsql), MySQL;

1.9.7.4. Server Message Block (SMB), nas versões 1 e 2;

1.9.7.5. Transport Layer Security (TLS), nas versões 1.0, 1.1 e 1.2;

1.9.7.6. Simple Mail Transfer Protocol (SMTP);

1.9.7.7. Lightweight Directory Access Protocol;

1.9.7.8. FTP, POP, IMAP, HTTP, NFS, Oracle (SGBD), SSH, HTTPS, HTTP Proxy, Telnet, RDP, Websocket.

1.9.8. Deve extrair informações a partir da rede, de forma passiva, em portas espelhadas em switches (ex. SPAN, RSPAN) ou com a utilização de dispositivos passivos (TAPs). Não serão aceitas soluções intrusivas, que requeiram a instalação de softwares em servidores ou que atuem de forma ativa na rede;

1.9.9. Extrair metadados de requisições e respostas de todas as transações analisadas, inclusive lentas e/ou com erros, efetuadas nos protocolos suportados, exportando os detalhes de cada transação executada, de forma granular (sem sumarizar/agregar);

1.9.10. Reconstruir o conteúdo de requisições e respostas em protocolo HTTP;

1.9.11. A reconstrução das transações/eventos nos protocolos suportados deve ser

executada em tempo real.

1.9.12. Prover configuração de filtro de pacotes nas interfaces de coleta, utilizando informações de IP e portas TCP/UDP;

1.9.13. Fazer a coleta contínua de fluxos e pacotes completos, em formato PCAP. Esses dados devem ser relacionados em interface com os demais metadados extraídos dos protocolos de rede em camada de aplicação, permitindo assim filtrar os dados que serão analisados por flow ou transação de rede;

1.9.14. Deve licenciar funcionalidade integrada para reconstrução completa de arquivos, a partir dos PCAPs capturados, inclusive de arquivos anexos a e-mails, trafegados na web ou compartilhados entre usuários;

1.9.15. A solução deve possuir a capacidade de exportar e importar arquivos no formato packet capture (pcap);

1.9.16. A solução deve ser capaz de analisar tráfego IPv4 e IPv6;

1.10. **REQUISITOS DAS FUNCIONALIDADES DE SOAR:**

1.10.1. As funcionalidades de Gestão da resposta a incidentes de segurança da informação SOAR (Security Orchestration, Automation and Response) tem o objetivo de automatizar os processos e fluxos de trabalho, a aplicação de atividades rotineiras ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana.

1.10.2. As funcionalidades de SOAR, bem como os softwares necessários para o funcionamento dele poderão ser instalados e executados:

1.10.2.1. **Na infraestrutura do MPDFT**, com fornecimento de **todos os softwares necessários** para operação, incluindo todas as licenças necessárias para operação do software.

1.10.2.1.1. A Instalação deverá ser em **appliance virtual**, com todo software integrado pelo fabricante em formato compatível com a plataforma Vmware;

1.10.2.1.2. A CONTRATANTE irá fornecer os recursos de armazenamento e processamento necessários para a implantação da solução no ambiente de virtualização VMware.

1.10.2.1.3. Caso a solução necessite de outros softwares para seu funcionamento, como Sistema Gerenciador de Banco de Dados, Geradores de Relatórios etc., as licenças desses softwares deverão ser fornecidas no bojo da solução, sem ônus para o CONTRATANTE.

1.10.2.2. **Na nuvem do prestador de serviço ou do fabricante**, desde que em território brasileiro, e terão acesso à rede do MPDFT através de um canal seguro com criptografia.

1.10.2.2.1. A coleta de eventos e dados deverá ser realizada a partir de elemento instalado no ambiente do CONTRATANTE por questões de performance.

1.10.2.2.2. A CONTRATADA deverá providenciar, junto ao fabricante ou ao provedor do serviço em nuvem, a assinatura do Termo de Garantia de Privacidade dos dados referentes ao MPDFT, podendo ser este termo um padrão usado por ele no atendimento a questões de privacidade. O teor do termo padrão do fabricante/provedor será homologado por equipe especializada do MPDFT, para avaliação de cláusulas que possam ir contra o interesse institucional.

1.10.3. A equipe Segurança da Informação do MPDFT deverá ter acesso irrestrito ao SOAR, de tal forma que possa:

1.10.3.1. Atuar em conjunto com a CONTRATADA no tratamento dos incidentes.

1.10.3.2. Registrar e tratar diretamente incidentes em que a CONTRATADA não deverá atuar, conforme definido no PRI (Plano de Resposta a Incidentes – PRI**), descrito nos requisitos da contratação**.

1.10.4. O SOAR deve implementar a ingestão de dados no mínimo através de:

1.10.4.1. Alertas do SIEM;

1.10.4.2. Integração via API;

1.10.5. Licenciamento **estimado** para atendimento de **4 usuários** simultâneos do MPDFT, os usuários que serão utilizados pela CONTRATADA em seu Centro de Monitoramento e Resposta a Incidentes (CMRI) devem ser somados e gerenciados pela CONTRATADA;

1.10.6. A solução não deve limitar a quantidade de playbooks ativos.

1.10.7. A ferramenta deverá ser capaz de gerenciar eficazmente incidentes de segurança e privacidade da informação. De ser capaz de definir um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.

1.10.8. Deverá ser capaz de acompanhar todo o ciclo de vida de atendimento de um incidente.

1.10.8.1. Deverá prover métricas detalhadas do atendimento de cada incidente incluindo tempo de detecção, triagem, remediação e erradicação.

1.10.8.1.1. As métricas deverão ser monitoradas por incidente e por analista responsável pelo atendimento.

1.10.8.2. Deverá implementar a reconstrução do *timeline* dos incidentes.

1.10.9. Deverá ser capaz de automatizar processos e fluxos de trabalho.

1.10.10. Deverá ser capaz de gerenciar e mapear fluxos de trabalho (*workflows)* alinhados com procedimentos e processos.

1.10.11. Deverá implementar a criação de *playbooks* para execução e automação de acordo com o tipo de incidente a ser tratado.

1.10.12. Deverá implementar a criação e manutenção de base de conhecimento com extração de artigos que permitam o registro das lições aprendidas e a melhoria dos processos de respostas para outros incidentes, conforme previsto no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação**, descrito nos **requisitos da contratação.**

1.10.13. Deverá ter capacidade de automação integrada aos *workflows* e *playbooks* para integrar com soluções de segurança do mercado na investigação e resposta de incidentes.

1.10.14. Deverá implementar a criação de tipos customizados de incidentes.

1.10.15. Apresentar componente próprio para a modelagem e a automação de processos e fluxos de trabalho da solução.

1.10.16. Ser capaz de configurar os fluxos de automação, regras de decisão e aprovação.

1.10.17. Dispensar a necessidade da criação de tabelas, colunas e campos de banco de dados na solução, ou a necessidade de programação ou alteração do código-fonte, tornando estas alterações, quando necessárias, transparentes aos operadores e administradores que implementam os fluxos de trabalho.

1.10.18. Ser capaz de configurar painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva.

1.10.19. Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards da solução, o usuário possa clicar e listar os registros relacionados com os dados contidos no gráfico (funcionalidade drill down).

1.10.20. Deverá ser capaz de extrair e enriquecer, com dados de inteligência de ameaças (*threat intelligence*), indicadores de comprometimento (*Indicator of Compromise* - IOC) dos incidentes ou casos identificados.

1.10.21. Deverá ser capaz de extrair dados de inteligência de ameaças e indicadores de comprometimento (Indicator of Compromise - IOC) da ferramenta de SIEM.

1.10.22. Deverá implementar role-based access control (RBAC) com criação de papéis customizados.

1.10.23. Deverá ser capaz de relacionar diversos incidentes em casos para tratamento em conjunto, numa abordagem de gerenciamento por caso (*case management*).

1.10.24. Deverá implementar funcionalidades de colaboração para que a equipe do MPDFT possa interagir com a CONTRATADA através do sistema para a resolução de incidentes.

1.10.24.1. Toda interação de colaboração deverá ficar registrada no histórico do incidente.

1.10.25. Deverá utilizar técnicas de *machine learning* e/ou inteligência artificial para auxiliar na triagem e/ou resposta dos incidentes que forem detectados.

1.10.26. Deverá armazenar o registro de incidentes durante toda a validade do contrato do ITEM 04 - Serviço de gestão, descoberta e resposta a incidentes de segurança da informação (SIEM/SOAR).

1.10.26.1. Deverá prover trilha de auditoria de todos os incidentes detectados e tratados, contendo todas as ações tomadas, sejam automáticas ou manuais.

1.10.27. Deverá implementar a criação de *dashboards* customizados.

1.10.28. Deverá implementar a emissão de **relatórios customizados e agendados** com no mínimo as seguintes informações:

1.10.28.1. Top 10 tipos de incidentes tratados.

1.10.28.2. Tempo para detectar e declarar incidente.

1.10.28.3. Tempo entre a detecção e a contenção do incidente.

1.10.28.4. Top 10 tempo gasto por incidente.

1.10.28.5. Top 10 tempo gasto por severidade do incidente.

1.10.28.6. Top 10 incidentes por técnico responsável pelo atendimento.

1.10.29. Os relatórios deverão ser emitidos em formato PDF.

1.10.30. Deverá exportar o histórico dos incidentes tratados para fins de arquivamento ou migração de ferramenta em formatos padronizados como: XML, JSON ou CSV.

1.10.31. O SOAR deve ser capaz de gerar e escalar automaticamente os casos.

1.11. **GARANTIA:**

1.11.1. A solução deverá ter garantia de **5 anos**, para equipamentos, produtos e seus componentes, sem quaisquer ônus para a CONTRATANTE, a contar da data de emissão do Termo de Homologação, estendendo-se por todo o período de vigência do contrato. Subdivide-se em:

1.11.1.1. Garantia técnica evolutiva: fornecimento de novas versões e/ou releases corretivas e/ou evolutivas de softwares, lançadas durante a vigência do contrato, mesmo em caso de mudança de designação do nome. A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem. Inclui também, implementações de novas funcionalidades relativas aos equipamentos e produtos;

1.11.1.2. Garantia técnica corretiva: série de procedimentos executados para recolocar a solução em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

1.11.1.3. Garantia Técnica proativa: Manutenções proativas pré-acordadas entre CONTRADADA e CONTRATANTE para execução de análises, ações e correções que visem preservar funcionamento e otimizar desempenho dos equipamentos e produtos, seguindo melhores práticas recomendadas pela fabricante

1.11.1.4. Garantia técnica assistencial: atividades que incluem, mas não se limitam a execução e provimento de informação, assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (software) e dispositivos físicos (hardware); aplicação de correções (patches) e atualizações de software; diagnósticos, avaliações e resolução de problemas; ajustes finos e customização da solução; esclarecimento acerca das características dos produtos; e demais atividades relacionadas à correta operação e funcionamento da solução da melhor maneira possível.

1.11.2. A CONTRATADA deverá entregar documentação comprobatória da contratação da Garantia Técnica junto ao fabricante da solução ofertada;

1.11.2.1. A Garantia Técnica deverá ser em nome da CONTRATANTE;

1.11.2.2. A contratação da garantia técnica junto ao fabricante não exime a CONTRATADA das responsabilidades contratuais;

1.11.2.3. A Garantia Técnica deverá ser prestada pelo fabricante dos equipamentos e produtos ou pela rede de assistência técnica autorizada

que o represente, sempre sob responsabilidade da CONTRATADA.

1.11.3. A CONTRATADA deverá apresentar soluções definitivas para os problemas relatados e identificados por solicitação de garantia técnica pelo CONTRATANTE, dentro dos prazos e condições estabelecidos neste Termo de Referência;

1.11.4. A CONTRATADA prestará a garantia técnica on-site, remotamente ou por telefone sempre que se fizer necessário ou quando solicitado pelo CONTRATANTE. O tipo de atendimento será definido pela equipe técnica do CONTRATANTE;

1.11.5. A CONTRATADA deve disponibilizar Central de Atendimento para a abertura e fechamento de chamados de garantia técnica, conforme períodos e condições estabelecidas neste Termo de Referência;

1.11.6. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço de atendimento telefônico com discagem gratuita 0800 ou de custo local fixo e, adicionalmente, sítio Web ou e-mail, sem ônus adicional para a CONTRATANTE, para abertura e acompanhamento de chamados. É imprescindível que os funcionários de atendimento da CONTRATADA conheçam a solução CONTRATADA e estejam aptos a dar as informações básicas sobre a solução;

1.11.7. Os chamados provenientes dessa contratação deverão ter acesso prioritário à especialistas nas áreas técnicas convenientes

1.11.8. Os chamados abertos deverão ter acompanhamento de um Gerente de Serviços de TI

1.11.8.1. O gerente de serviços de TI deverá atuar no acompanhamento dos chamados, garantindo total atendimento dentro do Acordo de Nível de Serviço definido

1.11.9. Quando aplicável, serão emitidas em conjunto com o fechamento de chamados avaliações e sugestões de melhores práticas e ajustes do ambiente de TI do CONTRATANTE

1.11.10. A Garantia Técnica deverá, ao ser acionada, registrar o chamado, protocolar a data e hora da solicitação, nome do SOLICITANTE e descrição detalhada da solicitação;

1.11.11. A CONTRATADA encaminhará mensagem de e-mail para endereço a ser indicado pelo CONTRATANTE informando o número de protocolo do chamado técnico, data e hora de abertura e sua descrição;

1.11.12. O serviço de abertura de chamados para a garantia deverá ser realizado em regime de 24x7 (vinte e quatro horas por dia, sete dias por semana), todos os dias do ano, no idioma português, incluindo o atendimento telefônico, o

e-mail e o sítio Web;

1.11.13. A critério do CONTRATANTE, o atendimento às solicitações deverá ser realizado nas instalações do CONTRATANTE (on-site) e não poderá ser interrompido até o completo reestabelecimento dos equipamentos e da solução, mesmo que se estenda por períodos noturnos, sábados, domingos e feriados, salvo acordo prévio e expresso com a CONTRATANTE. Também não implicará em custos adicionais ao CONTRATANTE;

1.11.14. A interrupção do atendimento por parte da CONTRATADA e sem a prévia autorização da equipe técnica do CONTRATANTE poderá ensejar na aplicação das penalidades previstas;

1.11.15. Deverá haver uma descrição da solução, imediatamente após fechamento dos chamados, acerca das soluções aplicadas para definitivamente retornar a solução ao pleno estado de funcionamento. Essa descrição deverá fornecer em detalhes, por e-mail ou via sítio Web, a solução para o problema detectado. Deverá cobrir todo e qualquer defeito apresentado no serviço, incluindo todos os componentes da solução, equipamentos de comunicação, peças e esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias;

1.11.16. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componentes da solução, essa deverá ocorrer sem custo adicional para o CONTRATANTE;

1.11.17. No caso de substituição temporária, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas com a anuência do CONTRATANTE.

1.11.18. A substituição temporária do equipamento, peça e componente será por até 30 dias, ficando suspensa a contagem do prazo de solução definitiva;

1.11.19. A CONTRATADA substituirá, no prazo máximo de 10 (dez) dias, qualquer equipamento que venha a se enquadrar em, pelo menos, um dos seguintes casos:

1.11.19.1. Indisponibilidade ocasionada por componente defeituoso que não tenha sido substituído no prazo de até 4 (quatro) dias;

1.11.19.2. Ocorrência de 3 (três) ou mais substituições de um mesmo componente do equipamento dentro de um período contínuo de 60 (sessenta) dias;

1.11.19.3. Se a soma dos tempos de indisponibilidade de um mesmo componente ultrapassar 48 (quarenta e oito) horas dentro de um período contínuo de 90 (noventa) dias;

1.11.19.4. Se a soma dos tempos em que o equipamento apresentar

indisponibilidade total, comprometimento de performance ou de funcionalidade ultrapassar 48 (quarenta e oito) horas dentro de um período contínuo de 60 (sessenta) dias.

1.11.20. No caso de substituição definitiva, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas, serem novas e de primeiro uso;

1.11.21. O envio para centros de Garantia técnica em outra localidade não exime a CONTRATADA do cumprimento dos prazos estabelecidos nos níveis de serviço exigidos;

1.11.22. Para a remoção de equipamento, peça e componente será necessária autorização de saída emitida pelo Fiscal do Contrato, a ser concedida ao funcionário da CONTRATADA, formalmente identificado.

1.11.23. A CONTRATADA deve prover as correções e atualizações mais recentes dos hardwares instalados, tais como firmware, que permitam melhorar as funcionalidades dos equipamentos e mantê-los compatíveis com os demais componentes de hardware e software do parque tecnológico do MPDFT, sem ônus adicional para ao CONTRATANTE;

1.11.24. A CONTRATADA deve prestar as informações e/ou esclarecimentos que venham a ser solicitados pela equipe técnica do CONTRATANTE referente a qualquer problema detectado ou sobre o andamento das atividades de manutenção;

1.11.25. A CONTRATADA deve assegurar a Garantia Técnica necessária ao perfeito funcionamento dos equipamentos e produtos que compõem a solução, efetuando ajustes, reparos ou substituição parcial ou total dos equipamentos, peças e partes sob sua propriedade e responsabilidade, sem ônus adicionais para o CONTRATANTE.

1.11.26. Todas as despesas decorrentes da necessidade de substituição de equipamentos, infraestrutura, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional à CONTRATANTE;

1.11.27. A CONTRATADA responderá por quaisquer prejuízos que seus empregados causarem ao patrimônio do CONTRATANTE ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente.

1.11.28. A CONTRATADA arcará com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução CONTRATADA, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.

1.11.29. Possuir recurso disponibilizado via web, site do próprio fabricante (informar url para comprovação), que permita verificar a garantia do equipamento e/ou produtos através da inserção do seu número de série;

1.11.29.1. Caso o fabricante não possua esse serviço WEB de validação poderá ser apresentada documentação fornecida pelo fabricante detalhando o licenciamento, produtos e vigência;

1.11.30. Oferecer serviço e ferramentas de diagnóstico e troubleshooting remotos na qual os técnicos da CONTRATADA se conectam diretamente ao sistema do usuário através de uma conexão de Internet segura para agilizar e melhorar o processo de solução de problemas;

1.11.31. A CONTRATADA se compromete a utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações neste Termo de Referência.

1.11.32. Os chamados técnicos serão categorizados nas severidades Alta, Média e Baixa, devendo ser atendidos nos prazos especificados neste edital nos **Níveis Mínimos de Serviço Exigidos (NMSE)**.

1.11.33. Serão considerados, para efeito do nível de serviço exigido:

1.11.33.1. Término do atendimento: Tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução definitiva da demanda pela CONTRATADA.

1.11.34. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas;

1.11.35. A severidade do chamado será informada pela CONTRATANTE no momento da sua abertura e seguirá o disposto neste edital nos **Níveis Mínimos de Serviço Exigidos (NMSE)**;

1.11.36. A severidade poderá ser reclassificada pela CONTRATANTE. Caso isso ocorra, haverá nova contagem de prazo, conforme a nova severidade e seguirá os prazos dispostos neste edital nos **Níveis Mínimos de Serviço Exigidos (NMSE)**;

1.11.37. É vedado à CONTRATADA interromper o atendimento de severidade ALTA até que o equipamento esteja em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Ainda assim, não haverá custos adicionais à CONTRATANTE.

1.11.38. É necessária autorização da CONTRATANTE para qualquer

modificação na solução;

1.11.39. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a garantia;

1.11.40. A CONTRATADA deverá ser parceira autorizada do fabricante estando apta e autorizada a fornecer o objeto, conforme Termo de Referência.

2. ITEM 02 - SERVIÇO DE INSTALAÇÃO E IMPLANTAÇÃO DA SOLUÇÃO.

2.1. Para todo o produto (hardware ou software) adquirido no escopo do **ITEM 1** deverá ser fornecido serviço especializado de instalação, customização e configuração da solução contratada no ambiente do MPDFT. Entende-se por serviço especializado de instalação, customização e configuração a montagem física dos equipamentos e seus respectivos acessórios pela CONTRATADA, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com a necessidade do MPDFT.

2.2. A implantação deverá ser realizada por profissionais certificados e qualificados para customizar as ferramentas às necessidades do MPDFT, devendo ter a orientação profissional do fabricante da solução nas atividades de elaboração do projeto de implantação dos casos de uso da solução e na validação da configuração feita durante a implantação.

2.2.1. **Justificativa**: A implantação de uma ferramenta e de um serviço de resposta a incidentes é complexo e para sua customização são necessários conhecimentos técnicos especializados que profissionais certificados e qualificados pelo fabricante podem prover. A equipe técnica do MPDFT não tem conhecimento na solução e somente a transferência de conhecimento prevista no Edital não é suficiente para ter o completo domínio da solução.

2.3. O serviço contempla:

2.3.1. Instalação, customização e configuração da solução no ambiente da CONTRATADA, incluindo:

2.3.1.1. Desenvolvimento de políticas e processos de manutenção de logs para as fontes, bem como procedimentos e processos de revisão.

2.3.1.2. Desenvolvimento da arquitetura de gerenciamento de logs de acordo com o ambiente implantado, desenvolvendo filtros, formas de agregação, retenção e configuração das fontes.

2.3.1.3. Definição, planejamento, implementação do recebimento de logs

originados nas fontes monitoradas.

2.3.1.4. Criação de conectores ou *parsing* para recebimento de logs por elementos que não tenham conectores na solução implantada, incluindo no mínimo os conectores e *parsing* para as tecnologias listadas neste edital.

2.3.2. Implementação inicial do Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança, descrito nos requisitos da contratação;

2.3.3. Implementação inicial do Processo de Identificação e Resposta a Incidentes de Segurança da Informação, descrito nos requisitos da contratação;

2.3.4. Elaboração de **Plano de resposta a incidentes (PRI)** previsto no Processo de Identificação e Resposta a Incidentes de Segurança da Informação no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação,** descrito nos requisitos da contratação;

2.3.5. Desenvolvimento de modelo de relatório mensal, que será utilizado no serviço mensal **(ITEM 4)** com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados.

2.3.6. Desenvolvimento de modelo de relatório mensal, que será utilizado no serviço mensal **(ITEM 4)** com análise de tendências de incidentes de segurança da informação.

2.3.7. Importação de logs antigos armazenados no servidor Syslog da CONTRATANTE e implementação e configuração dos relatórios dos Casos de Uso de Auditoria.

2.4. Para o aceite do Serviço de instalação e implantação da solução, a CONTRATADA deverá:

2.4.1. Implementar em conjunto com o CONTRATANTE no mínimo 5 (cinco) entre os casos de uso de monitoramento de segurança previstos nos requisitos do Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança.

2.4.2. Implementar em conjunto com o CONTRATANTE no mínimo 5 (cinco) entre casos de uso de auditoria previstos nos requisitos do Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança.

2.4.3. A CONTRATADA deverá promover a automação de processos e fluxos de trabalho e desenvolver no mínimo **5 *playbooks*** na ferramenta de SOAR para auxiliar no tratamento dos incidentes identificados com a implantação dos casos de uso de monitoramento de segurança;

2.4.4. Entregar o Plano de respostas a incidentes (PRI) previsto nos requisitos do

Processo de Identificação e Resposta a Incidentes de Segurança da Informação

2.4.5. Entregar modelo de relatório mensal, que será utilizado no serviço continuado (**ITEM 4**) com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados.

2.4.6. Entregar modelo de relatório mensal, que será utilizado no serviço continuado (**ITEM 4**) com análise de tendências de incidentes de segurança da informação.

2.4.7. Entregar documentação sobre o ambiente do MPDFT, descrita nos requisitos da contratação, para que qualquer funcionário que seja encarregado de trabalhar na prestação ou fiscalização do serviço - **ITEM 04** - seja treinado com base nessa documentação.

2.4.8. Finalizar o PFE - Período de Funcionamento Experimental, conforme descrito nos requisitos da contratação.

3. ITEM 03 – TRANSFERÊCIA DE CONHECIMENTO

3.1. Para todo o produto adquirido no escopo do **ITEM 1** deverá ser fornecida uma transferência de conhecimento.

3.2. A transferência de conhecimento deverá ser ministrada por profissional certificado pelo fabricante.

3.3. A CONTRATADA deverá apresentar um Plano de Transferência de Conhecimento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

3.4. O Plano citado no item anterior deverá apresentar o programa de cada transferência de conhecimento com conteúdo, carga horária, duração em dias e avaliações de aprendizagem;

3.5. A transferência de conhecimento pode ser pela manhã, manhã e tarde, ou de noite, a critério da CONTRATANTE;

3.6. O Transferência de conhecimento deverá ser em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração e utilização delas;

3.7. A transferência de conhecimento deverá prever a capacitação para 6 alunos divididos em 2 turmas;

3.8. Para que uma transferência de conhecimento seja considerada efetiva deverá ser considerada satisfatória por pelo menos 70% dos treinandos;

3.9. A CONTRATANTE poderá avaliar as transferências de conhecimentos com meios próprios e, caso este seja julgado deficiente, a CONTRATADA deverá prover o devido reforço;

3.10. A CONTRATADA deverá prover toda a estrutura para as transferências de conhecimentos;

3.11. A transferência de conhecimento será realizada na modalidade de ensino a distância (EAD);

3.11.1. Em casos excepcionais a serem julgados pela CONTRATADA a transferência de conhecimento poderá ser realizada presencialmente em Brasília.

3.12. Todo material didático disponibilizado na transferência de conhecimento deverá ser fornecido pela CONTRATADA e estarão inclusos no escopo da transferência de conhecimento;

3.13. Ao final de cada transferência de conhecimento, cada treinando deverá receber um certificado de participação;

3.13.1. No certificado de participação de que trata o item anterior deverá constar todas as informações exigidas pela Secretaria de gestão de pessoas do MPDFT para que o mesmo seja homologado. Minimamente, mas não limitado a: nome completo do aluno, data de execução da transferência de conhecimento, carga horária e ementa do curso;

3.14. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades da transferência de conhecimento;

3.15. A fim de que os técnicos da CONTRATANTE possam avaliar com precisão a solução durante o Período de Funcionamento Experimental (PFE), ao menos uma turma da transferência de conhecimento deve ser finalizada antes do início deste.

4. ITEM 04 – SERVIÇO DE GESTÃO, DESCOBERTA E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (SIEM/SOAR)

4.1. O Serviço de gestão, descoberta e resposta a incidentes de segurança da informação (SIEM/SOAR), **pelo período de 36 meses**, engloba:

4.1.1. Suporte Técnico para a solução adquirida, engloba: o monitoramento, operação, administração e assistência técnica de todos os componentes da solução fornecido pela CONTRATADA;

4.1.2. Atividades operacionais de segurança: atividades operacionais de monitoramento e resposta a incidentes de segurança:

4.1.2.1. Processo contínuo de Desenvolvimento e Manutenção de Casos de Uso de Segurança e;

4.1.2.1.1. Os requisitos desse processo estão listados nos requisitos da contratação.

4.1.2.2. Processo de Identificação e Resposta a Incidentes de Segurança da Informação;

4.1.2.2.1. Os requisitos desse processo estão listados nos requisitos da contratação.

4.2. O serviço deverá ser executado com base nos processos descritos neste edital e frameworks do NIST (National Institute of Standards and Technology) e SANS Institute para resposta a incidente de segurança da informação.

4.3. O serviço deve estar totalmente funcional no início do Período de Funcionamento Experimental – PFE, estendendo-se por todo o período de vigência do Contrato;

4.4. Os serviços deverão ser realizados por profissionais certificados e qualificados para operar as ferramentas.

4.4.1. **Justificativa**: O gerenciamento da solução e de um serviço de resposta a incidentes é complexo e para sua administração são necessários conhecimentos técnicos especializados que profissionais certificados e qualificados podem prover. A equipe técnica do MPDFT não tem conhecimento na solução e somente a transferência de conhecimento prevista no Edital não é suficiente para ter o completo domínio da solução.

4.5. Os serviços deverão ser prestados preferencialmente de forma remota;

4.6. O serviço deverá cobrir a localidade de Brasília/DF;

4.7. Os serviços contratados serão prestados em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

4.8. Sem apresentar qualquer ônus adicional à CONTRATANTE, o Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado incluindo, mas não se limitando a: esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias, acionar a garantia do produto para substituição total ou parcial do produto como peças, partes, componentes ou acessórios;

4.9. A CONTRATANTE poderá, a qualquer momento, determinar à CONTRATADA a execução de rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos;

4.10. Serviços de assistência técnica deverão ser executados pela CONTRATADA sempre que se fizer necessário, independentemente de haver solicitação por parte da CONTRATANTE;

4.11. A realização de assistência técnica preventiva deverá ser combinada entre as partes com antecedência mínima de 2 dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção da CONTRATANTE;

4.12. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho;

4.13. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

4.14. A CONTRATADA deverá monitorar e administrar os equipamentos ininterruptamente, 24 horas por dia, 7 dias da semana, 365 dias por ano, respondendo a eventos de forma proativa permitindo a verificação da conformidade com o estabelecido no Níveis Mínimos de Serviço Exigidos (NMSE), bem como o planejamento de capacidade e a análise da efetividade da solução;

4.15. Dentre as **atividades** que A CONTRATADA deverá realizar nas rotinas de monitoramento, resposta a incidentes de segurança e de administração das soluções de SIEM/SOAR (ITEM 01) estão incluídas, mas não limitadas a:

4.15.1. Manutenção preventiva e corretiva do SIEM, incluindo:

4.15.1.1. Desenvolvimento e manutenção de políticas e processos de manutenção de logs para as fontes, bem como procedimentos e processos de revisão.

4.15.1.2. Manutenção da arquitetura de gerenciamento de logs de acordo com o ambiente implantado, desenvolvendo filtros, formas de agregação, retenção e configuração das fontes.

4.15.1.3. Definição, planejamento, implementação e manutenção do recebimento de logs originados nas fontes monitoradas.

4.15.1.4. Alteração e revisão de regras e políticas de segurança;

4.15.1.5. Alteração de configurações;

4.15.1.6. Verificação de problemas de desempenho e/ou disponibilidade;

4.15.1.7. Verificação e filtragem de logs;

4.15.2. Monitoramento de eventos de segurança enviados para o SIEM e dos eventos relacionados aos casos de uso de seguranças elaborados no Processo contínuo de Desenvolvimento e Manutenção de Casos de Uso de Segurança;

4.15.3. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro do MPDFT (*Threat hunting)*;

4.15.4. Criar e revisar periodicamente regras (casos de uso) para detecção de ataques na solução adquirida (ITEM 01), realizando as adaptações e evoluções necessárias, conforme descrito no **Processo contínuo de Desenvolvimento e Manutenção de Casos de Uso de Segurança.**

4.15.5. Implementação de casos de uso SIEM pró ativamente e quando solicitado.

4.15.5.1. A implementação de casos de uso inclui configurações necessárias para consolidação e correlação de informações, coleta de eventos nos ativos envolvidos e interação com os responsáveis das respectivas soluções para envio de logs;

4.15.6. Implementar procedimentos para triagem de alertas e resposta a incidentes, conforme descrito no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação.**

4.15.7. Responder e analisar aos incidentes de segurança identificados pela solução adquirida e pelas atividades preventivas de *Threat hunting*, conforme descrito no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação.**

4.15.8. Produzir Relatório de Incidente de Segurança;

4.15.9. Produzir Boletins e indicadores de SI;

4.15.10. Atualização, quando pertinente, do SIEM.

4.15.11. Criação de conectores ou *parsing* para recebimento de logs por elementos que não tenham conectores na solução implantada, incluindo no mínimo os conectores e *parsing* para as tecnologias listadas no edital.

4.15.12. Apresentação de **relatório mensal** com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados.

4.15.13. Manutenção preventiva e corretiva do SOAR.

4.15.14. Solicitação de Implementação de rotina de automação (SOAR);

4.15.15. Atualização, quando pertinente, do SOAR.

4.15.16. Apresentação de **relatório mensal** com análise de tendências de incidentes de segurança da informação.

4.15.17. Prestar esclarecimento de dúvidas;

4.16. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (indisponibilidade) da solução de forma interativa ("*online*"), a partir do início do Período de Funcionamento Experimental (PFE), dando acesso ao sistema de monitoramento da CONTRATADA ou implementando o monitoramento na infraestrutura da CONTRATANTE;

4.17. A CONTRATANTE também realizará o monitoramento dos serviços/elementos que compõem a solução;

4.18. Todos os equipamentos responsáveis pela execução dos serviços contratados deverão ser acessíveis a partir de plataformas de gerenciamento e monitoramento SNMP localizadas na rede interna do CONTRATANTE.

4.19. As ferramentas de monitoramento utilizadas pela CONTRATANTE são *CACTI* e *Nagios (Thruk)*;

4.20. A CONTRATADA deve fornecer os *templates* de monitoramento dos equipamentos que compõem a solução ou as informações de OID's (identificadores de objetos) das MIB's (Base de Informação de Gerenciamento) que devem ser monitoradas via SMNP.

4.21. O monitoramento será utilizado para gerar relatórios mensais de disponibilidade e desempenho da solução e aplicações de penalidades.

4.22. O monitoramento deverá ser realizado através de sensores, que coletarão as informações e enviarão de forma segura ao Centro de Monitoramento e Resposta a Incidentes (CMRI) da CONTRATADA;

4.22.1. Os sensores poderão ser software interno ou funcionalidade da própria solução adquirida; ou softwares externos instalados fora da solução;

4.23. Os sensores deverão coletar minimamente, mas não limitado a:

4.23.1. Informações relevantes sobre o desempenho dos elementos monitorados como, por exemplo, utilização de disco, utilização de memória, uso de CPU, CPU *Load*, tráfego na interface de rede, entre outros;

4.23.2. Informações relevantes sobre a disponibilidade dos elementos monitorados;

4.23.3. Informações relevantes sobre a segurança dos elementos monitorados;

4.24. Os sensores deverão identificar e reportar, em tempo real, eventos relevantes que necessitem da interação humana;

4.25. As informações monitoradas, detectadas ou coletadas deverão ser enviadas sempre de forma segura (comunicação criptografada) ao CMRI;

4.26. O CMRI deve guardar na solução de SOAR todos os dados que permitam visualizar informações relacionadas a notificação e tratamento de incidentes: Data e hora de registro do incidente, identificação do responsável pelo registro, código de identificação do incidente, descrição do incidente, severidade do incidente, data e hora da notificação do incidente e tratamento adotado para o incidente;

4.26.1. Um incidente de segurança é definido como qualquer evento adverso em sistemas computacionais, feito de forma intencional ou acidental, levando a violação de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade;

4.27. Em caso de perda de comunicação com o Centro de Monitoramento e Resposta a Incidentes, os sensores deverão realizar armazenamento local (cache) das informações coletadas até que a comunicação seja reestabelecida, momento no qual a sonda irá enviar todos os dados históricos ao CMRI, de forma que não ocorram perdas de dados (gaps);

4.28. O acesso ao CMRI deve ser restrito apenas a funcionários autorizados;

4.29. O CMRI deverá contar com funcionários capacitados para a realização das atividades de monitoramento de redes e análise e resposta a incidentes de segurança.

4.30. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados remotamente a todos os produtos fornecidos pela CONTRATADA, podendo ser realizados nas dependências da CONTRATANTE, desde que haja necessidade e prévia autorização pela CONTRATANTE ou a pedido desta.

4.31. A CONTRATADA deverá manter atualizados os equipamentos destinados à execução dos serviços, implementando as últimas versões estáveis, atualizações e correções de hardware e software recomendadas pelo fabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção, de forma programada em acordo com a equipe de infraestrutura de produção do MPDFT.

4.32. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do Contrato;

4.33. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço para abertura e acompanhamento de chamados que deverá estar acessível durante 24 horas por dia, 7 dias por semana, 365 dias por ano, sem ônus adicional para a CONTRATANTE, constituído de no mínimo:

4.33.1. Serviço de atendimento com discagem gratuita (0800) ou de custo local para telefone fixo (DDD 61);

4.33.2. E-mail;

4.33.3. Sítio Web com HTTPS como meio de comunicação de disponibilidade imediata, em língua portuguesa e/ou inglesa, que possibilite:

4.33.3.1. Gerar relatórios customizáveis de modo a permitir a seleção de períodos de abrangência com possibilidade de exportar para HTML ou PDF ou CSV.

4.33.3.2. Visualizar informações relacionadas aos chamados técnicos: data e hora de abertura da solicitação; Identificação do solicitante, código de identificação da solicitação, descrição da solicitação, andamento da solicitação (*worklog*), data e hora de fechamento da solicitação;

4.34. Serão abertos chamados de severidade Alta ou Média para a realização da assistência técnica corretiva;

4.35. Os chamados técnicos serão abertos a partir da queda, falha ou registro de indisponibilidade gerado pelo monitoramento da CONTRATADA; por alertas da solução de SIEM/SOAR; e/ou por meio de abertura de chamado a critério da equipe técnica da CONTRATANTE. Esses chamados serão classificados conforme as severidades e prazos especificados em Níveis Mínimos de Serviço Exigidos (NMSE);

4.36. Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá, imediatamente, abrir um chamado técnico, informar ao CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos no NMSE**;**

4.37. A CONTRATADA encaminhará mensagem de e-mail para os contatos definidos pela CONTRATANTE informando, no mínimo, o número do chamado, a severidade, a data e hora da solicitação, nome do SOLICITANTE, descrição detalhada da solicitação, independentemente da forma de sua abertura, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado pela da equipe técnica da CONTRATANTE;

4.38. A CONTRATADA terá de apresentar relatórios técnicos mensalmente contendo informações de desempenho, para que seja identificada com antecedência a necessidade de adição/substituição de hardware/software;

4.39. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 5 (cinco) minutos, a CONTRATADA deverá entregar ao MPDFT, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, contendo suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível;

4.40. A CONTRATADA deverá manter registro dos eventos, que porventura tenham

provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar à CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências da CONTRATANTE, por ações ou solicitações da CONTRATANTE ou ainda por manutenções programadas;

4.41. A CONTRATADA somente poderá efetuar manutenção técnica que tenha previsão de indisponibilidade na solução e seus componentes após aprovação por parte da CONTRATANTE.

4.42. É vedado à CONTRATADA interromper o atendimento de um chamado até que, RECOLOCANDO EM PLENO ESTADO DE FUNCIONAMENTO, se chegue à solução definitiva. A CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento do chamado;

4.43. A CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 10 usuários que terão *login* e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério da CONTRATANTE e configurados pela CONTRATADA. Essa lista pode mudar durante o período de vigência do contrato;

4.44. Caberá à CONTRATADA gerenciar permanentemente durante toda a vigência do contrato, de forma proativa, toda a solução adquirida, garantindo os níveis de serviço acordados;

4.45. Caso seja necessária a instalação de equipamentos de administração da solução nas instalações do CONTRATANTE, a CONTRATADA deverá fornecer todos os recursos necessários para tanto. O CONTRATANTE ficará responsável apenas pelo fornecimento de alimentação elétrica e portas lógicas para as conexões;

4.46. O acesso aos equipamentos e soluções eventualmente hospedados no MPDFT dar-se-á por meio de VPNs via Internet, a serem implementadas pela CONTRATADA. De forma a possibilitar a administração remota, a CONTRATADA poderá optar por proceder a instalação e a manutenção de canal de comunicação direto com os equipamentos sob sua responsabilidade, devendo se responsabilizar e garantir total segurança para este acesso. Atuações locais, que necessitem de acesso físico direto ao ambiente e ao equipamento, deverão ser previamente comunicados e acordados com a equipe do MPDFT;

4.47. O CONTRATANTE possui link de internet que poderá ser utilizado para o estabelecimento das VPNs mencionadas no item anterior;

4.48. A CONTRATADA deverá, por meio da administração remota, ser capaz de implementar políticas, regras, filtros ou quaisquer outros recursos e implementações lógicas, necessárias a manutenção do serviço em conformidade com o especificado. As solicitações de alterações e inclusões de novas políticas, regras e filtros efetuados pelo CONTRATANTE não serão limitadas e deverão

ser implementadas, de acordo com o NMSE;

4.49. A CONTRATADA deverá criar contas de acesso privilegiado à administração dos serviços para a equipe técnica do CONTRATANTE, que permitam a execução de funções de administração da solução, em especial alterações e inclusões de novas políticas, regras e filtros. Todos os acessos à administração dos serviços, inclusive aqueles efetuados pela CONTRATADA, deverão ser autenticados, criptografados e registrados para posterior auditoria;

4.50. Caberá à CONTRATADA o registro, monitoração, triagem e classificação prévia de severidade de todos os alertas de incidentes emitidos pelos serviços administrados, em especial os relacionados a tentativas de ataques em direção à rede do CONTRATANTE ou por ela originados; adotar, de imediato, as medidas de tratamento que forem acordadas com o CONTRATANTE, cabendo a este a classificação final da severidade. Tais medidas estarão relacionadas com o grau de severidade constante no alerta do ataque indicado pela solução adquirida;

4.51. A instalação, remoção ou desligamento das funcionalidades dos equipamentos deverá, sempre que possível, ser realizada sem que outros componentes da rede local do CONTRATANTE necessitem de configuração adicional;

4.52. A CONTRATADA deverá desempenhar suas atividades por intermédio de **pelo menos dois técnicos** devidamente identificados, especializados e qualificados da seguinte forma: formação específica e oficial do fabricante para as atividades de instalação, configuração e suporte, envolvendo os equipamentos e programas da solução, a ser comprovada com certificado e/ou declaração de curso(s) técnico(s), emitidos pelo fabricante dos mesmos ou empresa credenciada e qualificada para esta finalidade;

4.53. A CONTRATADA deverá enviar à CONTRATANTE a relação dos técnicos que devem ser autorizados a entrar nas dependências da CONTRATADA, juntamente com os documentos necessários para cadastro na segurança institucional do órgão. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE;

4.54. Caso a Equipe de Atendimento Técnico da CONTRATADA sofra alguma alteração em sua composição durante a vigência deste contrato, tal fato deve ser imediatamente informado ao gestor do contrato e à equipe técnica do MPDFT, incluindo as respectivas comprovações acerca dos requisitos de qualificação exigidos para esses profissionais e as informações necessárias para liberação do acesso dos técnicos às dependências do MPDFT, conforme itens anteriores;

4.55. Caso seja constatada a falta de conhecimento mínimo necessário para operação da solução por parte do prestador de serviço, a equipe técnica do MPDFT poderá solicitar sua substituição por técnico devidamente qualificado.

5. REQUISITOS DA CONTRATAÇÃO (ITENS 1, 2, 3 E 4)

5.1. **REQUISITOS DO PROCESSO DE DESENVOLVIMENTO E MANUTENÇÃO DE CASOS DE USO DE SEGURANÇA:**

5.1.1. O **Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança** deve ser executado na implantação da solução (**ITEM 2**), de forma periódica e sob demanda conforme solicitações do tipo **Severidade BAIXA**, previstas no serviço (**ITEM 4**). O processo deverá contemplar no mínimo as seguintes **etapas**:

5.1.1.1. **Identificar candidatos a casos de uso**, contemplando as seguintes atividades:

5.1.1.1.1. Levantar fontes necessárias.

5.1.1.1.2. Levantar requisitos para o caso de uso.

5.1.1.1.3. Documentar caso de uso.

5.1.1.2. **Priorizar casos de uso**, contemplando as seguintes atividades:

5.1.1.2.1. Determinar importância de cada caso de uso identificado.

5.1.1.2.2. Determinar viabilidade de implementação de cada caso de uso.

5.1.1.2.3. Construir lista de casos de uso priorizados.

5.1.1.2.4. Construir lista de casos de uso com implementação inviável.

5.1.1.3. **Implementar casos de uso**, contemplando as seguintes atividades:

5.1.1.3.1. Revisar e refinar descrição e requisitos dos casos de uso a serem implementados.

5.1.1.3.2. Determinar requisitos de fontes de dados necessários para implementar cada caso de uso.

5.1.1.3.3. Determinar requisitos de contexto de dados.

5.1.1.3.4. Desenvolver, testar e colocar em produção o caso de uso.

5.1.1.4. Revisar casos de uso periodicamente, em especial quando:

5.1.1.4.1. Após mudanças no ambiente que afetem determinado caso de uso.

5.1.1.4.2. Após atingir limites preestabelecidos.

5.1.2. Os casos de uso implementados e outros *dashboards* do SIEM e do SOAR deverão ser a base para a prestação do serviço de resposta a incidentes **ITEM 04.**

5.1.3. Os casos de uso de seguranças poder ser classificados em **casos de uso de monitoramento** e **casos de uso de auditoria**.

5.1.4. Para o aceite do **Serviço de instalação e implantação da solução (ITEM 02)**, a CONTRATADA deverá implementar em conjunto com o CONTRATANTE no mínimo 5 (cinco) dos seguintes casos de uso de monitoramento de segurança, seguindo o **Processo de Desenvolvimento e**

Manutenção de Casos de Uso de Segurança:

5.1.4.1. **Caso de uso 01 - Rastreamento de autenticação e detecção de comprometimento de contas:** Detectar comprometimento de contas via rastreamento de autenticações; autenticação simultânea de usuários de múltiplos locais ou em horários impossíveis ou poucos usuais.

5.1.4.2. Caso de uso 02 - Monitoração de conexões de saída suspeitas: Monitoração de atividade suspeita (volume, frequência, destinos, portas e etc) relacionada a conexões de saída e transferências de dados utilizando logs de firewall, logs de web proxy e informações coletadas pelo monitoramento de tráfego de rede; detectar exfiltração de dados e outras conexões externas suspeitas.

5.1.4.3. **Caso de uso 03 - Detectar tráfego de rede de sistemas comprometidos e infectados:** Rastrear sistemas comprometidos e infectados, incluindo detecção de malware, utilizando logs de conexões de firewalls, alertas de intrusion prevention system (IPS), logs de web proxy, logs de EDR e informações coletadas pelo monitoramento de tráfego de rede.

5.1.4.4. **Caso de uso 04 - Rastrear mudanças em sistemas e outras atividades administrativas:** Rastrear mudanças em sistemas e outras atividades administrativas em diversos sistemas internos e comparar com as políticas definidas; detectar violações de políticas internas.

5.1.4.5. **Caso de uso 05 - Rastrear ataques a aplicações web:** Rastrear ataques a aplicações web e suas consequências utilizando logs de servidores web, web application firewall (WAF) e servidores de aplicações; detectar tentativas de comprometimento e abuso de aplicações web ao combinar logs de diferentes componentes.

5.1.4.6. Caso de uso 06 - Detectar abuso de acessos privilegiados: Identificar acessos excessivos feitos por usuários privilegiados.

5.1.4.7. **Caso de uso 07 - Detectar uso anormal de internet por usuários:** Identificar anomalias em comportamento de usuários ao acessar a internet (como, por exemplo, volume de dados, frequência de acesso, número de destinos, acesso a serviços e portas fora do comum).

5.1.4.8. **Caso de uso 08 - Utilizar inteligência de ameaças (*threat intelligence*) nos logs para detectar ameaças:** Gerar alertas para acessos bem-sucedidos para/ou de IPs externos identificados como maliciosos por fontes de inteligência de ameaças (*threat intelligence feeds*).

5.1.4.9. **Caso de uso 09 - Identificar movimento lateral na rede interna:** Identificar tráfego anormal entre estações/servidores ou acesso anormal

a recursos internos por dispositivos internos.

5.1.4.10. **Caso de uso 10 - Detectar tentativas bem-sucedidas de *phishing*:** Identificar tentativas bem-sucedidas de *phishing* através de correlação de logs de gateway de e-mail e web proxy.

5.1.4.11. Caso de uso 11: Validar alertas de sistemas de detecção/prevenção de intrusão (IDS/IPS): Validar alertas de IDS/IPS usando dados de vulnerabilidades além de dados de outros contextos sobre ativos.

5.1.4.12. Caso de uso 12: Priorizar correção de vulnerabilidades: Validar detecções de vulnerabilidades feita por scan usando dados outros contextos sobre ativos, como por exemplo informações coletadas pelo monitoramento de tráfego de rede, logs de acesso web e alertas de IDS/IPS, EDR e antimalware.

5.1.5. Os casos de uso previstos no item anterior, além de outros não previstos, que não forem implementados durante a implantação deverão ter cronograma de implementação acordado periodicamente, conforme **Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança** distrito nesse edital.

5.1.6. Cada caso de uso implantado deverá ter documentação detalhada entregue a contratada.

5.1.7. Para auxiliar no tratamento dos incidentes identificados com a implantação dos casos de uso de monitoramento de seguranças, deverão ser desenvolvidos *playbooks* na ferramenta de SOAR.

5.1.8. Para o aceite do **Serviço de instalação e implantação da solução (ITEM 02),** a CONTRATADA deverá implementar em conjunto com o CONTRATANTE no mínimo 5 (cinco) dos seguintes casos de uso de auditoria, seguindo o **Processo de Desenvolvimento e Manutenção de Casos de Uso de Segurança**:

5.1.8.1. Caso de uso de auditoria 01: Auditoria de eventos do **Windows AD**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.1.1. Logs brutos e formatados;

5.1.8.1.2. Tabela e/ou planilha com os registros processados com as seguintes informações de autenticação: Data e hora do evento; IP do cliente que solicitou a autenticação**;** Usuário (login)**;** Nome do serviço que fez a autenticação**;** Id do evento Windows;

5.1.8.1.3. Tabela e/ou planilha com os registros processados com as seguintes informações de acesso a serviços: Data e hora do evento**;** IP do cliente

que solicitou o serviço**;** Usuário (login)**;** Nome do serviço acessado**;** Id do evento Windows;

5.1.8.1.4. Tabela e/ou planilha datas e hora de primeiro acesso nos dias em que pelo menos um acesso autenticado ocorreu;

5.1.8.1.5. Relatório das estações de trabalho e serviços que o usuário foi autenticado;

5.1.8.1.6. Histograma de: IPs utilizados pelo login do usuário; Datas dos eventos; Usuários; Serviços acessados;

5.1.8.2. Caso de uso de auditoria 02: Auditoria de acesso a **aplicações web**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.2.1. Logs brutos e formatados;

5.1.8.2.2. Tabela e/ou planilha com os registros processados com as seguintes informações de acesso: Data e hora do evento**;** IP do cliente**;** Usuário (login)**;** Nome do serviço/aplicação acessada;

5.1.8.2.3. Tabela e/ou planilha com datas e hora de primeiro acesso dos acessos internos e externos nos serviços web

5.1.8.3. Caso de uso de auditoria 03: Auditoria de acesso a **servidores de arquivos (NAS)**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) e/ou a um caminho de arquivo (nome do arquivo ou pasta) em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.3.1. Logs brutos e formatados;

5.1.8.3.2. Tabela e/ou planilha com os registros processados com as seguintes informações de acesso a arquivos: Data e hora do evento; Usuário (login); IP de origem do acesso; Local onde o arquivo foi acessado (servidor de arquivos); Ação no arquivo (escrita, leitura, deleção); Nome do arquivo; Id do evento Windows;

5.1.8.4. Caso de uso de auditoria 04: Auditoria de **uso de e-mail**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) e/ou a uma caixa de e-mail em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.4.1. Logs brutos e formatados;

5.1.8.4.2. Tabela e/ou planilha com os registros processados com as seguintes informações: Data e hora do evento; Remetente; Destinatário; Assunto do e-mail; IP de origem; Status da entrega do e-mail;

5.1.8.5. Caso de uso de auditoria 05: Auditoria de uso de **VPN**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.5.1. Logs brutos e formatados;

5.1.8.5.2. Tabela e/ou planilha com os registros processados com as seguintes informações: Data e hora do evento; Usuário; IP de origem; IP interno atribuído na sessão de vpn;

5.1.8.6. Caso de uso de auditoria 06: Auditoria de acesso feita por um usuário em **qualquer tipo de ativo ou serviço**. Coletar todos os eventos de auditoria relacionados a um usuário (login ou ip) em um determinado período e gerar as seguintes visualizações e relatórios:

5.1.8.6.1. Relatório das estações de trabalho e serviços que o usuário foi autenticado;

5.1.8.6.2. Histograma de: IPs utilizados pelo login do usuário; Datas dos eventos; Usuários; Serviços acessados;

5.1.8.6.3. Tabela e/ou planilha com datas e hora de primeiro acesso nos dias em que pelo menos um acesso autenticado ocorreu;

5.1.8.6.4. Tabela e/ou planilha com datas e hora de primeiro acesso dos acessos internos em máquinas e serviços web;

5.1.8.6.5. Tabela e/ou planilha com datas e hora de primeiro acesso dos acessos externos nos serviços web;

5.2. REQUISITOS DO PROCESSO DE IDENTIFICAÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

5.2.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao MPDFT através de correlação de logs e/ou comportamento anômalos de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em processo de gestão de incidentes.

5.2.2. O **Processo de Identificação e Resposta a Incidentes de Segurança da Informação** deverá ser executado em conjunto pela CONTRATADA e pela CONTRATANTE, tendo responsabilidades bem definidas.

5.2.3. O **Processo de Identificação e Resposta a Incidentes de Segurança da Informação** deverá ser executado de forma contínua tomando como base no mínimo as seguintes fontes de incidentes:

5.2.3.1. Incidentes reportados pela equipe de respostas a incidentes do MPDFT;

5.2.3.2. Incidentes detectados através de monitoração contínua da Solução de gestão de eventos de segurança da informação (SIEM) e gestão da resposta a incidentes de segurança da informação (SOAR**) – ITEM 01**.

5.2.3.3. Incidentes detectados através de atividades de *Threat hunting* previstas no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação**.

5.2.4. O **Processo de Identificação e Resposta a Incidentes de Segurança da Informação** deve ser executado de forma contínua e também sob demanda, por meio de abertura de chamados de solicitações de resposta a incidente, previstas no serviço de resposta a incidentes **(ITEM 4)**. O processo deverá contemplar no mínimo as seguintes **etapas**:

5.2.4.1. **Preparação**, contemplando as seguintes atividades:

5.2.4.1.1. **Elaboração de Plano de resposta a incidentes**: O Plano de respostas a incidentes (PRI) deverá ser elaborado durante a implantação do serviço em conjunto entre a CONTRATADA e a CONTRATANTE e deve ser revisado periodicamente, no mínimo a cada ano.

5.2.4.1.2. A entrega do PRI é condição necessária para o recebimento provisório do serviço.

5.2.4.1.3. Requisitos do Plano de resposta a incidentes – Deve incluir no mínimo:

5.2.4.1.3.1. Definições do que é um incidente de segurança no contexto do MPDFT e os critérios para determinar a criticidade de cada incidente.

5.2.4.1.3.2. Árvores de escalação (*Escalation tree*).

5.2.4.1.3.3. Plano de comunicação.

5.2.4.1.3.4. Classes de incidentes e cenários.

5.2.4.1.3.5. Procedimentos, *checklists* e *workflows* por tipo de incidente.

5.2.4.1.3.6. Planejamento de exercícios de simulação.

5.2.4.1.3.7. Mapeamento do processo como um todo em notação padronizada (Business Process Model and Notation (BPMN)).

5.2.4.2. Identificação:

5.2.4.2.1. A etapa de identificação é de inteira responsabilidade da CONTRATADA.

5.2.4.2.2. A etapa de identificação deverá seguir o processo e os critérios definidos no PRI.

5.2.4.2.3. Deverá contemplar no mínimo as seguintes atividades de identificação:

5.2.4.2.3.1. Monitoramento constante da Solução de gestão de eventos de segurança da informação (SIEM) seja através dos **Casos de Uso de Segurança** já definidos ou **através dos logs diretamente**.

5.2.4.2.3.2. Identificação proativa de incidentes através de atividades de *Threat hunting*.

5.2.4.2.3.2.1. A CONTRATADA deverá fazer uso do framework MITRE ATT&CK para essa atividade.

5.2.4.2.3.3. Registro dos incidentes ou casos identificados no SOAR para documentação e acompanhamento dos incidentes, incluindo os tempos de atendimento para averiguação da conformidade com previstos nos **Níveis Mínimos de Serviços Exigidos (NMSE)** do Serviço de resposta a incidentes **(ITEM 4)**

5.2.4.2.3.3.1. A CONTRATANTE deverá ser notificada através do SOAR sempre que um incidente for registrado, em especial nos casos de incidentes graves a CONTRATADA deverá comunicar a CONTRATANTE através de canal que reflita a gravidade do incidente, como e-mail ou outro meio acordado. Toda a comunicação deverá seguir o plano de comunicação contido no PRI.

5.2.4.2.3.3.2. Todas as ações tomadas pela CONTRATADA deverão ser registradas no SOAR.

5.2.4.2.4. Uma vez identificado o incidente a CONTRATADA deverá:

5.2.4.2.4.1. Aprofundar análise do incidente para se assegurar que o incidente não é um falso-positivo ou para relacionar o incidente a um grupo de incidentes, gerando um caso.

5.2.4.2.4.2. Requisitar acesso a logs de servidores ou informações do MPDFT que não estejam disponíveis no SIEM para análise mais aprofundada.

5.2.4.2.4.2.1. A CONTRATANTE avaliará cada pedido e mesmo que não seja concedido acesso a CONTRATADA deverá continuar o processo de tratamento com as informações que possui.

5.2.4.3. Contenção:

5.2.4.3.1. Uma vez identificado e investigado o incidente a CONTRATADA deverá propor medidas de contenção para a CONTRATANTE. As medidas de contenção deverão ser de curto prazo para tratar o incidente o mais rapidamente possível, podendo ser soluções de contorno ou temporárias.

5.2.4.3.2. As medidas propostas deverão levar em conta todos os equipamentos de segurança usados no MPDFT para que sejam aplicadas na camada correta de proteção.

5.2.4.3.2.1. As medidas propostas deverão conter script para alteração ou adequação de ambiente caso seja possível, como, por exemplo, script para criação de regra de firewall, WAF ou IPS.

5.2.4.3.3. A CONTRATADA não será responsável por executar a medida de contenção sugerida.

5.2.4.3.3.1. O MPDFT pode autorizar em casos excepcionais ou de acordo com o PRI a execução direta de medidas de contenção pela CONTRATADA ou pela ferramenta SOAR de forma automatizada.

5.2.4.3.4. Uma vez que sejam entregues as medidas de contenção propostas o incidente será considerado resolvido, conforme os tempos previstos nos **NMSE (ITEM 4)** para as atividades de resposta a incidentes.

5.2.4.4. Erradicação:

5.2.4.4.1. De acordo com a criticidade, risco e tipos de incidentes ou outros critérios previstos no PRI a contratada deverá elaborar relatório em que investiga mais a fundo o incidente e propõe medida para erradicar determinado incidente ou conjunto de incidentes.

5.2.4.4.2. Essa solicitação sempre que autorizada ou requisitada deverá ser registrada com chamado de severidade baixa – Solicitação Relatório de Incidente de Segurança;

5.2.4.4.3. Se necessário deverá ser feita análise de causa raiz do problema para identificar e tratar a origem do incidente ou grupo de incidentes.

5.2.4.5. Recuperação:

5.2.4.5.1. A CONTRATADA deverá acompanhar a contenção e/ou erradicação executada pelo MPDFT para garantir que o incidente tenha sido contido ou erradicado apropriadamente e não continue em atividade no ambiente do MPDFT.

5.2.4.5.2. A CONTRATADA deverá recomendar procedimentos de teste para verificar a efetividade das ações de contenção e/ou erradicação propostas.

5.2.4.6. Lições aprendidas:

5.2.4.6.1. Todos os incidentes detectados deverão ser registrados no sistema SOAR para análise, acompanhamento, mensuração de tempo de atendimento, análise de tendências e registro de lições aprendidas.

5.2.4.6.2. O sistema SOAR deverá ser usado como base de conhecimento dos incidentes.

5.2.4.6.3. De acordo com os critérios definidos no PRI ou sempre que solicitado deverá ser elaborado relatório *post mortem* em que se deve tentar responder as seguintes perguntas:

5.2.4.6.3.1. Quem, o quê, onde, como, quando e por quê.

5.2.4.6.3.2. Quando o problema foi detectado e por quem.

5.2.4.6.3.3. O escopo do incidente.

5.2.4.6.3.4. Como o incidente foi contido e erradicado.

5.2.4.6.3.5. Trabalho feito para recuperação e erradicação.

5.2.4.6.3.6. Áreas em que o processo de tratamento foi efetivo.

5.2.4.6.3.7. Áreas em que o processo de tratamento precisa de melhorias.

5.2.4.6.4. A CONTRATANTE poderá solicitar reunião para apresentação do relatório *post mortem*.

5.2.4.6.4.1. Cada relatório *post mortem* deverá ser registrado e acompanhado como um chamado de severidade baixa – Solicitação Relatório de Incidente de Segurança.

5.3. TRANSFERÊNCIA DE CONHECIMENTO SOBRE O AMBIENTE DO MPDFT E DOCUMENTAÇÃO TÉCNICA:

5.3.1. Para o compartilhamento de informações deverá ser assinado Termo de Confidencialidade e Sigilo.

5.3.2. A CONTRATANTE deverá passar o máximo de informações necessárias para a CONTRATADA prestar o serviço, de tal forma que a CONTRATADA terá condições de entender o ambiente do MPDFT para a adequada instalação e implantação da solução e para o adequado tratamento de incidentes de segurança da informação.

5.3.3. A CONTRATADA deverá elaborar documentação sobre o ambiente do MPDFT para que qualquer funcionário que seja encarregado de trabalhar na prestação ou fiscalização do serviço seja treinado com base nessa documentação. Deve conter as seguintes informações:

5.3.3.1. Descrição dos serviços implantados;

5.3.3.2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

5.3.3.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

5.3.3.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

5.3.3.5. Definição de responsabilidades;

5.3.3.6. Recursos de alta disponibilidade;

5.3.3.7. Scripts de operação;

5.3.3.8. Procedimentos para abertura e atendimento a chamados;

5.3.3.9. Procedimentos de recuperação da solução;

5.3.3.10. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

5.3.3.11. Rotinas periódicas configuradas;

5.3.3.12. Documentação dos processos de trabalho associados a solução e ao serviço, em esquema de fluxograma, com definição de responsáveis por atividade, prazos de execução, rotinas de atualização e revisão periódica de regras;

5.3.3.13. Casos de uso implantados na solução de correlação de eventos;

5.3.3.14. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);

5.3.4. Deverá ser entregue pela CONTRATADA a "Documentação Técnica" (DT) de toda a solução implementada no ambiente da CONTRATANTE, composta de:

5.3.4.1. Plano de Implantação, contendo as configurações específicas dos equipamentos, arquiteturas e suas topologias e diagramas lógicos da solução;

5.3.4.2. Plano de Testes;

5.3.4.3. Plano de Transferência de Conhecimento;

5.3.4.4. Documentação do ambiente do MPDFT, base para treinamento de novos funcionários;

5.3.4.5. Plano de respostas a incidentes (PRI) previsto nos requisitos do Processo de Identificação e Resposta a Incidentes de Segurança da Informação;

5.3.4.6. Modelo de relatório mensal, que será utilizado no **ITEM 4** com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados.

5.3.4.7. Modelo de relatório mensal, que será utilizado no **ITEM 4** com análise de tendências de incidentes de segurança da informação.

5.3.4.8. Manual de abertura e relatório de chamados.

5.3.5. Essa documentação fica sujeita à análise e à aprovação da equipe técnica da CONTRATANTE;

5.3.6. Toda a DT deverá ser entregue em mídia digital, devendo as topologias da solução serem entregues em formato a ser definido pela CONTRATANTE;

5.3.7. Essa documentação fica sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

5.3.8. Toda a DT fornecida pela CONTRATADA referente às ferramentas e

solução implantadas no ambiente da CONTRATANTE é de propriedade da CONTRATANTE.

5.3.9. Toda a DT fornecida pela CONTRATADA deverá estar em português do Brasil.

5.4. **REUNIÃO DE ALINHAMENTO DE EXPECTATIVAS:**

5.4.1. Deverá ser realizada uma reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da infraestrutura de TI da CONTRATANTE;

5.4.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato, o Fiscal Técnico do Contrato, o Preposto e membro da equipe técnica da CONTRATADA;

5.4.3. A reunião realizar-se-á na sede da CONTRATANTE **ou na modalidade remota por vídeo conferência** em prazo especificado neste documento;

5.4.4. Na reunião de Alinhamento de Expectativas a CONTRATADA deverá apresentar:

5.4.4.1. Sugestão de arquitetura e conjunto de casos de uso a serem configurados na implantação da solução contratada;

5.4.4.2. As sugestões deverão ser apresentadas para discussão durante a reunião e as configurações definitivas devem ser apresentadas no Plano de Implantação.

5.4.5. Durante a implantação, o conjunto de casos de uso de que trata o item anterior poderão ser alterados conforme a necessidade da CONTRATANTE.

5.5. **CREDENCIAMENTO DOS COLABORADORES**

5.5.1. Todos os profissionais que prestarem serviços relativos à solução devem ser credenciados junto ao MPDFT para que sejam autorizados a prestar serviços nas dependências do órgão.

5.5.2. A CONTRATADA deverá observar, rigorosamente, todas as normas, padrões e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do MPDFT.

5.5.3. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE.

5.5.4. Caberá à CONTRATADA comunicar ao MPDFT qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e

recursos do MPDFT, porventura colocados à disposição para realização dos serviços contratados.

5.5.5. Deve ser mantido sigilo sobre todos os ativos de informações e de processos do MPDFT e da CONTRATADA que se refiram ao MPDFT.

5.5.6. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do MPDFT, sob pena de aplicação das sanções cabíveis.

5.5.7. A CONTRATADA deverá manter em caráter confidencial, as informações relativas à política de segurança adotada pelo MPDFT e as configurações de hardware e de Softwares decorrentes.

5.5.8. A CONTRATADA deverá manter em caráter confidencial, as informações relativas ao processo de instalação, configuração e adaptações de produtos e ferramentas.

5.5.9. A CONTRATADA deverá submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pelo MPDFT, durante o tempo de permanência nas dependências do órgão.

5.6. **IMPLANTAÇÃO, HOMOLOGAÇÃO E FUNCIONAMENTO EXPERIMENTAL:**

5.6.1. A CONTRATADA deverá apresentar um Plano de Implantação que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

5.6.2. O Plano de Implantação deverá conter a descrição de, no mínimo:

5.6.2.1. Atividades a serem desenvolvidas, incluindo testes, e seus respectivos cronogramas;

5.6.2.2. Políticas de configuração dos elementos da solução;

5.6.2.3. Topologia lógica para a solução;

5.6.2.4. Ações de *rollback*.

5.6.3. Todo o trabalho a ser realizado deve seguir o especificado no Plano de Implantação;

5.6.4. Para cada nova *release*, *build*ou funcionalidade, poderá ser solicitada uma nova implantação de qualquer funcionalidade presente na solução;

5.6.5. A CONTRATADA deverá realizar toda a instalação dos produtos, incluindo a configuração das ferramentas e os testes da solução, sob supervisão da CONTRATANTE;

5.6.6. Todas as atividades envolvidas na Implantação deverão ser acompanhadas pela equipe técnica da CONTRATANTE;

5.6.7. Todos os técnicos envolvidos na instalação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade de acordo com este termo de referência;

5.6.8. A CONTRATADA será responsável por dimensionar a solução a ser adotada na rede da CONTRATANTE atendendo minimamente os requisitos solicitados neste termo de referência. Esta solução estará sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

5.6.9. A solução apresentada não pode causar impacto no funcionamento da rede (por exemplo, lentidão na rede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente ao usuário;

5.6.10. Caso o dimensionamento feito pela CONTRATADA não apresentar desempenho satisfatório, baseado nas recomendações do fabricante, a solução deverá ser redimensionada sem ônus adicional para a CONTRATANTE, mesmo que o redimensionamento envolva adição/substituição de hardware e software;

5.6.11. Junto com o Plano de Implantação, a CONTRATADA deverá apresentar um Plano de Testes à equipe técnica da CONTRATANTE para avaliação;

5.6.12. O Plano de Testes consiste num documento onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos, descritas neste Termo;

5.6.13. O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar o acompanhamento por parte da CONTRATANTE;

5.6.14. Na tabela mencionada no item anterior, deve-se incluir os resultados esperados para cada teste realizado, conforme **Modelo de Plano de Testes** em anexo**;**

5.6.15. Os procedimentos descritos no Plano de Testes serão realizados pela CONTRATADA após a instalação e configuração dos produtos. Esses testes serão acompanhados pela equipe técnica da CONTRATANTE;

5.6.16. Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização dessas correções, os testes serão reiniciados;

5.6.17. Se todos os testes forem realizados com sucesso, **os produtos serão considerados implantados**;

5.6.18. A CONTRATADA deverá fornecer todos os materiais necessários à

instalação física, à configuração e ao perfeito funcionamento dos equipamentos, cabos elétricos e cabos lógicos, quando for o caso. Caberá à CONTRATANTE o provimento de alimentação elétrica e das portas lógicas para conexão à rede local;

5.6.19. Para a homologação da solução, será estabelecido pela CONTRATANTE um PFE - Período de Funcionamento Experimental, com duração definida conforme este Termo de Referência, para testar o perfeito funcionamento dos produtos, verificar suas funcionalidades, analisando sua aderência às especificações deste Edital e seus Anexos, bem como à Proposta da CONTRATADA, e a sua compatibilidade com a estrutura já existente na CONTRATANTE;

5.6.20. O PFE somente poderá ser iniciado após a conclusão da implantação e deve respeitar o prazo máximo definido neste Termo de Referência.

5.6.21. Pelo menos um técnico da CONTRATADA deverá estar dedicado a acompanhar o decorrer do PFE, podendo ser solicitada sua presença no MPDFT em caso de necessidade.

5.6.22. Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos;

5.6.22.1. Caso haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização destas correções, o PFE será reiniciado.

5.6.22.2. Caso não haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a solução será considerada homologada.

5.6.23. Os produtos funcionarão de acordo com as recomendações do fabricante, levando-se em consideração que todas as funcionalidades requeridas neste Termo de Referência estarão habilitadas simultaneamente;

5.6.24. A emissão do Termo de Homologação está vinculada à homologação, entrega da Documentação Técnica - DT e a realização da Transferência de Conhecimento, conforme mencionado neste Termo de Referência;

5.6.25. As etapas de implantação e PFE deverão ser contíguas, não havendo interstícios entre elas.

6. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS (NMSE)

6.1. **ITEM 1** - Níveis de severidade e prazos dos chamados da garantia e assistência técnica da Solução de gestão e correlação de eventos de segurança da informação (SIEM) e gestão da resposta a incidentes de segurança da informação (SOAR):

Grau de severidade	Definição	Tempo de resposta
ALTA	Esse nível de severidade é aplicado para: Serviços totalmente indisponíveis ou comprometimento do desempenho ou funcionalidade do produto.	Prazo de solução: **6 horas** após abertura do chamado
MÉDIA	Esse nível de severidade é aplicado para: Quando há um alerta no produto, mas ainda se encontra operacional e sem diminuição do desempenho.	Prazo de solução: **12 horas** após abertura do chamado
BAIXA	Esse nível de severidade é aplicado para: Solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/produto. Não haverá abertura de chamado com esta severidade em sábados, domingos e feriados.	Prazo de solução**: 5 dias úteis** após abertura do chamado

6.2. **ITEM 4** - Níveis de severidade e prazos dos chamados do Serviço de gestão, descoberta e resposta a incidentes de segurança da informação (SIEM/SOAR):

Grau de severidade	Definição	Tempo de resposta
ALTA	Esse nível de severidade é aplicado para: 1. Resolução de problemas, incluindo, mas não se limitando a sobrecarga da solução, quando há indisponibilidade na solução ou em qualquer serviço que a compõe. 2. Solicitações de resposta a incidentes (análise e contenção) **que resultaram em comprometimento da segurança** da rede do MPDFT. a. Serão abertas automaticamente por alertas da solução, por solicitação da CONTRATANTE e pelas atividades preventivas de *Threat hunting* conforme descrito no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação**; b. Nesses casos, a resolução consiste na sugestão de medidas de contenção de incidentes, não excluído a necessidade;	Prazo de solução: **4 horas** após abertura do chamado ou ocorrência/detecção de evento relacionado a essa severidade.
MÉDIA	Esse nível de severidade é aplicado para: 1. Solicitações de alteração de configurações;	Prazo de solução: **8 horas** após abertura do chamado ou ocorrência/detecção de evento relacionado a essa severidade.

	2. Solicitações de resposta a incidentes (análise e contenção) **que tenham potencial de comprometimento da segurança** da rede do MPDFT. a. Serão abertas automaticamente por alertas da solução, por solicitação da CONTRATANTE e pelas atividades preventivas de *Threat hunting* conforme descrito no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação**; b. Nesses casos, a resolução consiste na sugestão de medidas de contenção de incidentes, não excluído a necessidade; 3. Qualquer outra ação, de natureza ainda corretiva, que não se encaixe como resolução de problemas;	
BAIXA	Esse nível de severidade é aplicado para: 1. Solicitação de manutenções preventivas, esclarecimento de dúvidas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos; ou atualização dos produtos que compõem a solução. 2. Solicitações de resposta a incidentes (análise e contenção) **que não tenham potencial de comprometimento** da segurança da rede do MPDFT. a. Serão abertas automaticamente por alertas da solução, por solicitação da CONTRATANTE e pelas atividades preventivas de *Threat hunting* conforme descrito no **Processo de Identificação e Resposta a Incidentes de Segurança da Informação**; b. Nesses casos, a resolução consiste na sugestão de medidas de contenção de incidentes, não excluído a necessidade; 3. Solicitação de Relatório de Incidente de Segurança; 4. Solicitação de Verificação e filtragem de logs; 5. Solicitação de Implementação de casos de uso de segurança (SIEM); 6. Solicitação de Implementação de rotina de automação (SOAR); 7. Solicitação de Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro do MPDFT (*Threat hunting)*;	Prazo de solução: **72 horas** após abertura do chamado ou ocorrência/detecção de evento relacionado a essa severidade.

	Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Em casos excepcionais o prazo de 72 horas pode ser negociado com a CONTRANTE dependendo da complexidade da demanda solicitada.	

6.3. Fica também estabelecido que haverá glosa sobre o valor mensal da solução, por hora ou fração de hora em atraso no atendimento de chamados, conforme a seguinte fórmula:

$$\mathbf{G = ((H_a * F_c) + (H_m * F_c) + (H_b * F_c)) * 4, \text{ onde:}}$$

G = Percentual de glosa no mês;

H_a = Quantidade de horas em atraso de chamados de severidade ALTA;

H_m = Quantidade de horas em atraso de chamados de severidade MÉDIA;

H_b = Quantidade de horas em atraso de chamados de severidade BAIXA;

F_c = Fator de correção de severidade, sendo:

0,5 para severidade ALTA;

0,25 para severidade MÉDIA; e

0,125 para severidade BAIXA;

6.4. O percentual de glosa no mês, resultante da fórmula do item anterior, ficará limitado a 50% do valor mensal do contrato.

6.5. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação de glosas previstas, poderá ser aberto processo específico pela CONTRATANTE para apuração de possível aplicação de penalidade.

ANEXO II – Modelo de Comprovação Ponto a Ponto

Tabela – comprovação de atendimento ponto a ponto

Código do item da especificação técnica do Termo de referência	Especificação Técnica	Referência na documentação oficial	Transcrição
1.1. 3.x.x	Processar 150 mil mensagens por hora, com tamanho médio de 100KB, sem ocorrência de enfileiramento para processamento (congestionamento).	Datasheetpág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.2. 3.x.x	Implementar o protocolo SMTP (Simple Mail TransferProtocol) em compliance com a RFC;	InstalationGuide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.3. 3.x.x	Autenticação SMTP com suporte a autenticação via LDAP, RADIUS, POP3 e IMAP;	Productguide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.4. ...	...	...	...

_____(nome e assinatura)_____

Nome completo, telefone, e-mail

ANEXO III – Modelo de Plano de Testes

Tabela – Modelo de Plano de Testes

Descrição do Teste	Resultado Esperado	Resultado Obtido
1. Validar geração de Logs de transferência de mensagens;	Visualizar os logs dentro da interface de gerência do equipamento	OK / FALHA
2. Configurar envio de logs para centralizador de logs;	Recebimento de logs pelo centralizador de logs	OK / FALHA
3. Integrar-se com servidores de autenticação Microsoft Active Directory para verificação de destinatários validos;	Listar caixas postais dos usuários	OK / FALHA
4. Validar implementação do modo cluster	Nós do cluster com comunicação de controle efetiva	OK / FALHA

_____(nome e assinatura)_____

Nome completo, telefone e e-mail.

ANEXO IV – Modelo de Proposta de Preços

Tabela – Modelo de Proposta de Preços

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	1	Solução de gestão e correlação de eventos de segurança da informação (SIEM) e gestão da resposta a incidentes de segurança da informação (SOAR). Incluindo licenciamento, garantia do fabricante e atualização de versão pelo período de 5 anos.	Unidade	1	(numerais)	(numerais)
	2	Serviços de implantação, instalação e configuração da solução contratada	Serviço	1	(numerais)	(numerais)
	3	Transferência de conhecimento	Serviço	1	(numerais)	(numerais)
	4	Serviço de gestão, descoberta e resposta a incidentes de segurança da informação (SIEM/SOAR)	Meses	36	(numerais)	(numerais)
VALOR TOTAL GLOBAL						**(numerais)**

_____(nome e assinatura)_____

Nome completo, telefone e e-mail

Assinado por:

MICHELLE DE CASTRO CARNEIRO - SECONSTI/STI em 13/09/2021.
PAULO LUIZ ALMEIDA DOS REIS - SECONSTI/STI em 13/09/2021.
PEDRO ROGÉRIO VIEIRA DIAS - SESEG/STI em 13/09/2021.

Assinatura(s) pendente(s):

DANIEL GUIMARÃES PENA
.