



MINISTÉRIO DA CULTURA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

Edifício Parque Cidade Corporate, Torre B, 10º andar - Bairro Asa Sul, Brasília/DF, CEP 70308-200
Telefone: - <http://www.cultura.gov.br>

CADERNO DE ESPECIFICAÇÕES TÉCNICAS

PROCESSO: [01400.013417/2023-97](#)

**DOCUMENTOS
RELACIONADOS**

OBJETO - Aquisição de Solução para Proteção de Avançada de Infraestrutura de TI (NDR/XDR) com garantia de suporte e atualização por trinta e seis (36) meses.

ESTUDO TÉCNICO PRELIMINAR XX/2024

CONTRATAÇÃO: 420001/0000XX/2024

QUADRO DE COMPOSIÇÃO - GRUPOS E ITENS.

GRUPO	ITEM	Descrição	QTDE	UNIDADE
01	01	Solução de monitoramento de comportamento anômalo da rede, detecção, análise, resposta e monitoramento de incidentes de segurança da informação.	1	Sensor
	02	Serviços de Instalação, Configuração e Implementação	1	Unidade de Serviço
	03	Treinamento (Transferência de Conhecimentos)	1	Turma

1. ITEM 1: SOLUÇÃO DE MONITORAMENTO DE COMPORTAMENTO ANÔMALO DA REDE, DETECÇÃO, ANÁLISE, RESPOSTA E MONITORAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.

1.1. Requisitos Mínimos Gerais

1.1.1. A solução de segurança deverá ser composta de dispositivo do TIPO Appliance Físico mais softwares necessários. Poderá ser composta por um ou mais softwares licenciados para atender ao requisitado. Deve ser entregue plenamente interoperáveis entre si e ser do mesmo fabricante.

1.1.2. As funcionalidades de detecção (sensor de detecção), deverão ser obrigatoriamente entregues em formato de Appliance física. As demais funcionalidades podem opcionalmente, serem fornecidas como Appliance virtual.

1.1.3. Todos os módulos e componentes que compõem a solução deverão se integrar, visando a homogeneidade do ambiente tecnológico para análise de tráfego, monitoramento, investigação, defesa, prevenção e resposta a ameaças e incidentes.

1.1.4. Toda a solução deve ser compatível com os componentes lógicos e físicos em operação no ambiente do MinC, tais como servidores, AD (Active Directory), IPS, SIEM, WAF, switches de rede, firewall, etc, funcionando sem impacto à essas soluções.

1.1.5. A retenção, por parte da solução, dos fluxos de rede (network flows) e seus respectivos metadados, bem como incidentes, eventos e demais informações, deve ser por um período mínimo de 90 (noventa) dias corridos.

1.1.6. A solução deverá possuir ferramenta do tipo honeypot (sistema configurado como uma espécie de emboscada mediante a emulação de um alvo para atrair ataques cibernéticos, registrando as tentativas de intrusão para obter informações e o comportamento dos cyber-criminosos).

1.1.7. A solução deverá permitir a detecção avançada de malware baseada em comportamento.

1.1.8. A solução deverá prover os seguintes perfis de acesso, a fim de permitir a visualização de incidentes/eventos em tempo real, alertas, status das ações tomadas, etc:

1.1.8.1. Alta administração (coordenadores, gestores);

1.1.8.2. Equipe técnica (painel completo e detalhado);

1.1.8.3. Auditores (auditor interno, auditores externos etc.).

1.2. **Requisitos de Arquitetura Tecnológica**

1.2.1. Toda a solução (hardware e software) fornecida deverá ser de um único fabricante em que seus módulos e/ou programas sejam totalmente integrados, de modo a preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação.

1.2.2. A solução deverá vir acompanhada de todos os elementos/acessórios necessários à sua implantação (conectores, cabeamentos, etc.).

1.2.3. Nenhum dos componentes da solução poderá ter seu end-of-sale e end-of-life anunciado no momento do aceite definitivo de sua entrega. Caso seja essa a situação, o fornecedor deverá entregar um modelo equivalente ou superior ao que entrou nas situações anteriores.

1.2.4. No caso do anúncio end-of-sale e end-of-life ocorrer após o aceite definitivo da entrega da solução, o end-of-support não poderá ocorrer nos próximos 30 (trinta) meses, a contar da emissão do anúncio.

1.2.5. Todos os componentes da solução (hardwares e softwares) deverão ser fornecidos com todas as licenças necessárias ao seu pleno funcionamento, de modo a realizar todas as funcionalidades requeridas.

1.2.6. Não serão aceitas soluções com software e hardware de fabricantes distintos, ou mesmo soluções de uso geral como Servidores, Estações de Trabalho ou Equipamentos como Blades.

1.2.7. As licenças a que se refere o item anterior deverão ter caráter perpétuo, não precisando de renovação, de modo que, após o tempo de contrato, a solução permaneça indefinidamente plenamente funcional, devendo sua atualização (subscrição) ser garantida pelo prazo do contrato.

1.2.8. Os equipamentos devem possuir profundidade dentro dos padrões

dos racks; caso não se enquadrem neste padrão, deverá ser fornecido todos os requisitos para a fixação no rack (bandeja, parafuso, etc).

1.2.9. Todos os equipamentos devem ser fornecidos com cabos de energia com no mínimo 1,80m já com o plug no padrão hoje utilizado pelo MinC, cabendo ao Licitante durante a oportunidade de vistoria verificar o modelo (ou solicitar a informação via e-mail ou contato telefônico), para que o fornecimento ocorra de acordo com a necessidade do Ministério. Caso não seja do mesmo padrão, deverá ser considerado o fornecimento de adaptadores para o citado padrão.

1.3. Requisitos Mínios do Appliance para análise de comportamento anômalo da rede (sensor)

1.3.1. O appliance e o sistema proposto devem atender às características técnicas mínimas obrigatórias exigidas em cada item.

1.3.2. O appliance deve ser novo e de primeiro uso, devendo estar em linha de produção, com a última versão de software e/ou firmware disponível e sendo comercializado pelo Fabricante.

1.3.3. O appliance deverá possuir altura de, no máximo, 1U, para ser instalado em rack de 19" e ser fornecido com o kit de instalação.

1.3.4. Caso o appliance ofertado possua altura maior do que 1U, a licitante deverá fornecer o rack equivalente, sem qualquer Ônus ao MinC.

1.3.5. A solução proposta deve suportar um throughput de detecção de violação de 2 Gbps.

1.3.6. A solução proposta deve suportar pelo menos 1TB SSD de espaço de armazenamento.

1.3.7. A solução proposta deve suportar 1.3 milhões de sessões simultâneas.

1.3.8. A solução proposta deve suportar 70 mil novas sessões/segundos com tráfego HTTP.

1.3.9. O appliance devem possuir capacidade de processamento e memória suficiente para operar com todas as funcionalidades contratadas simultaneamente e no volume máximo de tráfego estabelecido.

1.3.10. O appliance que compõem a solução deve possuir 1 (uma) fonte de alimentação, do tipo hot-swappable, com alimentação de 100~120VAC e 210~240VAC e frequência de 50 ou 60 Hz ou auto-ranging.

1.3.11. O appliance deve possuir 2 (duas) interfaces de 10 Gbps (SFP+), 8 (oito) interfaces de 1Gbps (SFP) e 8 (oito) interfaces GE, para ligação física ao switch core do ambiente local, devendo estar acompanhado de transceiver nas interfaces SFP+ para realizar essa ligação.

1.3.12. A plataforma deve ser capaz de monitorar todo o comportamento do tráfego da rede interna do MinC, a partir da captura de pacotes espelhados para a appliance através do switch core local.

1.4. Requisitos de Detecção de Incidentes (Incident Detection)

1.4.1. A solução deve criar linhas de base dos logs dos ativos de sustentação, visando montar um perfil do risco e do consumo de cada um deles.

1.4.2. A solução deve executar o correlacionamento dos eventos para detectar táticas, técnicas e procedimentos de ataques, identificados pela modelagem de ameaças desenvolvida pelo MITRE, disponível em <https://attack.mitre.org/>.

1.4.3. A solução deve detectar ataques internos (leste-oeste) e externos

(norte- sul) contra a infraestrutura de TIC do MinC.

1.4.4. A solução deve identificar os seguintes casos de uso nos ativos de sustentação:

- 1.4.4.1. Execução de programas maliciosos (exploits ou payloads);
- 1.4.4.2. Movimentação lateral;
- 1.4.4.3. Escalação de privilégios;
- 1.4.4.4. Sinalização (beaconing) ou conexão com Centrais de Comando e Controle;
- 1.4.4.5. Exfiltração de dados;
- 1.4.4.6. Ataques fileless, via Powershell;
- 1.4.4.7. Exploração de vulnerabilidades dos ativos de sustentação, de conhecimento público, publicada pelo MITRE em <https://cve.mitre.org/>;
- 1.4.4.8. Varreduras de portas tcp e udp;
- 1.4.4.9. Tráfego de IPs inscritos em listas negras, públicas ou privadas;
- 1.4.4.10. Tentativas de login em horário atípico;
- 1.4.4.11. Quebra de senha;
- 1.4.4.12. Surto de worm / vírus;

1.4.5. A solução deverá identificar no mínimo os seguintes casos de uso de detecção em aplicações web:

- 1.4.5.1. Ataques de Injeção SQL;
- 1.4.5.2. Ataques de Cross site scripting;
- 1.4.5.3. Todos os ataques da Web de camada 7 via internet / intranet;
- 1.4.5.4. Tentativa de violação de acesso;

1.4.6. A solução deverá identificar ataques a partir do tráfego da rede, incluindo, mas não se limitando a:

- 1.4.6.1. Movimentação lateral;
- 1.4.6.2. Beacon de malware;
- 1.4.6.3. Exfiltração de dados;
- 1.4.6.4. Ransomware;

1.4.7. Além dos casos de uso detecção de uso definidos estaticamente, a solução deverá incorporar Inteligência Artificial (IA) e/ou Machine Learning (ML) para detectar anomalias, a fim de acelerar a análise de comportamento incomum nos ativos de sustentação.

1.4.8. A solução deve suportar pelo menos 8 mil assinaturas de IPS/IDS. Deve suportar assinaturas personalizadas, atualizações manuais de inserção ou extração de assinaturas automáticas e uma enciclopédia de ameaças incorporada

- 1.4.8.1. A solução deve suportar detecção e proteção de anomalias de protocolo, incluindo os protocolos NETBIOS, SMTP, IMAP, POP3, VOIP e HTTP.

1.4.9. A solução deve ter a função de captura de pacotes.

1.4.10. A solução deve suportar pelo menos 13 milhões de assinaturas antivírus, com atualizações manuais ou automáticas de assinatura.

- 1.4.10.1. A solução deve ser compatível com o Flow Based Antivirus para os protocolos SMTP, POP3, IMAP, FTP e HTTP.
- 1.4.10.2. A solução deve suportar a detecção de vírus para arquivos

compactados como RAR, ZIP e TAR.

1.4.11. A solução deve suportar a descoberta eficaz de bots de intranet e a prevenção de novos ataques avançados de ameaças, comparando as informações obtidas com o banco de dados de endereços de C&C.

1.4.12. A solução deve suportar atualização automática da biblioteca de assinatura de defesa contra Botnet/C&C.

1.4.13. A solução deve suportar a detecção do DoS/DDoS e SYN Flood.

1.4.14. A solução deve possuir ambiente de execução virtual de malware (sandbox), baseado em nuvem para encontrar ameaças desconhecidas.

1.4.15. A solução deve suportar o upload de arquivos maliciosos para sandbox na nuvem para análise.

1.4.16. A solução deve suportar o upload de arquivos maliciosos de protocolos incluindo SMTP, FTP, HTTP/HTTPS, IMAP e POP3.

1.4.17. A solução deve suportar o compartilhamento global de inteligência de ameaças, para detectar a nova ameaça desconhecida.

1.4.18. A solução deve suportar classificação e detecção de spam em tempo real. A solução deve suportar as categorias de Spam Confirmado, Spam Massivo e Spam Suspeito.

1.4.19. A solução deve suportar a detecção, independentemente do idioma, formato ou conteúdo da mensagem.

1.4.20. A solução deve suportar os protocolos de e-mail SMTP e POP3

1.4.21. A solução deve suportar lista de permissão para e-mails de domínios confiáveis.

1.5. **Requisitos para Análise de Incidentes (Incident Analysis)**

1.5.1. A solução deverá suportar algoritmos de triagem orientados por máquina (Machine Learning), que considere parâmetros contextuais, comportamento histórico e inteligência de ameaças externas, a fim de definir a severidade/pontuação para o incidente, em tempo real. A referida severidade/pontuação deve servir de base para priorizar alertas e outras ações referentes ao incidente:

1.5.2. O feed de inteligência de ameaças também deve ser utilizado para identificar ataques por meio de agentes mal-intencionados.

1.5.3. A solução deverá oferecer suporte a um mecanismo que permita a adequação das regras.

1.5.4. A solução deverá permitir a investigação de alertas de triagem personalizados considerada crítica.

1.5.5. A solução deverá possuir recursos para analisar o impacto do ataque no ativo alvo, incluindo indicadores de comprometimento (IOCs), conexões de rede externas.

1.5.6. A solução deverá oferecer suporte para analisar e identificar o impacto de um ataque nos ativos de sustentação.

1.5.7. A solução deverá fornecer recursos de gerenciamento para armazenar evidências relativas a um alerta específico ou conjunto de alertas.

1.5.8. A solução deverá oferecer suporte à pesquisa rápida em conjuntos de dados armazenados, com base em critérios personalizados.

1.5.9. A solução deverá fornecer recursos para fazer análise visual do fluxo de alertas, integrada ao log de evidências, objetivando proporcionar uma análise eficiente, com opções para rastrear a cadeia de ataque em qualquer escala.

- 1.5.10. A solução deverá ser capaz de definir, desenvolver e implementar casos de uso de detecção dos incidentes, observada a modelagem de ameaças previstas no framework ATT&CK, a fim de avaliar o tratamento de todas as etapas do ciclo de vida do ataque.

1.6. **Requisitos de Resposta a Incidentes (Incident Response)**

- 1.6.1. A solução deve elaborar e programar fluxos de trabalho (playbooks) capazes de orquestrar e automatizar as atividades de resposta a incidentes, inclusive com tratamento de falso positivo, listas brancas, escalonamento e indicadores para gestão.
- 1.6.2. O sistema deverá analisar um incidente a partir de uma base de dados analítica de evidências e indícios de ataques.
- 1.6.3. O sistema deverá manter o controle da primeira resposta e das medidas subsequentes tomadas no incidente.
- 1.6.4. O sistema deverá registrar a ordem cronológica dos eventos.
- 1.6.5. O sistema deverá registrar os IOCs e artefatos relacionados ao incidente.
- 1.6.6. A plataforma deverá permitir, em conjunto com a equipe de segurança do MinC, a forma de registro de comentários e orientações, preservação do histórico de conversa, e capacidade de adicionar artefatos e evidências.
- 1.6.7. A resposta adequada e automatizada será utilizada para executar roteiros pré-aprovados juntamente com a equipe de segurança do MinC, tais como: bloquear IP's no firewall e criação de políticas de segurança.
- 1.6.8. Espera-se não apenas uma solução que tenha capacidade de integração com outras soluções existentes para resposta aos incidentes, mas também que a própria solução (através de componente nativo ou componente adicional) execute a remediação. A contratada se torna responsável pela entrega da solução completa que será inserida à rede da Contratante para bloqueio em tempo-real ou próximo à tempo-real, das ameaças identificadas pela solução.
- 1.6.9. A solução deverá ter capacidade de remediar e prevenir ameaças encontradas de acordo com os padrões citados anteriormente, possuindo assim capacidade de prevenção contra intrusões (IPS).
- 1.6.10. Essas prevenções devem ocorrer a nível de rede, e não serão permitidas soluções que dependam da solução de firewall em uso, ou de outro componente da estrutura do Contratante. Devendo a solução ser entregue de forma completa a fim de identificar, correlacionar, analisar, e responder às ameaças de forma autônoma.
- 1.6.11. A solução deve permitir que se crie listas de permissão (whitelists) para o módulo de remediação;
- 1.6.12. Caso seja necessário o uso de uma ferramenta diferente para prevenção e bloqueio (Sistema de Prevenção - IPS), esta deverá ser do mesmo fabricante das demais soluções ofertadas além de, obrigatoriamente, ser entregue em formato de hardware, com capacidade de throughput equivalente à 15Gbps conforme necessidade de rede no MinC. Deve ainda possuir minimamente 2 (duas) interfaces 10Gbps no padrão SFP+ com seus respectivos transceivers instalados.
- 1.6.13. A remediação através de função de prevenção, deve suportar as seguintes ações:
- 1.6.13.1. Monitorar;
 - 1.6.13.2. Bloquear;
 - 1.6.13.3. Reset (IP do atacante, IP da vítima ou interface de entrada), com tempo de expiração.
- 1.6.14. A solução deverá fornecer relatórios de respostas aos incidentes,

onde estes devem ser apresentados por ordem cronológica, por ativos afetados, por classificação de risco, ou por IOCs.

1.6.15. A solução deverá identificar o tráfego de rede atípico promovido por aplicativos, como por exemplo compartilhamento de arquivos, comunicação peer-to-peer (P2P), dentre outros.

1.6.16. A solução deverá produzir informações por meio da investigação de ataques, devendo estar estruturadas para apoiar o serviço de detecção.

1.7. **Requisitos para Investigação de Ameaças (Cyber Threat Hunting)**

1.7.1. A plataforma deve utilizar algoritmos e ferramentas para investigar ativa e proativamente ataques que estejam sendo perpetrados na infraestrutura de TI, e encaminhar alertas a serem analisados pelos analistas de detecção.

1.7.2. A plataforma deve ser capaz de estabelecer, desenvolver, programar, atualizar e manter uma estrutura de investigação que contemple:

1.7.2.1. Ações que identifiquem atividades maliciosas que ainda não tenham gerado alertas.

1.7.2.2. Ações apoiadas por indicadores de comprometimento (IOC), recebidos de centrais de Cyber Threat Intelligence.

1.7.3. A solução deverá possuir capacidade manter base de conhecimento de IOCs;

1.7.4. A solução deverá possuir capacidade de detectar ataques desconhecidos;

1.7.5. A solução deverá possuir modelos aptos a detectar estágios de uma cadeia de ataque cibernético;

1.7.6. A solução deverá elencar os casos de uso que podem detectar ataques, usando técnicas de aprendizado de máquina e modelos analíticos.

1.7.7. A solução deverá possuir modelos de Inteligência Artificial (IA) para detectar ataques desconhecidos de agentes desconhecidos.

1.7.8. A solução deverá possuir modelos analíticos para detectar diferentes estágios de cadeia de ataques.

1.8. **Requisitos para Inteligência de Ameaças e Automação Central**

1.8.1. A solução deverá possuir console baseada em software, que permita a centralização dos eventos e a resposta de bloqueio às ameaças. Essa console central deve estar preparada para o eventual crescimento da quantidade de sensores de detecção de ameaças no ambiente no MinC.

1.8.2. Para total atendimento as especificações solicitadas, pode-se realizar composição com solução adicional, desde que não seja software livre. Caso a solução adicional não seja do mesmo fabricante da solução principal, deve possuir integração nativa entre as plataformas, e com ponto único de suporte;

1.8.3. A console central poderá ser embarcada dentro dos sensores NDR ou separadamente. No caso de versão apartada, deverá ser virtual e instalada em localmente no ambiente da CONTRATANTE, devendo estar disponível de forma local (on-site), em modelo virtual. Deve estar disponível para instalação em ambientes VMware ESXi e Hyper-V.

1.8.4. A solução deverá fornecer painel central para demonstrar a postura de risco e os níveis de maturidade de organização para tratar as ameaças.

1.8.5. A solução deverá fornecer painel de segurança abrangente, baseado na web, para visualização de incidentes/eventos em tempo real, alertas, status das ações

tomadas, indicadores do ranking das ameaças, dentre outros.

1.8.6. Caso essa console ou o próprio sensor NDR possua métrica de consumo ou limitação de EPS (Eventos por segundo), a solução deve ser capaz de tratar até 5.000 (cinco mil) EPS para coleta, processamento, armazenamento e correlacionamento dos eventos de rede, de forma sustentada.

1.8.7. A solução deverá oferecer resposta automatizada para incidentes, por meio da conexão remota a outros componentes através de SSH, HTTP ou API com IPS, WAF, switches de rede, firewalls e roteadores.

1.8.8. A solução deverá possibilitar integração com o recurso de segurança System Monitor (Sysmon).

1.8.9. A solução deve ser capaz de coletar eventos de todos os ativos de sustentação do ambiente, e normalizá-los em um formato padrão para possibilitar a sua estruturação, correlação, criação de regras de análises e resposta a incidentes.

1.8.10. A solução deverá se integrar com as fontes de log (SIEM, EDR, EPP, IAM, PAM), via protocolo Syslog, a fim de ingerir dados do ambiente e enriquecer as investigações de ameaças.

1.8.11. A solução deverá suportar Netflow para recebimento de flows de rede a fim de ingerir dados do ambiente e enriquecer as investigações de ameaças.

1.8.12. Deve possuir banco de dados de inteligência de domínios DNS, códigos maliciosos, IP, vulnerabilidades, detecções de intrusão e geolocalização.

1.8.13. Deve suportar análise de killchain e integração com o MITRE ATT&CK para definição de técnica e tática.

1.8.14. Deve suportar pesquisa por palavras-chave, SPL e condições predefinidas nos logs recebidos.

1.8.15. A solução deve suportar REST API.

1.8.16. Deverá possuir capacidade de criação de regras para automação de respostas através de fluxos de trabalho (playbooks), com regras pré-definidos e capacidade de criação de regras customizados através da interface gráfica.

1.8.16.1. A funcionalidade de automação de respostas, deverá ainda permitir que estas regras sejam utilizados para automação de respostas aos incidentes conforme configuração de gatilhos (triggers).

1.8.16.2. Essas triggers a serem usadas, podem ser eventos/características de ameaças, consulta de inteligência de ameaças, condições de julgamento para resposta automática e ações de processamento de resposta (políticas de emissão, bloqueio de IP ou criação de ordens de serviço), de modo a realizar resposta automática diretamente pela solução contratada ou através de outro dispositivo.

1.8.17. Deve suportar a geração de relatórios de ameaças e eventos.

1.8.18. A solução deverá ser capaz de tomada de decisões por meio validação em fontes externas, tornando mais eficiente o processo de identificação, reduzindo deste modo os falsos positivos.

1.8.19. A solução deverá fornecer inteligência de nível estratégico contra ameaças, por meio de notificações de incidentes e violações que ocorrem na web, permitindo identificar:

1.8.20. Quais são os IoC's relacionados às ameaças

1.8.20.1. Quais etapas de mitigação devem ser tomadas para conter a ameaça.

1.8.21. A inteligência de ameaças deve alcançar todos os ativos de sustentação, tráfegos de rede, evento de segurança e usuários, de modo a fornecer prognósticos de impacto de ameaças sobre os ativos do MinC, e destacar as medidas preventivas

que devem ser adotadas.

1.8.22. A solução deverá possuir algoritmos para avaliar automaticamente um ativo, e atribuir um valor de risco ao mesmo.

1.8.23. A solução deverá oferecer suporte à inteligência de ameaças externas de terceiros para subsidiar a resposta a incidentes, inclusive com o contexto organizacional, informações internas e outras fontes de informações de segurança.

1.8.24. A solução deve apresentar visão agregada de todos os sensores que houver na rede, em um único local, e com visão no mínimo para:

1.8.24.1. Agregação de lista de eventos por endereço do atacante;

1.8.24.2. Agregação de lista de eventos por endereço da vítima;

1.9. **Requisitos de Garantia Técnica**

1.9.1. A garantia técnica deverá ser realizada durante todo o período contratual, permitindo cobertura completa e de uso operacional do equipamento em todas as funcionalidades atualmente contratadas.

Deve fazer parte da garantia todos os custos operacionais para reprogramações dos sistemas, correções de falhas de software, atualização de versões dos módulos de software, incluindo sistema operacional do equipamento e firmwares, disponibilizados pelo fabricante da solução durante o prazo contratado, sem custo adicional para o MinC das novas versões de atualização que porventura vierem a ser publicadas.

1.9.2. A garantia deverá cobrir a resolução de falhas, erros, problemas, instabilidades e vulnerabilidades em quaisquer dos componentes físicos e lógicos dos equipamentos fornecidos, incluindo a substituição completa ou parcial de equipamentos que venham a apresentar problemas de funcionamento, sem ônus adicional para o MinC, quando da necessidade de manutenções corretivas e/ou manutenções evolutivas do hardware.

1.9.3. Durante a vigência do contrato, todas as funcionalidades dos equipamentos adquiridos deverão ser atualizadas a medida do lançamento de novas versões, sem custos para o MinC.

1.9.4. A garantia dos equipamentos, além de englobar todos os seus componentes e licenças, deverá cobrir o direito do MinC ao recebimento de todas as novas versões, atualizações, correções, sejam do próprio fabricante, sejam de features instaladas, bem como de licenças que eventualmente venham a ser substituídas, devendo ser instaladas ou atualizadas pela Contratada com o acompanhamento da equipe técnica do MinC.

1.9.5. A CONTRATADA deverá oferecer garantia dos produtos (hardware e software) entregues pelo prazo de 36 (trinta e seis) meses, o qual será contado a partir do recebimento definitivo da solução.

1.9.6. O direito do MinC à garantia técnica cessará caso a solução seja alterada pela próprio MinC ou por fornecedores que não a Contratada responsável pelo serviço em questão.

1.9.7. A Contratada deverá possuir suporte e venda assegurados pelo Fabricante, com o fornecimento de peças de reposição e correção de falhas de software durante o prazo de garantia.

1.9.8. A guarda de componentes de reposição removidos não será de responsabilidade do MinC. Todo o trâmite para sua devolução deve ser providenciado pela Contratada, conforme os ditames previstos na Lei nº 12.305/2010, Política Nacional de Resíduos Sólidos.

1.9.9. Correrá por conta exclusiva da Contratada a responsabilidade pelo

deslocamento do pessoal necessário, bem como pela retirada e entrega dos equipamentos, peças, componentes e acessórios de substituição e todas as despesas de transporte e frete correspondentes.

1.9.10. Em caso de componentes ou dispositivos da solução substituídos nas instalações do ambiente do MinC, estes deverão possuir garantia de 36 (trinta e seis) meses, tal qual os originais substituídos.

2. ITEM 2: SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLEMENTAÇÃO

2.1. Para todos os produtos da solução (hardware ou software) adquirida, a Contratada deverá fornecer serviço especializado de instalação, configuração e implementação da solução no ambiente do MinC.

2.2. A Contratada deverá realizar o armazenamento, a embalagem e desembalagem, o transporte, a entrega e a instalação de todo e qualquer item da solução no local de implantação da solução.

2.3. Os serviços especializados de instalação, configuração e implementação deverão ocorrer em dias úteis, no horário compreendido entre 8:00h e 17:00h, salvo definição contrária estabelecida em comum acordo entre Contratante e Contratada.

2.4. O serviço de instalação, configuração e implementação deverá ser agendado previamente com a equipe técnica do MinC.

2.5. Entende-se por serviço instalação, configuração e implementação a montagem física de todos os equipamentos da solução adquirida (incluindo o fornecimento, por parte da Contratada, de trilhos de fixação e cabos UTP ou FO), a configuração e interligação física (cabeamento) e lógica à rede de dados do MinC, bem como a instalação e configuração dos softwares necessários ao pleno funcionamento da solução, sendo a Contratada responsável integral por todo o escopo referente a este item.

2.6. Os serviços especializados de instalação, configuração e implementação deverão ser executados por profissionais alocados pela Contratada, que deverão ser devidamente certificados pelos respectivos fabricantes dos produtos ofertados, sendo que tal condição deverá ser demonstrada mediante documento de comprovação (certificação técnica na plataforma a ser implantada) durante a execução do objeto.

2.7. As despesas de viagens, hospedagem, diárias, alimentação e demais para execução dos serviços correrão integralmente por conta da Contratada.

2.8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente ou via conferência web, devendo a futura Contratada sugerir as configurações de acordo com normas e boas práticas, cabendo ao MinC a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

2.9. A Contratada deverá agendar visitas técnicas de pré-instalação (site survey) nas dependências designadas pelo MinC para definição do posicionamento dos equipamentos, da instalação elétrica e demais requisitos necessários à instalação física da solução. As visitas deverão ser realizadas em até 5 (cinco) dias corridos contados da assinatura do Contrato, e o produto destas visitas técnicas será um relatório detalhado do site survey, a ser elaborado pela Contratada, e posteriormente apresentado na reunião de abertura de projeto (kick-off).

2.10. A Contratada deverá fazer análise do ambiente tecnológico atual, devendo o MinC fornecer:

2.10.1. Informações necessárias sobre a infraestrutura instalada, de modo que se possa assegurar a continuidade dos serviços prestados pelo Ministério durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.), e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.);

e

2.10.2. Informações necessárias à implantação da solução, como topologia de rede, VLANs, endereçamento IP, portas de switches que devem ser utilizadas e outras necessárias à perfeita configuração e interligação.

2.10.3. A Contratada deverá apresentar um Projeto Executivo, que será avaliado e aprovado pela equipe técnica do MinC, contendo no mínimo o seguinte:

2.10.4. descrição dos equipamentos e softwares que deverão ser instalados;

2.10.5. deverão ser descritos pré-requisitos com os recursos e condições que deverão ser providos pelo MinC, necessários para que a Contratada possa realizar os serviços de instalação;

2.10.6. relatórios das visitas técnicas (site survey) de pré-instalação;

2.10.7. atividades a serem desenvolvidas, incluindo cronogramas;

2.10.8. desenho da arquitetura lógica da solução, contendo a topologia da solução, indicando as alterações com relação à topologia atual;

2.10.9. desenho da arquitetura física da solução, contendo tabela de conectividade física da solução, com o mapeamento das conexões necessárias diretamente nos dispositivos de rede do MinC;

2.10.10. políticas de configuração dos elementos da solução;

2.10.11. ações de rollback, descrevendo as ações necessárias para restabelecimento do ambiente à normalidade, no evento de falhas no funcionamento das novas soluções que causem interrupção no fluxo de dados da rede;

2.10.12. Caderno de Testes e Homologação, para validação da solução.

2.11. O MinC será responsável pelo fornecimento de listagem com todas as aplicações/sistemas que serão configuradas na implantação.

2.12. No prazo de até 5 (cinco) dias corridos, a partir do recebimento formal do Projeto Executivo, o MinC deverá se manifestar sobre sua aprovação. Caso seja(m) necessário(s) ajuste(s) no documento, este será devolvido à Contratada e será concedido à mesma um novo prazo de até 2 (dois) dias corridos, para elaboração e entrega da versão definitiva do citado documento, a ser aprovada pelo MinC.

2.13. Será de total responsabilidade da Contratada o dimensionamento da solução a ser implantada na rede do MinC, sendo este sujeito à análise e validação da equipe técnica do MinC, em conformidade aos requisitos solicitados na contratação.

2.14. Caso o dimensionamento feito pela Contratada não apresente desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto no item anterior, a solução deverá ser redimensionada sem ônus adicional para o MinC, mesmo que o redimensionamento envolva adição/substituição de hardware e software.

2.15. Os serviços especializados de instalação, configuração e implementação deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante, em seus manuais de instalação e configuração e/ou em artigos técnicos.

2.16. A equipe técnica do MinC acompanhará e supervisionará todas as etapas de instalação física dos equipamentos no Datacenter.

2.17. A solução apresentada não pode causar impacto na operação da rede do MinC (por exemplo, lentidão na rede local, degradação no desempenho dos ativos, entre outros).

2.18. A implementação da solução deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional do MinC; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser executadas durante janela de manutenção

agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados, sem ônus adicional para o MinC.

2.19. O Caderno de Testes e Homologação consiste num documento onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos e os resultados aguardados para cada teste executado, bem como avaliar o perfeito funcionamento dos produtos, em conformidade às especificações definidas quando da contratação do objeto e à proposta da Contratada, e a sua compatibilidade com a estrutura já existente no MinC.

2.20. Os testes serão realizados pela Contratada após a instalação e configuração dos produtos, e deverão ser acompanhados pela equipe técnica do MinC.

2.21. Caso seja detectado qualquer problema nos testes, em qualquer funcionalidade, a Contratada deverá efetuar as devidas correções e, após a realização dessas, os testes serão reiniciados.

2.22. Caso todos os testes executados logrem êxito, os produtos serão considerados implantados.

2.23. A homologação somente poderá ser iniciada após a conclusão da implantação.

2.24. Pelo menos um técnico da Contratada deverá acompanhar presencialmente o decorrer dos procedimentos de homologação.

2.25. No decorrer dos procedimentos de homologação, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos.

2.25.1. Em caso de qualquer falha ou interrupção em qualquer uma das funcionalidades, a Contratada deverá efetuar as devidas correções e, após a realização destas correções, a homologação será reiniciada.

2.25.2. Na ausência de qualquer falha ou interrupção em qualquer uma das funcionalidades, a solução será considerada homologada.

2.26. Caso seja constatada a ocorrência de divergências na especificação técnica ou qualquer outro defeito de operação durante quaisquer etapas da instalação da solução, fica a Contratada obrigada a providenciar a sua correção ou a substituição dos produtos adquiridos.

2.27. Em caso de detecção de anormalidades ou problemas, o MinC comunicará formalmente os problemas detectados e a inconclusão da instalação, sendo que a Contratada terá prazo adicional de 10 (dez) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da comunicação, para sanar os problemas/anormalidades detectados, sujeitando-se a Contratada às sanções e/ou penalidades previstas.

2.28. Para todos os efeitos, a conclusão dos serviços de instalação, configuração e implementação será atestada pela entrega da solução em pleno funcionamento, incluindo documentação técnica (as-built) contendo planejamento, relatório de todos os procedimentos realizados, parametrizações, testes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidas contratualmente.

2.29. Os serviços de fornecimento do objeto, isto é, a execução completa dos serviços e tarefas previstas por todas as etapas de trabalho conforme o Cronograma de Execução, deverão ser executados no prazo máximo de até 120 (cento e vinte) dias consecutivos a partir da assinatura da Ordem de Fornecimento de Bens.

2.29.1. Caberá à Contratada o irrestrito cumprimento de, no mínimo, as seguintes prerrogativas:

2.29.1.1. Realizar a transferência de conexão dos equipamentos conectados à rede LAN existente no MinC para todos os equipamentos da solução adquirida;

2.29.1.2. Adequar e configurar os produtos fornecidos ao longo das

etapas destinadas a colocar a solução em produção;

2.29.1.3. Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma;

2.29.1.4. Providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;

2.29.1.5. Realizar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;

2.29.1.6. Elaborar a “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

2.30. Os serviços especializados de instalação e implementação deverão ser executados por profissionais alocados pela Contratada, que deverão ser devidamente certificados pelos respectivos fabricantes dos produtos ofertados, sendo que tal condição deverá ser demonstrada mediante documento de comprovação (certificação técnica na plataforma a ser implantada) durante a execução do objeto.

3. ITEM 3: TREINAMENTO (TRANSFERÊNCIA DE CONHECIMENTOS)

3.1. Visando capacitar a equipe técnica do MinC na operacionalização plena da solução completa, a Contratada deverá executar transferência de conhecimentos da solução, de modo a capacitar a equipe técnica do MinC para a utilização de todos os recursos operacionais disponíveis da solução.

3.2. A Contratada deverá apresentar um Plano de Capacitação no prazo máximo de 20 (vinte) dias corridos após assinatura do Termo de Contrato, onde deverá constar no mínimo:

3.2.1. conteúdo programático;

3.2.2. carga horária;

3.2.3. que lhe confira(m) as competências necessárias para ministrar a capacitação – neste caso, o profissional deverá ser certificado pelo fabricante da solução, e com experiência comprovada nos produtos fornecidos.

3.3. Após a apresentação formal da ementa da capacitação, o MinC poderá solicitar à Contratada a alteração do conteúdo mediante eventuais ajustes visando atender aos objetivos da capacitação na administração e uso da solução.

3.4. A transferência de conhecimentos só ocorrerá após agendamento prévio pela MinC, com antecedência mínima de 15 (quinze) dias.

3.5. A transferência de conhecimentos deverá ser executada em no máximo 15 (quinze) dias corridos após a implantação da solução e disponibilização das licenças no ambiente tecnológico do MinC, sem obrigatoriedade de ser treinamento oficial do Fabricante.

3.6. A transferência de conhecimentos deverá ser ministrada com carga horária mínima de 20 (vinte) horas, para o quantitativo máximo de 4 (quatro) participantes, a serem selecionados pelo MinC.

3.7. A transferência de conhecimentos não poderá ser meramente expositiva; devendo ser focada no uso prático de toda a solução implementada no ambiente tecnológico do Órgão.

3.8. A transferência de conhecimentos deverá ser ministrada preferencialmente

nas dependências do MinC, em data e horário conforme cronograma a ser estabelecido em comum acordo entre as partes.

3.8.1. Caberá ao MinC providenciar o ambiente onde será realizada a transferência de conhecimentos, cabendo à Contratada informar da necessidade de se providenciar recursos necessários para o evento (projektor, computadores, notebooks etc.).

3.9. O curso a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.

3.10. Caberá à Contratada prover o material didático individual, podendo este ser oficial do Fabricante ou baseado neste.

3.11. O idioma a ser adotado deverá ser preferencialmente o português do Brasil.

3.12. A transferência de conhecimentos provida deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente tecnológico do MinC, abrangendo, no mínimo, mas não se restringindo, os seguintes tópicos:

3.12.1. conceitos e características das funcionalidades do produto e seus modos de funcionamento;

3.12.2. instalação e configuração do appliance físico, incluindo configuração das interfaces de rede, implementação de updates, configurações em geral, etc.;

3.12.3. gerenciamento da solução, incluindo monitoramento de eventos, configuração e utilização da gerência do produto, geração de relatórios com informações do tráfego de rede, dentre outras funcionalidades de administração da solução;

3.12.4. configurações de todas as funcionalidades disponíveis na solução, políticas de segurança, identificação e prevenção dos principais ataques, monitoramento e relatórios, logs, mitigação de ataques, criptografia e segurança de dados, dentre outras funcionalidades;

3.12.5. solução de problemas ("troubleshooting", log de eventos, etc.).

3.13. Os custos referentes ao deslocamento, hospedagem e diárias dos instrutores deverão estar previstos pela Contratada na elaboração de sua proposta comercial.

3.14. Para o caso de possíveis medidas de segurança adotadas em relação à pandemia do novo coronavírus, este treinamento poderá opcionalmente ser realizado por meio de Ensino a Distância (EAD) ou transmissão em tempo real, por meio de videoconferência (desde que permita a interação entre participante e instrutor em tempo real), onde a plataforma utilizada e a respectiva gravação do conteúdo ministrado será de responsabilidade exclusiva da Contratada que, ao final do repasse, deverá fornecer a mídia gravada em formato eletrônico.

3.15. Neste caso, a plataforma utilizada será de responsabilidade exclusiva da Contratada. Todavia tal modalidade de treinamento deverá, além de permitir a interação entre participante e instrutor em tempo real, igualmente contemplar todas as exigências mínimas previstas no modelo presencial quanto da utilização de todos os recursos da solução implantada no ambiente do Órgão.

3.16. O MinC resguardar-se-á do direito de acompanhar e avaliar a capacitação mediante utilização de formulário de avaliação próprio baseado nos requisitos técnicos mínimos exigidos, que medirá o nível de satisfação dos participantes do MinC em relação à metodologia, instrutoria, qualidade dos recursos e materiais didáticos, e à carga horária efetiva, em escala de 0 (zero) até 10 (dez) pontos, cujo resultado final será a média aritmética simples obtida a partir da soma das notas de cada item avaliado dividida pela quantidade numérica destes itens avaliados pelos participantes.

3.16.1. no caso de avaliação com média global igual ou superior a 7 (sete) pontos, a transferência de conhecimentos será considerada aprovada e finalizada;

3.16.2. para uma avaliação com média global abaixo de 7 (sete) pontos, a transferência de conhecimentos será considerada insuficiente, devendo a Contratada efetuar reestruturação e/ou ajustes necessários e realizar o curso novamente, sem nenhum ônus adicional ao MinC.

3.17. Ao término da capacitação, a Contratada deverá emitir certificado individual de conclusão, para todos os participantes, sem nenhum ônus adicional ao MinC.

RAMON LEONN VICTOR MEDEIROS Integrante Requisitante	MARIA APARECIDA GOMES Integrante Técnico
Portaria SPOA/MINC Nº 230/2024 (SEI nº 1959891)	



Documento assinado eletronicamente por **Ramon Leonn Victor Medeiros, Integrante Requisitante da Equipe de Planejamento da Contratação**, em 25/11/2024, às 17:30, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



Documento assinado eletronicamente por **Maria Aparecida Gomes, Integrante Técnico da Equipe de Planejamento da Contratação**, em 25/11/2024, às 17:39, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1980811** e o código CRC **90046009**.