

Estudo Técnico Preliminar 9/2024

1. Informações Básicas

Número do processo: 47648.000320/2024-01

2. Descrição da necessidade

Atualização de licenças de software antivírus corporativo para a Sede/CTN e Escritórios Avançados, com a disponibilização de solução de segurança cibernética para proteção de endpoints (estações de trabalho físicas e virtuais, servidores de rede físicos e virtuais e computadores portáteis) da rede corporativa da Fundacentro, com garantia de atualizações de versões e assinaturas e suporte técnico durante todo o prazo de vigência da contratação.

3. Área requisitante

Área Requisitante	Responsável
Serviço de Tecnologia - Infraestrutura e Operações	Norisvaldo Ferraz Junior

4. Necessidades de Negócio

Controle e gestão da segurança lógica dos computadores dos usuários:

- Console de administração para os antivírus clientes nos computadores da Sede/CTN e Escritórios Avançados (EA) em um painel único
- Distribuição de atualizações a partir desse painel único

Controle e gestão da segurança lógica dos servidores de aplicação e bancos de dados da Instituição

- Console de administração para os antivírus clientes nos servidores de aplicação do centro de dados da CTIC
- Acompanhamento das atualizações nos servidores em consonância com o tipo de servidor (Windows, Linux)

Acompanhamento e monitoramento da segurança lógica da FUNDACENTRO Sede/CTN e EA

- Extração de relatórios de vírus e ameaças nos desktops, notebooks e servidores de aplicação

A Fundacentro tem um ambiente computacional composto por diversos ativos de TI, tais como: estações de trabalho, notebooks, servidores de rede físicos e virtuais, sistemas de armazenamento de dados, entre outros que, uma vez interligados em uma rede corporativa permitem o fluxo de dados eletrônicos entre eles e à Internet; são fundamentais para o provimento de serviços de TI ao seu público interno e externo contribuindo diretamente para a concretização de suas atividades e o cumprimento de sua missão. Por isso, a Fundacentro precisa garantir a segurança (com confidencialidade, integridade, disponibilidade e autenticidade) das informações eletrônicas disponibilizadas ao seu público interno e externo por meio desses ativos de TI mencionados.

O atual panorama global de ameaças cibernéticas refletiu, nos últimos dois anos, em um aumento expressivo de ocorrências de ataques cibernéticos às organizações públicas e privadas que fazem uso de malwares destrutivos, entre eles: ransomwares. Tal tendência é de elevação também para os próximos anos, na medida em que a transformação digital avança e as tais organizações disponibilizam cada vez mais serviços digitais públicos e privados na Internet.

Com isso, faz-se necessário buscar meios e mecanismos adequados para garantir a segurança cibernética desses serviços. A estratégia mais adotada é o emprego da segurança em profundidade, onde há aplicação de controles de segurança nas várias camadas de uma rede corporativa que visam mitigar, ou pelo menos reduzir, a probabilidade de concretização de riscos de ataques cibernéticos bem-sucedidos e suas consequências ao negócio: perda definitiva de dados, vazamentos de dados protegidos por legislações, indisponibilidades de serviços digitais, danos aos equipamentos e à reputação, entre outros impactos possíveis.

5. Necessidades Tecnológicas

Desktops: Operar em sistema operacional Windows 10 e superior

Notebooks: Operar em sistema operacional Windows 10 e superior e Mac

Servidores de aplicação e de banco de dados: Operar em sistema operacional para servidores de aplicação Windows (mínimo 2008 R2) e Linux

Duração da licença: Acompanhar a vigência contratual mínima de 24 meses

Língua: Os softwares deverão ser fornecidos em língua portuguesa, no mínimo, para os clientes em desktops e notebooks

Plataformas de hardware e software: Operar com mínimo de 4GB RAM em desktops, notebooks e servidores

Proteção contra malwares: Proteger os equipamentos fixos e móveis, bem como servidores de aplicação físicos e virtuais da FUNDACENTRO contra malwares

Proteção contra ataques de dia-zero: Proteger os equipamentos fixos e móveis, bem como servidores de aplicação físicos e virtuais da FUNDACENTRO contra ataques de dia-zero

Prover gerência das atualizações de vírus: Fornecer ambiente de gerenciamento centralizado da situação das licenças e dos antivírus existentes na FUNDACENTRO em todos os equipamentos da Sede/CTN e EA

Prazo de implantação: Máximo de 60 dias após a assinatura do Contrato

Níveis Mínimos de Serviço Exigidos: Contemplar, no mínimo, o prazo de atendimento de chamados de suporte técnico

Suporte e manutenção: Acompanhar a vigência contratual mínima de 24 meses, contemplando esclarecimento de dúvidas, atualizações e correções de bugs

Garantia técnica das licenças: Acompanhar a vigência contratual mínima de 24 meses a partir da assinatura do Termo de Recebimento Definitivo

Garantia contratual: Considerando a necessidade de atendimento de chamados durante a vigência do Contrato, é necessário estipular no Termo de Referência a obrigatoriedade de garantia contratual

Características da solução tecnológica:

- Reduzir a superfície de ataque do endpoint: uso de técnicas que limitem a exposição das vulnerabilidades dos endpoints aumentando a resistência a um ataque bem-sucedido. Como exemplo, citam-se as ameaças de vírus, worms, ransomwares, spywares, adwares, rootkits, trojans, entre outros, bem como de ameaças desconhecidas (ataques de zero-day);

- Proteger o endpoint contra ataques baseados em arquivos e também sem arquivos (fileless malwares):

Antes da execução: normalmente essa proteção de pré-execução utiliza técnicas de análise de arquivos estáticos, tais como: correspondência de assinatura ou aprendizado de máquina;

Durante a execução: em contraste com as técnicas de pré-execução, tais técnicas funcionam apenas enquanto um arquivo binário está em execução e podem detectar e prevenir ataques em endpoints se as técnicas de pré-execução falharem em bloquear um arquivo malicioso ou se o ataque for completamente sem arquivo.

- Realizar a proteção em nível de rede do endpoint: firewalls básicos do sistema são necessários para a proteção de quase todos os endpoints contra ataques em rede exceto para aqueles que necessitam de maior segurança, onde outras camadas de proteção poderão ser empregadas;

- Realizar a detecção e resposta à incidentes em endpoints (EDR – Endpoint Detection and Response): fornecer um método para profissionais técnicos responderem a duas perguntas sobre a segurança dos endpoints: “O que aconteceu aqui?” e “O que está

acontecendo agora?”. Com isso, deverá funcionar como uma espécie de gravador de dados ou “caixa preta” para os terminais nos quais estão instaladas coletando dados de telemetria sobre a atividade dos dispositivos para fins de disponibilização em uma análise posterior, caso seja necessário;

- Gerenciamento e geração de relatórios centralizados: gerência centralizada com acesso a todas as funcionalidades de gestão necessárias com provimento de alertas e relatórios para que as operações antimalware sejam apoiadas diariamente; e
- Provimento de serviços de suporte técnico do fabricante: preocupação essencial para conjuntos de proteção de endpoints seguros, assim como para a operação adequada de qualquer tecnologia de informação crítica para as atividades da Fundacentro.
- A subscrição do licenciamento e garantia da solução terão vigência de 24 (vinte e quatro) meses após a entrega dos softwares onde a Fundacentro terá direito a toda e qualquer nova atualização do software, sejam versões, patches, hotfixes ou assinaturas e subscrições de segurança que fizerem parte da solução durante esse período.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1 Requisitos mínimo de serviços prestados existentes nas licenças antivírus da solução tecnológica:

- Emprego de mecanismos modernos de combate às infecções por malwares em ativos de TI da Fundacentro, com a previsão de uso de varreduras que utilizam aprendizagem de máquina e análise comportamental para detecção de atividades maliciosas, bem como de mecanismos de visibilidade (detecção) e resposta aprimorada à ocorrência de infecções;
- Recebimento de atualizações contínuas pelo fabricante da solução por meio da disponibilização automática de novas vacinas de malwares, revisões dos mecanismos de varredura e de atualizações para novas versões de software/firmware;

6.2 Requisitos de segurança e privacidade

- A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da Fundacentro e aos padrões estabelecidos pela ISO 17799;
- A solução deve ser mantida atualizada para assegurar sua disponibilidade e integridade continuadas;
- Os produtos deverão possuir política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados;
- A Contratada se comprometerá a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços;
- A Contratada deve reportar de imediato à Fundacentro incidentes que envolvam vazamento de dados, fraude ou comprometimento da informação relacionados ao objeto do contrato;
- A Contratada deverá implementar medidas de salvaguarda para os logs, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (logs) de suas próprias atividades;
- A Contratada deverá implementar e manter controles e procedimentos específicos para assegurar o completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da Contratada venham tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da solução objeto do contrato, cumprindo e fazendo cumprir o disposto nos acordos de confidencialidade firmados, partes integrantes deste documento.

6.3 Requisitos sociais, ambientais e culturais

- A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental;
- Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG e no Decreto nº 7.746/2012;
- A CONTRATADA deverá cumprir, no que couber, as exigências do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

6.4 Requisitos de Arquitetura Tecnológica:

6.4.1 Requisitos Gerais.

- 6.4.1.1 Ter características de solução de segurança Antimalware, Endpoint Detection Response - EDR e oferecer proteção contra ameaças avançadas aos endpoints;
- 6.4.1.2 Ser projetada como um produto completo e exclusivo para atender funcionalidade de proteção de endpoints em ambiente corporativo. Não serão aceitos sistemas baseados em hardware ou de software de código aberto (open source) de uso genérico;
- 6.4.1.3 Não serão aceitas soluções de segurança customizadas para a Fundacentro. Serão aceitos somente soluções que fizerem

parte do portfólio de soluções oferecidas pelo fabricante para o mercado corporativo;

6.4.1.4 Todos os componentes da solução deverão ser do mesmo fabricante, estar em linha de produção e não deve haver previsão de descontinuidade, end-of-support ou end-of-life;

6.4.1.5 A solução deverá ser fornecida com licenciamento de uso (subscrição) por 24 (vinte e quatro) meses renováveis pelo mesmo período até o limite previsto na Lei 14.133/2021;

6.4.1.6 A comunicação dos Agentes com o Gerenciador e Servidores deverá ser efetuada por meio de portas seguras e criptografia;

6.4.1.7 Ter mecanismo de whitelist customizável de processos, serviços ou arquivos, com objetivo de não conflitar com outras soluções. A whitelist deverá ter opção de filtro por nome do processo, hash ou extensão do arquivo;

6.4.1.8 Ter mecanismo de blacklist customizável de processos, serviços ou arquivos. A blacklist deverá ter opção de filtro por nome do processo, hash ou extensão do arquivo;

6.4.1.9 É vedado o encaminhamento do artefato que está sendo analisado para o ambiente externo à Fundacentro. As análises deverão ser efetuadas on-premises ou no próprio Agente. Será permitido apenas o envio de metadados para eventuais componentes em nuvem (EDR, proteção para dispositivos móveis, reputação e inteligência);

6.4.1.10 Licenciamento de uso de software de solução de segurança de endpoint (EPP) contemplando módulo/funcionalidade de endpoint detection and response (EDR) para 250 endpoints do parque computacional da Fundacentro, onde:

6.4.1.10.1 No caso de escolha pela manutenção da marca da atual solução da Fundacentro (McAfee), a arquitetura tecnológica será composta de:

6.4.1.10.1.1 Atualização tecnológica de 250 (duzentos e cinquenta) licenças da solução de endpoint protection McAfee atualmente instaladas na Fundacentro (Grant Number: 17759711-NAI), contemplando a atualização para um pacote (suíte) mais recente (250 subscrições de licenças do MVISION Protection Plus EDR – MV6) com garantia de atualizações de versões e assinaturas e suporte técnico durante todo o prazo da contratação, uma vez que a solução existente (CEBYFM-AA e EDRAJE-AT+EDRZDM-AT) requer a hospedagem e provisionamento de infraestrutura interna do órgão e a suíte MV6 ultrapassa essa barreira ao viabilizar a orquestração, provisionamento e gerenciamento da suíte na nuvem, atendendo de maneira plena o especificado no item 4.1 do Anexo I da Instrução Normativa nº 94/2022 SGD/ME.

6.4.2 Requisitos Técnicos dos Agentes:

6.4.2.1 Requisitos Gerais:

6.4.2.1.1 Ser capaz de ser instalado em endpoints que utilizem, no mínimo, os seguintes sistemas operacionais: Windows 8 e versões posteriores, Windows Server 2012 R2 e versões posteriores 32 e 64 bits, Linux Red Hat Enterprise 8.

x, 64bits e CentOS 8.x, 64bits;

6.4.2.1.2 Ser capaz de ser instalado em endpoints Windows por meio de GPO, SCCM (System Center Configuration Manager) ou por outra forma automatizada. A instalação deverá ser feita de forma autônoma e oculta, sem a necessidade de interação com o usuário;

6.4.2.1.3 Permanecer funcional independentemente de conexão com o Gerenciador, ou seja, as análises, monitoramento e ações contra ameaças deverão ser efetuadas de forma independente, sem depender do Gerenciador;

6.4.2.1.4 Possuir funcionalidades para filtrar eventos, bem como, definir quais eventos deverão ser enviados ao Gerenciador;

6.4.2.1.5 Permitir, de forma automatizada, o envio de registros de eventos considerados como incidente para o Gerenciador;

6.4.2.1.6 Ser capaz de acessar o Gerenciador por meio da Internet e da rede corporativa para a coleta de atualizações, configurações e envio de incidentes registrados. Essa configuração deverá ser customizável e aplicável para determinados grupos definidos ou divisões lógicas;

6.4.2.1.7 Ser capaz de enviar para o Gerenciador as informações sobre novas ameaças (zero-day) detectadas de modo que os demais Agentes possam consumir essas informações e aplicar ações de forma imediata (push ou similar);

6.4.2.1.8 Possuir mecanismo de proteção contra desinstalação, alteração e mudanças nos serviços vinculados ao Agente;

6.4.2.1.9 Possuir mecanismo de proteção dos processos do Agente e de alterações indevidas no registro do Agente;

6.4.2.1.10 Possuir mecanismo de proteção com uso de senha para remoção do Agente;

6.4.2.1.11 Possuir sistemática de patches e atualizações que permita a manutenção da qualidade e eficácia do Agente frente a novas ameaças e ataques;

6.4.2.1.12 Verificar a unicidade dos arquivos por meio da verificação de hash, evitando que o mesmo binário seja analisado diversas vezes. No caso de atualização na base de inteligência da solução, deve ser feita nova verificação;

6.4.2.1.13 Permitir a inclusão de arquivos e programas suspeitos em quarentena, impedindo a utilização de recursos do Endpoint;

6.4.2.1.14 Inspeccionar arquivos compactados e bloquear se estiverem infectados;

6.4.2.1.15 Possuir mecanismo para impedir disseminação lateral de malwares ao identificar endpoints infectados.

6.4.2.2 Requisitos de Antimalware:

6.4.2.2.1 Possuir prevenção contra ameaças avançadas fornecendo mecanismos de defesa contra malwares e spywares para endpoints;

6.4.2.2.2 Possuir no mínimo detecção por Assinatura (hash), Heurística, Reputação, Análise Comportamental e Tráfego de Rede;

6.4.2.2.3 Possuir mecanismo para detecção e bloqueio baseados em reputação de arquivos específicos utilizando, no mínimo, hash MD5, SHA-1 ou SHA-256;

6.4.2.2.4 Possuir gerenciamento integrado à console de gerência da solução;

6.4.2.2.5 Permitir a atualização da base local de reputação por meio da Internet com a base do fabricante da solução;

6.4.2.2.6 Possuir mecanismo de proteção a aplicações/serviços/sistemas operacionais vulneráveis. A funcionalidade deverá impedir a exploração de vulnerabilidades;

- 6.4.2.2.7 Possuir configuração customizada de proteção, caso o Agente não consiga se conectar com o Gerenciador;
- 6.4.2.2.8 Possuir mecanismo que impeça a desinstalação do Agente pelo usuário;
- 6.4.2.2.9 Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos;
- 6.4.2.2.10 Possibilitar aplicar regras diferenciadas por grupos de máquinas;
- 6.4.2.2.11 Permitir a atualização incremental da lista de definições de vírus nos Agentes, a partir de um único ponto da rede corporativa. Caso a solução seja capaz de mitigar as ameaças sem a necessidade de atualizações periódicas este item poderá ser desconsiderado;
- 6.4.2.2.12 Fornecer atualizações do produto incluindo patches, correções de bugs e melhorias periodicamente;
- 6.4.2.2.13 Fornecer atualização das definições de vírus ou proteção contra intrusos. Caso a solução seja capaz de mitigar as ameaças sem a necessidade de atualizações periódicas este item poderá ser desconsiderado;
- 6.4.2.2.14 Permitir travar as configurações por senha nos Agentes, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do Agente;
- 6.4.2.2.15 Possuir proteção contra exploração dos tipos conhecidos de ataques overflow;
- 6.4.2.2.16 Possuir proteção em tempo real contra vírus, trojans, worms, spywares, adwares e outros tipos de códigos maliciosos;
- 6.4.2.2.17 Permitir a configuração de ações diferenciadas por níveis de riscos de segurança;
- 6.4.2.2.18 Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: Somente Alertar, Limpar Automaticamente, Apagar Automaticamente;
- 6.4.2.2.19 Permitir verificação das ameaças da maneira manual, agendada e em tempo real detectando ameaças incluindo no nível do kernel do sistema operacional. Caso a solução seja capaz de mitigar as ameaças sem a necessidade de varreduras periódicas este item poderá ser desconsiderado;
- 6.4.2.2.20 Possuir funcionalidades que permitam o isolamento de arquivos contaminados por códigos maliciosos (área de quarentena);
- 6.4.2.2.21 Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados por ZIP, 7Z, RAR, TAR e GZIP tendo como abrangência até o 7º (sétimo) nível de compactação;
- 6.4.2.2.22 Possuir capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina, com opção da sensibilidade da detecção (baixo, médio e alto);
- 6.4.2.2.23 Possuir capacidade de remoção automática total de spywares, adwares e worms, com limpeza de registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;
- 6.4.2.2.24 Possuir capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou IP da origem com opção de bloqueio da comunicação via rede;
- 6.4.2.2.25 Criar uma cópia backup do arquivo suspeito antes de limpá-lo;
- 6.4.2.2.26 Possuir capacidade de executar varreduras em tempo real (real time) contra-ataques direcionado(s) à(s) vulnerabilidade(s) do navegador de internet (browser);
- 6.4.2.2.27 Possuir capacidade de verificar a reputação de arquivos;
- 6.4.2.2.28 Possuir base local de reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já verificados anteriormente;
- 6.4.2.2.29 Possuir capacidade de reconhecer arquivos suspeitos para encaminhamento de seus metadados ao fabricante para que seja investigado e incluído na base de reputação, caso seja malicioso;
- 6.4.2.2.30 Possuir capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais;
- 6.4.2.2.31 Possuir capacidade de realizar monitoramento em tempo real (real time) por heurística ou inteligência artificial correlacionando com a reputação de arquivos;
- 6.4.2.2.32 Possuir capacidade de implementar regras distintas por grupo, categoria ou subcategoria.
- 6.4.2.3 Requisitos referentes à Detecção, Resposta e Proteção de Ameaças Avançadas:
- 6.4.2.3.1 O Agente deve possuir as seguintes funcionalidades de detecção e bloqueio de malwares:
- 6.4.2.3.1.1 Detectar e bloquear ameaças utilizando técnicas comportamentais e estatísticas (heurísticas, comportamental ou preditiva);
- 6.4.2.3.1.2 Detectar e bloquear artefato malicioso com capacidade de realizar mutação no HASH;
- 6.4.2.3.1.3 Detectar e bloquear artefato malicioso que executar processos exclusivamente na memória volátil (sem arquivo no disco físico);
- 6.4.2.3.1.4 Detectar e bloquear artefato malicioso que altera as permissões dos arquivos e processos com poder de usuário privilegiado.
O Agente deve ser capaz de finalizar, deletar, impedir e mover arquivos /processos;
- 6.4.2.3.1.5 Detectar e bloquear artefato malicioso que se utiliza de mecanismos de “Side Load DLL” (um binário executa uma DLL alterada e maliciosa);
- 6.4.2.3.1.6 Detectar e bloquear artefato malicioso na fase pré-infecção (anterior a execução da ameaça);
- 6.4.2.3.1.7 Detectar e bloquear artefato malicioso na fase pós-infecção.
Em máquinas que já se encontram infectadas, a solução, após instalada, deverá ser capaz de detectar e executar as ações necessárias para a desinfecção do endpoint;
- 6.4.2.3.1.8 Detectar e bloquear ataques laterais. A solução deverá proteger um endpoint de uma tentativa de efetuar deploy de um artefato malicioso a partir de um outro endpoint da rede;
- 6.4.2.3.1.9 Detectar e bloquear ameaças executadas em módulos binários (.DLL, .SYS, .EXE, .DMG, .APP), processos e principais scripts conhecidos (.PS1,.PSM1,.JS,.SH,.BAT, .VBS, .SCR, .PY, entre outros) a partir do disco local, proveniente de

compartilhamento de rede, de dispositivos externos ou de download de serviços Internet ou Intranet;

6.4.2.3.1.10 Detectar e bloquear exploits;

6.4.2.3.1.11 Possuir inspeção e proteção de memória, bem como a proteção contra alterações em “live memory”;

6.4.2.3.1.12 Possuir inspeção e proteção contra exploits residentes em memória;

6.4.2.3.1.13 Possuir proteção contra vulnerabilidades e ameaças avançadas (inclusive zero-day);

6.4.2.3.1.14 Detectar e bloquear a ação e propagação de malwares do tipo ransomware e impedir atividades suspeitas envolvendo criptografia de arquivos;

6.4.2.3.1.15 Possuir detecção e prevenção de malwares por comportamento (sem assinaturas) por meio de inspeção de atributos dos arquivos, comportamento e probabilidade do mesmo ser malicioso;

6.4.2.3.1.16 Possuir detecção e prevenção de ataques de vírus, malwares, worms, trojans, spywares, backdoors e qualquer outra forma de código mal-intencionado;

6.4.2.3.1.17 Possuir detecção e prevenção de casos de infecção por navegação na internet em sites com código de exploração de navegadores e seus plugins, ataques de “drive-by download”, na abertura de documentos em formato PDF, Microsoft Office, ataques de “spear phishing” e explorações em outros vetores de ataque como Java e ActiveX;

6.4.2.3.1.18 Detectar e bloquear, no mínimo, as seguintes técnicas de exploração de vulnerabilidade:

6.4.2.3.1.18.1 Heap spray;

6.4.2.3.1.18.2 Falha em aplicação causada por exploit;

6.4.2.3.1.18.3 Ataque ROP;

6.4.2.3.1.18.4 Ataque SEHOP;

6.4.2.3.1.18.5 Drive-by download de programas;

6.4.2.3.1.18.6 Exploração de páginas em branco;

6.4.2.3.1.18.7 Exploração Java;

6.4.2.3.1.18.8 Exploração de macro em arquivos do Microsoft Office;

6.4.2.3.1.18.9 Escalação de privilégios.

6.4.2.3.1.19 Permitir visualização dos eventos contextualizados e ocorridos no passado (base histórica), permitindo investigação dos incidentes até suas causas raízes;

6.4.2.3.1.20 Disponibilizar todo o ciclo de execução de processos suspeitos nos endpoints monitorados (recursos do endpoint, comunicações, edição e criação de arquivos, dentre outros) e permitir a visualização de metadados relevantes à análise dos incidentes, a partir dos campos usados nas buscas;

6.4.2.3.1.21 Demonstrar, na forma de linha do tempo, todos os passos da execução das atividades consideradas suspeitas e efetivas;

6.4.2.3.1.22 Será aceito serviço em nuvem para as funcionalidades de detecção e resposta a incidentes, desde que integrado à console de gerenciamento centralizado.

6.4.2.4 Requisitos de Controle de Dispositivos:

6.4.2.4.1 Controlar o uso de dispositivos por parte dos usuários, como por exemplo: mídias removíveis, unidades USB, dispositivos bluetooth, DVDs, e CDs regraváveis;

6.4.2.4.2 Permitir a configuração dos dispositivos nos modos: bloqueio ou somente leitura;

6.4.2.4.3 Classificar os dispositivos removíveis em 2 categorias: gerenciado e não-gerenciado;

6.4.2.4.4 Ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:

6.4.2.4.4.1 Classe do Dispositivo (Device Class);

6.4.2.4.4.2 ID do fabricante (Vendor ID);

6.4.2.4.4.3 ID do produto (Product ID).

6.4.2.4.5 Ser capaz de identificar Dispositivos Removíveis através das seguintes informações:

6.4.2.4.5.1.1 Tipo de BUS;

6.4.2.4.5.1.2 Se o sistema de arquivo é passível de escrita;

6.4.2.4.5.1.3 Se o sistema de arquivo é somente leitura.

6.4.2.4.6 Ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (exemplo: quando conectado à rede do órgão bloqueia/libera o uso de pen-drive).

6.4.2.5 Monitoração, registros e logs:

6.4.2.5.1 Monitorar e manter registro de operações suspeitas (acesso, cópia, modificação, duplicação e exclusão) com arquivos no disco local, dispositivos USB, dispositivos móveis conectados, mídias removíveis, compartilhamento em rede ou em nuvem e acesso a drivers de rede;

6.4.2.5.2 Monitorar e manter registro de atividades suspeitas e capturar informações críticas referentes a essas atividades para análise;

6.4.2.5.3 Registrar tentativas e impedir limpeza ou manipulação dos logs do sistema operacional;

6.4.2.5.4 Monitorar, analisar e bloquear tentativas de bloqueio de coleta de dados pela solução;

6.4.2.5.5 Monitorar, analisar e bloquear alterações nas chaves de registro e em arquivos de configuração do sistema operacional realizadas por malware;

6.4.2.5.6 Detectar, monitorar, bloquear e manter registro de artefato malicioso que se auto provisionar no Scheduled Tasks, Autoruns (registro, logon, drive USB, dentre outros), Services e Inicializar na barra de tarefas do Windows, indicando onde o processo iniciou.

6.4.2.6 Reputação e Inteligência:

- 6.4.2.6.1 A solução deve possuir capacidade de criar uma reputação local ou utilizar a existente em nuvem do fabricante através da catalogação de todos os executáveis existentes no ambiente;
- 6.4.2.6.2 O módulo de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos;
- 6.4.2.6.3 Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;
- 6.4.2.6.4 A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles: Reputação local e Reputação do Centro de Inteligência;
- 6.4.2.6.5 Ao catalogar um arquivo, a solução deverá apresentar, no mínimo as seguintes informações:
- 6.4.2.6.5.1 Nome do arquivo;
- 6.4.2.6.5.2 Caminho do arquivo;
- 6.4.2.6.5.3 Hash sha-1 e sha-256;
- 6.4.2.6.6 Após análise pela solução o administrador deverá ter a possibilidade de:
- 6.4.2.6.6.1 Rastrear em quais endpoints o arquivo foi executado;
- 6.4.2.6.6.2 Identificar o arquivo como confiável, desconhecido ou malicioso.
- 6.4.2.6.7 Para minimizar o impacto, a solução deverá ter a capacidade de ser ativada no modo de observação nos endpoints protegidos;
- 6.4.2.6.8 Bloquear a execução de arquivos nunca vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem;
- 6.4.2.6.9 A solução deverá possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;
- 6.4.2.6.10 A solução deverá ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por vertical de negócio;
- 6.4.2.6.11 A solução deve deverá ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por país, incluindo o Brasil;
- 6.4.2.6.12 A solução deverá ser capaz de proporcionar a busca em campanhas globais por ameaças baseadas em nome e/ou IOCs;
- 6.4.2.6.13 A solução deverá ser capaz de indicar quantos e quais dispositivos dentro da organização estão vulneráveis a uma determinada campanha;
- 6.4.2.6.14 A solução deverá ser capaz de mostrar o nível de postura de segurança da organização, em relação as campanhas de ameaças globais identificadas na base de inteligência do fabricante;
- 6.4.2.6.15 A solução deverá ser capaz de propor procedimentos de mitigação dos riscos de segurança nos endpoints referentes a campanhas de ameaças específicas;
- 6.4.2.6.16 Cada campanha identificada pela solução deverá possuir as seguintes informações:
- 6.4.2.6.16.1 Descrição;
- 6.4.2.6.16.2 IOCs;
- 6.4.2.6.16.3 Endpoints afetados e impactos;
- 6.4.2.6.16.4 Comportamento da ameaça.
- 6.4.2.6.17 A solução deverá ser capaz de identificar em cada campanha de ameaça as técnicas utilizadas, relacionadas e mapeadas ao MITRE Framework;
- 6.4.2.6.18 As funcionalidades devem ser gerenciadas ou estar integradas a console de gerenciamento da solução de proteção de endpoints e servidores;
- 6.4.2.6.19 Será aceito serviço em nuvem para as funcionalidades de detecção e resposta a incidentes, desde que integrado à console de gerenciamento centralizado.
- 6.4.2.7 Requisitos de proteção para dispositivos móveis:
- 6.4.2.7.1 A solução de proteção para dispositivos móveis deverá proteger contra as ameaças em dispositivos móveis Android e IOS incluindo malwares, ameaças de rede, identificação de vulnerabilidades e defesa física dos dispositivos;
- 6.4.2.7.2 Será aceito serviço em nuvem para as funcionalidades de proteção para dispositivos móveis desde que integrado à console de gerenciamento centralizado;
- 6.4.2.7.3 A solução deverá possuir console WEB para administração da solução;
- 6.4.2.7.4 Possuir dashboard com os principais indicadores da solução, como distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;
- 6.4.2.7.5 Apresentar nos dashboards uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede, vulnerabilidades e malwares encontrados;
- 6.4.2.7.6 Deverá possuir uma apresentação gráfica referente as informações dos dispositivos registrados na solução;
- 6.4.2.7.7 Associar o nome do usuário ao nome do dispositivo, o modelo e a versão do sistema operacional, em console gráfica;
- 6.4.2.7.8 A console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o mesmo e o dispositivo que gerou o incidente;
- 6.4.2.7.9 A solução deverá apresentar um relatório de ações recomendadas, para que com tais dados os administradores da solução possam criar ações para melhorar a segurança dos dispositivos móveis da empresa;
- 6.4.2.7.10 A solução deverá ser categorizada como uma solução de MTD (Mobile Threat Defense);
- 6.4.2.7.11 O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para IOS e Google Play para Android;
- 6.4.2.7.12 Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alertas seja visível para o usuário final, através de modo não interativo;

6.4.2.7.13 Deverá possuir as seguintes características mínimas de proteção:

6.4.2.7.13.1 Proteção em tempo real contra malwares conhecidos e desconhecidos;

6.4.2.7.13.2 Defesa física;

6.4.2.7.13.3 Identificação de upgrades do sistema operacional;

6.4.2.7.13.4 Identificação de dispositivo com root;

6.4.2.7.13.5 Identificação de configurações de segurança, como tela de bloqueio não habilitada;

6.4.2.7.13.6 Deverá ser possível instalar a solução através de integração com solução de MDM/EMM ou através da própria console, utilizando e-mail;

6.4.2.7.13.7 Deverá possuir integração com solução de SIEM de mercado;

6.4.2.7.13.8 A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de e-mail.

6.4.3 Requisitos Técnicos do Sistema de Gerenciamento Centralizado e Servidores (on-premises):

6.4.3.1 Requisitos Gerais:

6.4.3.1.1 Ser plenamente compatível com o software dos Agentes;

6.4.3.1.2 Ser capaz de monitorar e gerenciar todo o quantitativo de endpoints da solução simultaneamente;

6.4.3.1.3 As comunicações dos Agentes deverão ser feitas exclusivamente com o Gerenciador da solução. O canal de comunicação poderá ser tanto via Internet como internamente, cada qual com endereços distintos;

6.4.3.1.4 Os dados trafegados devem ser para coleta de atualizações, configurações e envio de incidentes registrados. Essa configuração deve ser customizável e aplicável em determinados grupos definidos ou divisão lógica;

6.4.3.1.5 Para a atualização da base de assinaturas e inteligência poderá ser permitido o acesso à Internet;

6.4.3.1.6 É vedado o encaminhamento do artefato que está sendo analisado para o ambiente externo à Fundacentro. As análises devem ser feitas em ambiente on-premises ou no próprio Agente;

6.4.3.1.7 Deverá identificar e atualizar os endpoints com Agentes desatualizados;

6.4.3.1.8 Verificar a unicidade dos arquivos por meio da verificação de hash, evitando que o mesmo binário seja analisado diversas vezes. No caso de atualização na base da solução deverá ser feita nova verificação;

6.4.3.1.9 Deverá possuir funcionalidade de identificar ameaças através de correlação de eventos e comportamentos dos endpoints gerenciados;

6.4.3.1.10 A gerência deverá permitir análise e tomada de ações contra ameaças independentemente das ações tomadas de forma automática pelo Agente;

6.4.3.1.11 Deverá possuir funcionalidade de resposta automatizada e configurável aos incidentes de segurança. As funcionalidades referentes a resposta a incidentes de segurança e contenção de ameaças devem ser passíveis de automatização;

6.4.3.1.12 Deverá fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o Agente instalado, com opção de instalação remota.

6.4.3.2 Requisitos operacionais:

6.4.3.2.1 Possibilitar a listagem dos computadores infectados, em um dado momento, usando como parâmetros as informações enviadas pelos Agentes e bases de inteligência acerca de malwares fornecidos pela solução;

6.4.3.2.2 Permitir que cada endpoint monitorado seja inserido em grupos ou perfis de configuração para:

6.4.3.2.2.1 Enviar informações específicas;

6.4.3.2.2.2 Receber configurações de conexão com gerenciador específicas;

6.4.3.2.2.3 Definir a quantidade de disco a ser utilizada para armazenamento local de eventos;

6.4.3.2.2.4 Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

6.4.3.2.2.5 Permitir ao administrador criar diversos grupos de políticas de segurança para diferentes divisões lógicas;

6.4.3.2.2.6 As pesquisas nos eventos reportados a gerência pelos endpoints devem permitir o uso de operadores lógicos em conjunto com hashes ou outras formas.

6.4.3.2.3 Ter a capacidade de identificar as seguintes informações, sem a necessidade de reprocessamento da busca nos dados armazenados localmente nos sistemas operacionais monitorados:

6.4.3.2.3.1 Como um ataque começou, por meio da visualização do encadeamento de processos executados até a causa raiz de um ataque;

6.4.3.2.3.2 O que o malware fez, por meio do detalhamento dos processos e comandos executados, inclusive com parâmetros utilizados e alterações em sistema de arquivos.

6.4.3.2.4 Possuir a informação de quantos e quais sistemas foram impactados, por meio da pesquisa dos seguintes metadados específicos:

6.4.3.2.4.1 Arquivos (nomes e hashes criptográficos);

6.4.3.2.4.2 Ameaça cadastrada na base de dados da solução;

6.4.3.2.4.3 Chaves de Registro;

6.4.3.2.4.4 Nomes de processos ou arquivos executáveis;

6.4.3.2.4.5 Conexões de rede (endereços IP e domínios);

6.4.3.2.4.6 Quais arquivos foram criados, modificados, acessados e removidos, por meio da visualização de alterações feitas no sistema de arquivos;

6.4.3.2.4.7 As comunicações efetuadas pelos processos analisados, por meio da listagem de conexões TCP/IP que foram efetuadas pelos sistemas;

6.4.3.2.4.8 Quais arquivos foram baixados e por quais processos.

6.4.3.2.5 Permitir a qualquer momento, a listagem e pesquisa de valores históricos anteriores de metadados dos artefatos monitorados;

6.4.3.2.6 Permitir visualização dos parâmetros passados para os arquivos executáveis, quando houver a execução de binários em modo console (prompt de comando);

6.4.3.2.7 Permitir o acesso, por meio do histórico armazenado no próprio Gerenciador às alterações feitas nos sistemas de arquivo, leituras e alterações de registro, leituras, criações, remoções e modificações de arquivos, comunicações TCP/IP e todos os processos executados no sistema operacional de todos os computadores monitorados;

6.4.3.2.8 Possibilitar a identificação da origem de um ataque, mesmo que não exista um executável malicioso envolvido, como nos casos de infecção por navegação na internet em sites com código de exploração de navegadores e seus plugins (ataques de “drive-by download”), na abertura de documentos em formato PDF, Microsoft Office (ataques de “spear phishing”) e explorações em outros vetores de ataque como Java e ActiveX;

6.4.3.2.9 Permitir bloquear as configurações dos Agentes por senha, definindo permissões para que somente o administrador da solução possa alterar as configurações, desinstalar ou parar o serviço do Agente;

6.4.3.2.10 Permitir agendamento de instalação, atualização e desinstalação do software dos Agentes dos Endpoints gerenciados via políticas no Gerenciador de forma silenciosa, ou seja, sem interação com usuário, sendo que essas poderão ser aplicadas por grupos de Endpoints. Caso a solução não tenha um gerenciador de instalação de seus Agentes e utilize outras formas de deploy (SCCM, GPO) esse item não será exigido;

6.4.3.2.11 Permitir a ativação e desativação do software do Agente em determinados Endpoints;

6.4.3.2.12 Aplicar regras diferenciadas por grupos de usuários, de máquinas, de domínios para todas as funcionalidades da solução;

6.4.3.2.13 Possuir configuração de fuso horário e conexão com servidor NTP;

6.4.3.2.14 Exportar configurações do centralizador que facilite o backup da configuração e a cópia entre máquinas;

6.4.3.2.15 Possuir alimentação automática de fontes externas de inteligência para detecção e combate a novas ameaças e ataques (threat intelligence);

6.4.3.2.16 O Gerenciador deverá ter opção de configuração dos dados que os endpoints ou grupos de endpoints deverão enviar para ele.

6.4.3.3 Administração e autenticação de usuários:

6.4.3.3.1 O Gerenciador deverá ser remotamente administrável por meio de interface gráfica (GUI), utilizando canais autenticados e criptografados. Serão aceitas interfaces gráficas em formato web ou em forma de aplicativo cliente, desde que este último seja compatível com Microsoft Windows 10 (versões 32 bits e 64 bits) e superiores;

6.4.3.3.2 Todos os acessos administrativos devem ser autenticados, criptografados e com registros mantidos;

6.4.3.3.3 Autenticar usuários administrativos por meio do Active Directory;

6.4.3.3.4 Deve ser capaz de segregar perfis de acesso, permitindo diferentes níveis de acesso à console de gerenciamento, onde cada perfil possa ter permissões específicas associadas à sua função;

6.4.3.3.5 Permitir que os perfis de acesso sejam relacionados a grupo de usuários para possibilitar conceder ou revogar acessos conforme a inclusão ou exclusão de usuários desses grupos;

6.4.3.3.6 Permitir múltiplos acessos simultâneos à console de gerenciamento, seja para análise de informações ou aplicação de configurações.

6.4.3.4 Gerenciamento de Licenças:

6.4.3.4.1 Possuir gerenciamento das licenças de maneira centralizada, incluindo a adição e remoção de licenças;

6.4.3.4.2 A console deve ter possibilidade de filtrar endpoints atrelados à licença que não se comuniquem com o gerenciamento a determinado período de tempo. O filtro deverá permitir selecionar todos e deletar da base de endpoints /licenciamento. Essa funcionalidade deverá ser feita de forma independente do fornecedor pelo próprio administrador da solução na Fundacentro.

6.4.3.5 Conexão offsite:

6.4.3.5.1 Ser capaz de implementar servidor exclusivo para função de comunicação com os Agentes vindos de conexões “offsite” (conexão VPN, nuvem e Internet);

6.4.3.5.2 As informações trocadas entre o Agente e o servidor exclusivo citado no item anterior devem ser passíveis de configuração diferenciada a ser definida por meio de políticas;

6.4.3.5.3 O servidor a ser instalado em DMZ ou similar deverá ser exclusivo para essa função, tendo comunicação interna com o Gerenciador, possibilitando administração de um único ponto.

6.4.3.6 Appliance Virtual:

6.4.3.6.1 O servidor do Gerenciador deve ser compatível com o VMware VSphere Hypervisor (ESXi) 6.5 ou superior (não haverá necessidade do fornecimento de licenças da VMware junto com a solução);

6.4.3.6.2 a Fundacentro dispõe das seguintes licenças de sistemas operacionais (x86 64 bits) para a instalação da solução: Microsoft Windows Server 2012 R2 ou superior;

6.4.3.6.3 Para a instalação do Gerenciador da solução, a Fundacentro dispõe de servidores instalados com os seguintes sistemas de gerenciamento de banco de dados (SGBD) licenciado: Microsoft SQL Server 2012 ou superior;

6.4.3.6.4 Não serão aceitas soluções que utilizem servidores de banco de dados com SGBD comerciais diferentes daqueles já instalados na Fundacentro;

6.4.3.6.5 Serão admitidas soluções que possuem banco de dados proprietários, desde que estejam instalados em appliance virtual.

6.4.3.7 Dashboard:

- 6.4.3.7.1 Demonstrar ameaças de alta severidade para o ambiente;
- 6.4.3.7.2 Demonstrar os principais meios e tipos de ataques;
- 6.4.3.7.3 Demonstrar máquinas com a lista de definições de vírus desatualizada;
- 6.4.3.7.4 Demonstrar qual a versão do software de proteção e EDR instalado em cada máquina;
- 6.4.3.7.5 Demonstrar as máquinas que mais sofreram infecções em um determinado período;
- 6.4.3.7.6 Demonstrar os usuários que mais sofreram infecções em um determinado período.
- 6.4.3.8 Log:
 - 6.4.3.8.1 Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento, ameaças detectadas e bloqueadas e ações executadas;
 - 6.4.3.8.2 O Gerenciador deve ter capacidade de armazenamento de logs de funcionamento da solução por um período mínimo 6 (seis) meses e que devem ser acessados através de filtros;
 - 6.4.3.8.3 Possibilitar o envio dos logs a outros sistemas de armazenamento, seguindo padrões syslog;
 - 6.4.3.8.4 Os logs registrados através do agente devem ser acessíveis por SSH, SCP ou HTTPS, sempre com controle de acesso.
- 6.4.3.9 Relatórios:
 - 6.4.3.9.1 Gerar relatórios a partir dos dados monitorados;
 - 6.4.3.9.2 Gerar relatórios automatizados em períodos, por hora, por dia, por semana, por mês e por ano, configuráveis pelo administrador;
 - 6.4.3.9.3 Gerar relatórios em diversos formatos como: texto ou CSV e PDF;
 - 6.4.3.9.4 Relatórios devem conter, no mínimo:
 - 6.4.3.9.4.1 Informações por domínio;
 - 6.4.3.9.4.2 Informações do grupo de endpoints;
 - 6.4.3.9.4.3 Informações por usuário;
 - 6.4.3.9.4.4 Informações da estação ou grupo de estações;
 - 6.4.3.9.4.5 Informações de ataques identificados;
 - 6.4.3.9.4.6 Informações de ataques bloqueados;
 - 6.4.3.9.4.7 Informações de arquivos (modificados, excluídos, copiados, acessados e duplicados).
- 6.4.3.10 Alertas:
 - 6.4.3.10.1 Ter um sistema de alertas personalizável pelo administrador que poderá configurar o motivo do disparo do alerta, como ataques identificados, infecções detectadas, malwares;
 - 6.4.3.10.2 Ser capaz de enviar alertas e dados nativamente com opção de selecionar quais alertas serão enviados, via protocolo syslog, e de forma automatizada;
 - 6.4.3.10.3 A console do Gerenciador deverá ter a funcionalidade de apresentar automaticamente alertas pré-configurados em tempo real;
 - 6.4.3.10.4 Prover triagem dos alertas, auxiliando na priorização, investigação e evidenciar o estado dos alertas gerados pela ferramenta;
 - 6.4.3.10.5 Ser capaz de emitir alertas baseados na execução, em um ou mais computadores, de hashes ou nome do processo inclusos na blacklist.
- 6.4.3.11 Consultas:
 - 6.4.3.11.1 Ter funcionalidade de consulta customizável com as seguintes informações:
 - 6.4.3.11.1.1 Data Início e Fim;
 - 6.4.3.11.1.2 Hash;
 - 6.4.3.11.1.3 Nome do processo;
 - 6.4.3.11.1.4 Nome da Máquina;
 - 6.4.3.11.1.5 IP;
 - 6.4.3.11.1.6 Tipo de ataque/detecção;
 - 6.4.3.11.1.7 Possibilitar exibição em gráfico ou tabelas;
 - 6.4.3.11.1.8 Permitir o uso de operadores lógicos, hashes, termos ou frases.
- 6.5 Requisitos de projeto:
 - 6.5.1 A instalação terá um prazo máximo de 30 (trinta) dias;
 - 6.5.2 A CONTRATADA procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos do Serviço de Tecnologia - Infraestrutura e Operações e, sendo posteriormente aferido e testado o seu perfeito funcionamento;
 - 6.5.3 Compreende-se, nesta etapa, a instalação de equipamentos, sistemas, softwares e aplicativos dos PRODUTOS fornecidos pela CONTRATADA, bem como a migração das configurações existentes na Fundacentro para os novos PRODUTOS;
 - 6.5.4 A CONTRATADA deve elaborar um documento de planejamento de instalação e implantação para aprovação da Fundacentro antes da execução da instalação;
 - 6.5.5 A etapa de implantação e migração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE;
 - 6.5.6 Durante a implantação e migração, a CONTRATADA deverá realizar, entre outras atividades:
 - 6.5.6.1 Atualização inicial de firmware, software e/ou patches, caso necessário, para que a versão de instalação corresponda com

a última versão válida disponibilizada pelo fabricante;

6.5.6.2 Configurações básicas;

6.5.6.3 Acompanhamento de migrações de regras e políticas;

6.5.6.4 Elaboração e execução de scripts;

6.5.6.5 Análise de performance;

6.5.6.6 Resolução de problemas.

6.5.7 Durante a etapa de implantação e migração, os PRODUTOS fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção;

6.5.8 Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de implantação e migração definidos pela CONTRATANTE;

6.5.9 Caberá a CONTRATANTE o acompanhamento da migração, fornecimento de informações sobre os aplicativos e ferramentas existentes no ambiente, bem como a definição e concessão de janelas de intervenção;

6.5.10 As atividades de implantação e migração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana;

6.5.11 A CONTRATADA deve garantir que a migração não irá alterar as versões ou o funcionamento dos serviços instalados na unidade objeto da migração, sem a prévia autorização da CONTRATANTE;

6.5.12 A CONTRATADA deverá, com a supervisão da CONTRATANTE, planejar e realizar a instalação dos softwares e a configuração dos novos equipamentos com total interoperabilidade operacional com ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

6.6 Requisitos de implantação:

6.6.1 Para implantação devem ser consideradas as seguintes premissas:

6.6.1.1 Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como softwares, recursos humanos necessários à instalação dos PRODUTOS;

6.6.1.2 A CONTRATADA realizará transferência de conexão dos equipamentos conectados à rede LAN existente na CONTRATANTE para os PRODUTOS fornecidos;

6.6.1.3 A CONTRATADA realizará adequação/configuração dos PRODUTOS fornecidos ao longo da etapa de migração e realização de novas configurações;

6.6.1.4 A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação/migração e ao pleno funcionamento do ambiente de produção.

6.7 Requisitos de Garantia

6.7.1 A CONTRATADA deverá oferecer garantia por 24 (vinte e quatro) meses para as licenças da solução contratada, estando disponível para acionamento de garantia 8 horas por dia, 5 dias por semana (8x5);

6.7.2 A subscrição deve ser fornecida com licenciamento e garantia de atualização de softwares/firmwares para todo o período da contratação.

6.8 Requisitos de experiência profissional

6.8.1 A CONTRATADA deverá executar os serviços de suporte técnico especializado por meio de profissionais certificados na administração e suporte pelo próprio fabricante da solução.

6.9 Requisitos de formação da equipe

6.9.1 O projeto, implementação e implantação da solução deverá ser realizada pela CONTRATADA por meio de profissionais certificados pelo próprio fabricante na instalação e administração da solução.

6.10 Requisitos de Metodologia de Trabalho

6.10.1 Realização de Reunião Inicial previamente à entrega da solução e execução dos serviços de instalação;

6.10.2 Reuniões entre a Fundacentro e CONTRATADA para discussão de assuntos referentes às instalações em execução e acompanhamento do cronograma;

6.10.3 Execução das etapas demandadas e posterior aceite/rejeição pela equipe de fiscalização da contratação e o Gestor do Contrato;

6.10.4 Profissionais qualificados da CONTRATADA deverão realizar o repasse de conhecimento para operacionalização e configuração da solução fornecida, direcionada à equipe técnica da Fundacentro;

6.10.5 Prestar o serviço objeto desta contratação nos horários estipulados pelo órgão, ou em outro horário, mediante negociação com a Fundacentro, inclusive feriados e nos finais de semana;

6.10.6 Fornecer número telefônico para contato e registro de ocorrências sobre o acompanhamento do serviço contratado;

6.10.7 Emitir e entregar os certificados de garantia dos softwares e serviços.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Atualização de 250 (duzentos e cinquenta) licenças da solução de antivírus McAfee atualmente instaladas na Fundacentro, contemplando a atualização da solução para 250 subscrições de licenças do MVISION Protection Plus EDR – MV6 com garantia de atualizações de versões e assinaturas e suporte técnico do fabricante por 24 (vinte e quatro) meses, prorrogáveis por iguais e sucessivos períodos, até o limite estabelecido na Lei 14.133/2021.

7.2 O número de licenças leva em consideração levantamento realizado pelo Serviço de Tecnologia - Infraestrutura e Operações (STIO) em março/2024, considerando-se o número de estações de trabalho, notebooks e servidores de aplicação físicos e virtuais em uso na Instituição.

8. Levantamento de soluções

ID	Descrição da solução (ou cenário)
1	Não contratar/utilizar nenhuma solução de antivírus
2	Utilizar solução gratuita para antivírus
3	Contratar nova solução de antivírus
4	Atualizar a solução de antivírus atual

9. Análise comparativa de soluções

9.1 SOLUÇÃO 1 - NÃO CONTRATAR/UTILIZAR NENHUMA SOLUÇÃO DE ANTIVÍRUS

9.1.1 Esta solução consiste em não realizar novo procedimento licitatório ou não utilizar nenhuma solução software-livre ou gratuita para a proteção de endpoints da Fundacentro contra execução de códigos maliciosos, entre outros tipos de ameaças bloqueadas por tal solução;

9.1.2 Nessa solução, a atual solução de proteção de endpoints da fabricante McAfee/Trellix, a partir de 31/10/2024 não receberá mais atualizações de assinaturas de vírus e de versões, que contém melhorias nos mecanismos de detecção de malwares resultantes do aprimoramento ou desenvolvimento de novas funcionalidades tendo em vista o cenário de ameaças em constante evolução;

9.1.3 Com isso, a ferramenta aos poucos perderá a eficácia de detecção e bloqueio de ameaças de malwares, elevando-se o número de falso-negativos e aumentando-se os riscos de ataques cibernéticos bem-sucedidos;

9.1.4 Além disso, a solução não receberá mais o suporte técnico do fabricante em caso de bug;

9.1.5 Apesar dessa solução aparentemente não gerar custos para a Fundacentro, pois não há gastos com novos investimentos no curto prazo, no médio e longo prazo serão gerados dispêndios relativos à abertura de chamados com as Contratadas para o serviço de Service Desk e Operação de Infraestrutura/Segurança da Informação e, no limite, em custos envolvidos na recuperação do ambiente computacional em decorrência de um ataque cibernético destrutivo iniciado por meio da execução de ameaças virtuais em ativos computacionais que não possuem uma solução de segurança de endpoints instalada ou, caso instalada, sem manutenção e sem atualizações continuamente realizadas pelo fabricante.

9.2 SOLUÇÃO 2 - UTILIZAR SOLUÇÃO GRATUITA DE ANTIVÍRUS

9.2.1 Essa solução envolve a instalação e configuração de "software-livre" ou uso de soluções de antivírus gratuitas, tais como: ClamWin, ClamAV, Avast, AVG, Avira, Bit Defender, entre outros;

9.2.2 Sabe-se que soluções "software-livre" de antivírus não empregam o mesmo volume de recursos em pesquisa e desenvolvimento de seus produtos quando comparadas às soluções comerciais, tornando-as menos eficazes e robustas para uso em ambientes computacionais corporativos tal qual o da Fundacentro. Já as soluções comerciais gratuitas não são acompanhadas de todas as funcionalidades de proteção e administração que o ambiente corporativo da Fundacentro necessita, como por exemplo, o gerenciamento centralizado de elevado número de endpoints conectados em rede de forma que os padrões e políticas de segurança corporativas sejam uniformemente aplicados;

9.2.3 Além disso, a maioria das soluções de antivírus na modalidade "software-livre" ou gratuitas não fornecem suporte técnico e garantia do fabricante, em detrimento das soluções comerciais, que fornecem suporte técnico do fabricante para fins de garantia

da qualidade e manutenção adequada do seu produto;

9.2.4 O emprego de ferramenta antivírus baseada em "software-livre" em substituição às ferramentas comerciais também exigirá que ela seja mantida diariamente na Fundacentro por especialistas na instalação, configuração e administração de tais soluções, que são considerados escassos no mercado;

9.2.5 Com isso, ao empregar soluções de antivírus baseadas em "software-livre" ou gratuitas, a Fundacentro trocará o investimento por custos operacionais resultantes da elevação da carga administrativa no serviço de antivírus (serviço de TI), bem como poderá incorrer em outros custos diretos e indiretos relacionados aos períodos de indisponibilidade de serviço de TI resultante de mau funcionamento da solução instalada em endpoint e agravado pela inexistência de garantia do fabricante. Somando-se a isso, há elevação do risco de ocorrência bem-sucedida de ataque cibernético destrutivo resultante da execução de códigos maliciosos e/ou outras ameaças virtuais avançadas nos endpoints quando comparados com as menores probabilidades de concretização providas em soluções comercialmente adquiridas.

9.3 SOLUÇÃO 3 - CONTRATAÇÃO DE NOVA SOLUÇÃO DE ANTIVÍRUS CORPORATIVO.

9.3.1 Esta solução constitui-se em realizar:

9.3.1.1 Aquisição de nova solução de antivírus, de fabricante diverso da atual, compreendendo 250 (duzentas e cinquenta) licenças de uso de antivírus para endpoints (estações de trabalho, notebooks, servidores de rede físicos e virtuais) contemplando licenciamento, garantia de atualizações de versões e assinaturas conforme volumetria necessária para o atendimento da atual necessidade Fundacentro, conforme detalhado a seguir;

9.3.1.2 Contratação de serviço de instalação da nova solução, compreendendo a desinstalação dos agentes e demais módulos da solução anterior, instalação dos componentes da nova solução e customização conforme as atuais políticas de antivírus implantadas em todos os ativos do parque computacional, sobretudo configuração das exceções de varredura nos endpoints que hospedam as aplicações da Fundacentro;

9.3.1.3 Contratação de serviço de treinamento para a equipe técnica da Fundacentro;

9.3.2 Tal aquisição poderá ser realizada por meio do licenciamento perpétuo ou subscrição de licenças de solução de "endpoint protection platform" (EPP) com garantia de atualizações de versões e assinaturas e suporte técnico do fabricante durante todo o período da contratação, normalmente definido entre 12 (doze) e 60 (sessenta) meses.

9.3.3 Para aumento da proteção e agregação de maior valor à solução há módulos adicionais à solução de EPP fornecidos pelos fabricantes e destinados a prover funcionalidades de proteção avançada, detecção e resposta tais como o EDR (Endpoint Detection and Response) e anti-APT (Advanced Protection Threat).

9.3.4 Ressalta-se que alguns fabricantes podem fornecer a gerência da solução e outros componentes na forma de appliance virtual que se destina à instalação direta em máquinas virtuais do ambiente da Contratante ou como serviço totalmente em ambiente de nuvem computacional.

9.3.5 O valor unitário da solução é normalmente precificado por endpoint, podendo ser o número de usuários/estações de trabalho, servidores físicos/virtuais e computadores/dispositivos portáteis (notebooks). O valor global, resultante do produto do valor unitário pelo quantitativo acima deverá ainda se somar aos valores dos serviços de instalação, treinamento e suporte técnico especializado durante o período da contratação.

9.4 SOLUÇÃO 4 - ATUALIZAR TECNOLOGICAMENTE A SOLUÇÃO DE ANTIVÍRUS ATUAL DA FUNDACENTRO.

9.4.1 Esta solução consiste na realização de:

9.4.1.1 Atualização de 250 (duzentas e cinquenta) licenças da solução de antivírus McAfee atualmente instaladas na Fundacentro, contemplando atualização da solução para um novo pacote (suíte) mais recente (250 licenças CEB+EDR para 250 licenças Trellix /MVISION Protection Plus EDR – MV6) e garantia de atualizações de versões durante a vigência do contrato, módulos de segurança mais modernos e adequados à atual necessidade de segurança de ambientes corporativos;

9.4.2 Busca-se por meio dessa estratégia atualizar os componentes da solução McAfee atual agregando proteções e novas funcionalidades mais adequadas ao grau de ameaças cibernéticas atuais e não disponíveis na suíte atual da Fundacentro como, por exemplo, análise de reputação/inteligência aprimoradas.

9.4.3 Para fins de observância de requisitos da Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, que estabelece os princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem a serem seguidos pelos órgãos e demais entidades públicas da Administração Pública Federal, o gerenciamento da solução continuará instalado em ambiente local da Fundacentro enquanto que o módulo Endpoint Detection and Response (EDR) poderá ser hospedado em nuvem, onde apenas metadados são enviados. Compõem a solução antivírus, os seguintes módulos:

9.4.3.1 ePO on-premise/cloud;

9.4.3.2 McAfee/Trellix e-PO;

9.4.3.3 McAfee/Trellix Endpoint;

9.4.3.4 ENS 10.x (Win/Mac/Linux);

9.4.3.5 Adaptive Threat Protection (DAC + Real Protect);

9.4.3.6 Data Exchange Layer (DXL);

9.4.3.7 Threat Intelligence Exchange Server (TIE);

9.4.3.8 Device Control;

9.4.3.9 Application Control (desktop);

9.4.3.10 Endpoint Detection and Response (EDR);

9.4.3.11 McAfee/Trellix Insights.

9.4.4 Por fim, o prazo de vigência da eventual contratação das licenças da solução McAfee definido em 24 (vinte e quatro) meses, prorrogáveis até o limite previsto na Lei 14.133/2021 para contratações de serviços continuados, uma vez que a descontinuidade das atualizações diárias de assinaturas e versões da solução podem causar prejuízos à proteção cibernética do parque computacional pois, sem receber atualizações automáticas e periódicas, a solução torna-se obsoleta frente à evolução diária dos ataques cibernéticos a qual ela visa proteger.

9.4 ANÁLISE COMPARATIVA DAS SOLUÇÕES

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1			X
	2	X		
	3	X		
	4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	1			X
	2		X	
	3		X	
	4		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	1			X
	2	X		
	3		X	
	4		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo eMag, ePWG?	1		X	
	2		X	
	3	X		
	4	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1		X	
	2		X	
	3	X		
	4	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1		X	
	2		X	
	3	X		
	4	X		

10. Registro de soluções consideradas inviáveis

10.1 As soluções identificadas como inviáveis são as soluções 1 e 2. Seguem as justificativas:

10.1.1 Solução 1 – Não utilizar nenhuma solução de antivírus – é inviável tendo em vista os elevados riscos cibernéticos associados a esta alternativa uma vez que deixará o ambiente computacional da Fundacentro desprotegido contra ataques cibernéticos. Além disso, o custo advindo em decorrência de um ataque cibernético destrutivo à Fundacentro e os impactos operacionais e os relativos ao descumprimento de obrigações legais resultante da paralização de atividades decorrente da indisponibilidade do ambiente computacional da Fundacentro torna essa opção não aceitável;

10.1.2 Solução 2 - Utilizar solução "software-livre" ou gratuita de antivírus – é inviável tendo em vista os elevados riscos cibernéticos também associados a esta alternativa. A inexistência de garantia e suporte do fabricante de soluções software-livre /gratuitas de segurança se traduz em soluções menos eficazes em ambientes corporativos mais complexos como o da Fundacentro. Além disso, o custo operacional advindo da impossibilidade de gerenciamento centralizado do parque gerará a necessidade de contratação de especialistas para operação de infraestrutura/segurança de TI destinados a manter a solução constantemente atualizada e disponível, tornando essa alternativa menos atraente no médio e longo prazo.

11. Análise comparativa de custos (TCO)

11.1 As soluções identificadas como viáveis são a Solução 3 – Contratar nova solução de antivírus e a Solução 4 – Atualização e expansão da solução atual da Fundacentro (McAfee) tendo em vista as seguintes questões:

11.1.1 Solução 3 – Contratar nova solução de antivírus corporativo:

11.1.1.1 Para adoção desta estratégia, verificou-se inicialmente que na eventual seleção de fabricante diverso da solução atual da Fundacentro (McAfee), será necessário realizar um complexo projeto de instalação, compreendendo a desinstalação de todos os seus agentes e módulos/componentes em mais de dois mil estações de trabalho, notebooks e servidores de rede físicos e virtuais que fazem parte do ambiente computacional da Fundacentro.

11.1.1.2 Ressalta-se que, apesar do processo de desinstalação e instalação da nova solução possuir automatizações, este poderá gerar impactos à disponibilidade e segurança dos endpoints e serviços de TI da Fundacentro durante este processo. Para tanto, cita-se aqui como um dos riscos possíveis, entre outros, o eventual erro ocorrido no processo de desinstalação/instalação que deixa o ativo desprotegido ou indisponível até que seja realizada a atuação presencial do técnico no endpoint para finalização deste processo. Nesse caso, o endpoint estará com a segurança cibernética prejudicada, pois não possuirá solução de antivírus sendo executado em condições adequadas ou ainda a solução instalada de forma automatizada causar comportamentos inadequados no endpoint (p/ ex., lentidões e travamentos). Dessa forma, poderá ser altamente impactada não somente as atividades finalísticas dos usuários, mas também a própria segurança das informações da Fundacentro, uma vez que com isso será elevado o risco de ocorrência de ataques bem-sucedidos durante esse período.

11.1.1.3 Além disso, destaca-se ainda que durante a operação da solução da McAfee na Fundacentro ao longo dos anos, parâmetros e regras específicas foram inseridas manualmente pelos administradores para que ela atingisse um elevado nível de estabilidade e integração com todos os sistemas/aplicações e ativos de TI do órgão. Sabe-se que, na eventual configuração de uma nova solução de antivírus de fabricante diverso, não ser possível exportar integralmente tais regras/customizações, considerando as peculiaridades de cada solução. Dessa forma, os serviços de TI da Fundacentro, sobretudo os críticos, poderão ser impactados por necessidades de ajustes pontuais da nova solução (p. ex.: falso-positivos) até que as novas customizações sejam efetivadas pela Contratada, num processo que poderá ser longo e impactante à disponibilidade dos sistemas de TI fundamentais para as operações finalísticas da Fundacentro.

11.1.1.4 Além dos riscos operacionais supracitados decorrentes da troca da solução acima, os seguintes custos diretos e indiretos estarão presentes nesta solução:

11.1.1.4.1 Instalação, migração e customização de uma nova solução de antivírus: em razão da troca da solução, os custos de instalação, migração e customização deverão ser contabilizados nessa estratégia. A pesquisa de preços detalhada em seções mais à frente deste estudo considerou a inclusão de tais custos nas propostas comerciais dos concorrentes.

11.1.1.4.2 Acompanhamento da instalação e customização da nova solução de antivírus: durante esta etapa, outros custos indiretos poderão ser adicionados a essa solução, pois a mudança poderá ocasionar dispêndios em contratos de Serviços Técnicos Especializados de Operação de Infraestrutura de TI e Serviços de Service Desk, dada a necessidade do acompanhamento dos técnicos das Contratadas no atendimento de chamados/incidentes abertos pelos usuários e gestores de aplicações durante ou após uma instalação efetuada com impactos ou resultado inesperado.

11.1.1.5 Haverá, também, a necessidade de contratação de serviço de treinamento na solução para toda a equipe da Fundacentro.

11.1.1.6 Em resumo, do ponto de vista técnico e da economicidade da troca da solução esta opção possui uma série de desvantagens em relação à Solução 4 - Atualizar e expandir a solução de antivírus atual da Fundacentro (McAfee), porém ainda foi considerada viável para fins de avaliação do TCO e comparação, a ser realizado nas próximas seções deste estudo:

11.1.1.6.1 Elevado risco operacional de indisponibilidade de serviços de TI críticos, tais como SEI, MonitorIBUTG, SSTFácil, Aleph/Primo (Biblioteca), entre outros, disponibilizados externamente e para o público interno, causando impactos no cumprimento das atividades e da missão institucional, bem como eventuais prejuízos à imagem e reputação da Fundacentro;

11.1.1.6.2 Custos diretos derivados da necessidade de contratação de serviço de instalação da nova solução e da realização de projeto complexo de instalação, dado à atual complexidade do parque computacional da Fundacentro, onde será necessário refazer todos os procedimentos de configurações específicos de customização já consolidados na solução atual para o funcionamento integrado da nova solução aos diversos sistemas de TI internos da Fundacentro, gerando dessa forma elevado retrabalho da equipe;

11.1.1.6.3 Custos indiretos derivados da alta probabilidade de abertura de chamados/incidentes relativos à episódios de indisponibilidade e mau funcionamento de estações de trabalho, notebooks, sistemas/serviços de TI pelos usuários, derivados do processo de implantação da nova solução de antivírus, refletidos nos contratos de serviços técnicos especializados de Service Desk e de Sustentação de Infraestrutura/Segurança de TI, uma vez que o processo automatizado de implantação poderá não ocorrer de forma esperada em todos os ativos devido a abrangência e complexidade do parque computacional da Fundacentro;

11.1.1.6.4 Custos diretos derivados da necessidade de treinamento de colaboradores da Fundacentro na administração e operação da nova solução pela equipe;

11.1.1.6.5 Perda do conhecimento adquirido na solução McAfee pela equipe da Fundacentro mediante a sua administração cotidiana, este último obtido na operacionalização da atual /solução no ambiente computacional da Fundacentro ao longo dos anos que resultaram no nível de eficiência operacional elevado;

11.1.2 A Solução 4 – Atualização e expansão da solução atual da Fundacentro (McAfee) também foi considerada viável, onde não foram identificadas desvantagens técnicas com relação a sua adoção e, além disso, foram levantadas as seguintes vantagens

técnicas e econômicas:

11.1.2.1 Provimento de adequado nível técnico de segurança cibernética à Fundacentro frente ao panorama atual de ameaças mundial refletindo em menores probabilidades de ocorrência de ataques cibernéticos bem-sucedidos no parque computacional devido ao emprego de recursos tecnológicos modernos de segurança cibernética em endpoints, em linha com as análises técnicas e imparciais realizadas por entidade externa (marca líder no Quadrante Mágico para proteção de endpoints do GARTNER);

Figure 1: Magic Quadrant for Endpoint Protection Platforms



11.1.2.2 Baixo impacto no ambiente computacional da Fundacentro, uma vez que não haverá necessidade de realização de projeto complexo de implementação pois a solução encontra-se totalmente integrada com as aplicações, sistemas e equipamentos da Fundacentro, não dependendo, portanto, de um longo processo de implantação e customização, envolvendo definição de arquitetura, abrangência, pré-requisitos, testes de instalação, ativação e desempenho, verificação de compatibilidades e configuração das funcionalidades, que diminui consideravelmente o risco de indisponibilidade de aplicações críticas, sistemas e equipamentos de TI da Fundacentro, que poderão impactar no cumprimento de sua missão institucional.

11.2. Os itens a seguir apresentam comparativo demonstrando o custo total de propriedade para a solução 3 e 4.

11.2.1 Após definição das soluções viáveis: Solução 3 – Contratar nova solução de antivírus e Solução 4 – Atualização e expansão da solução atual da Fundacentro (McAfee), a Equipe de Planejamento da Contratação (EPC) nomeada pela Portaria nº 1292, de 01 de março de 2024, realizou uma pesquisa de preços conforme descrito na Instrução Normativa nº 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

14.2.2 Dessa forma, foram inicialmente realizadas consultas ao painel de preços e painel de compras do Governo Federal. Para tanto, foram pesquisados como “serviço” as compras públicas ocorridas em 2023 e 2024 que continham a expressão “antivírus” no campo “objeto da compra”, “pregão” no campo “modalidade da compra”.

14.2.3 A partir dos dados informados nos relatórios do painel de preços na data da consulta, os documentos das contratações (editais e termos de referências) cujo objeto se mostraram inicialmente similares ao objeto de contratação desse estudo foram consolidadas nas tabelas a seguir.

14.2.4 A tabela 1 a seguir apresenta a composição de valores de licença de software antivírus, em características similares às especificadas neste Estudo.

Tabela 1 – Valores de licenças antivírus com características similares à especificada				
Identificação da Compra	Detalhamento do objeto	Item	Valor da licença contratada	Valor da licença transposta para 12 meses
00001/2023, Dispensa de Licitação, UASG 389419, Fonte: Compras eletrônicas	CESSAO TEMPORARIA DE DIREITOS SOBRE PROGRAMAS DE COMPUTADOR LOCAÇÃO DE SOFTWARE - O objeto do presente aviso é a escolha da proposta mais vantajosa para a aquisição de licenças para antivírus, para atender às necessidades do CREA-AL, conforme condições, quantidades e exigências estabelecidas neste Aviso de Dispensa Eletrônica e no Termo de Referência (Anexo I) e demais anexos.	1	R\$ 251,96 (36 meses)	R\$ 83,98
00054/2023, Pregão, UASG 928790, Fonte: Painel de preços	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR - Registro de Preços para futura e eventual contratação de empresa especializada em fornecimento de materiais, equipamentos, licenças de softwares e licença de antivírus (com serviço de suporte, assistência técnica e atualizações), para atender as necessidades e demandas do SAAE - Serviço Autônomo de Saneamento Básico, no município de Itabirito MG.	47	R\$ 1.025,00 (60 meses)	R\$ 205,00
00872/2023, Pregão, UASG 238014, Fonte: Painel de Preços	LICENCIAMENTO DE OUTROS DIREITOS PERMANENTES SOBRE PROGRAMAS DE COMPUTADOR.	1 a) – Licenças perpétuas por host (para ambiente virtual – máquinas virtuais – e ambiente físico – servidores físicos), com garantia, suporte e atualização de assinaturas para 48 meses	R\$ 900,00 (48 meses)	R\$ 225,00

14.2.4.1 A média unitária para o item licença de antivírus para 12 meses é de R\$ 171,33.

14.2.5 A tabela 2 a seguir apresenta os valores de instalação e treinamento, os quais são necessários apenas no para a solução 3, conforme previamente mencionado neste Estudo:

Tabela 2 – Valores de instalação e treinamento, necessários no caso da solução 3					
Identificação da Compra	Detalhamento do objeto	Item	Valor unitário	Valor anual	Valor total
00004/2023, Pregão, UASG 27456, Fonte: Painei de Preços	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA ESTACAO DE TRABALHO	3 - Instalação solução antivírus	14.189,33	14.189,33	R\$ 35.169,33
		5 - Treinamento	20.980,00	20.980,00	
00025/2023, Pregão, UASG 974004, Fonte: Compras eletrônicas	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE OUTROS SOFTWARES / PROGRAMAS DE COMPUTADOR - Pregão Eletrônico - Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, atualização da base de vacinas e software, treinamento e suporte técnico especializado pelo período contratado, de acordo com as especificações e as exigências constantes no Termo de Referência Anexo I do Edital.	3 – Operação assistida	35.000,00	35.000,00	R\$ 54.000,00
		5 - Treinamento	19.000,00	19.000,00	

00872/2023, Pregão, UASG 238014, Fonte: Painel de Preços	LICENCIAMENTO DE OUTROS DIREITOS PERMANENTES SOBRE PROGRAMAS DE COMPUTADOR.	1 b) – Serviço de instalação – Licenciamento inicial	200.000,00	200.000,00	R\$ 266.666,66
		1 d) – Treinamento (Capacitação técnica em 3 turmas)	200.000,00 (3 turmas)	66.666,66 (1 turma)	

14.2.5.1 A média unitária para o item instalação é de R\$ 83.063,11.

14.2.5.2 A média unitária para o item treinamento é de R\$ 118.611,99.

14.2.6 Para confrontar os valores a serem investidos na solução 3 e na solução 4, apresenta-se a Tabela 3 a seguir:

Tabela 3 – Comparativo solução 3 e solução 4					
Solução	Descrição do item	Valor unitário médio	Quantidade a contratar	Valor para 12 meses	Valor para 24 meses
Solução 3	Instalação	R\$ 83.063,11	1	R\$ 83.063,11	R\$ 83.063,11
	Treinamento	R\$ 118.611,99	1	R\$ 118.611,99	R\$ 118.611,99
	Licença antivírus	R\$ 171,33	250	R\$ 42.832,50	R\$ 85.665,00
	Totais			R\$ 244.507,60	R\$ 287.340,10
Solução 4	Licença antivírus	R\$ 171,33	250	R\$ 42.832,50	R\$ 85.665,00
	Totais			R\$ 42.832,50	R\$ 85.665,00

14.2.6.1 Ao analisar o custo total de propriedade, verifica-se que do ponto de vista econômico a opção mais adequada entre as duas avaliadas (contratação de nova solução versus atualização da solução atual da Fundacentro) é a atualização com a solução de antivírus McAfee/Trellix atualmente instalada na Fundacentro (solução 4).

12. Descrição da solução de TIC a ser contratada

Atualização tecnológica da solução de segurança de endpoints McAfee/Trellix, com garantia de atualizações de versões e suporte técnico do fabricante por 24 (vinte e quatro) meses, prorrogáveis por iguais e sucessivos períodos, até o limite previsto na Lei 14.133/2021;

13. Estimativa de custo total da contratação

Valor (R\$): 85.665,00

Valores finais de referência da contratação				
Item	Objeto	Quantidade	Valor unitário	Valor total
1	Atualização tecnológica da solução de segurança de endpoints McAfee/Trellix, com garantia de atualizações de versões e suporte técnico do fabricante por 24 (vinte e quatro) meses, prorrogáveis por iguais e sucessivos períodos, até o limite previsto na Lei 14.133/2021	250 unidades de licença de software antivírus	R\$ 342,66	R\$ 85.665,00
Valor global de referência				R\$ 85.665,00

14. Justificativa técnica da escolha da solução

14.1 A escolha da solução destinada a “Atualização tecnológica e expansão da solução McAfee/Trellix no ambiente computacional da Fundacentro” tem as seguintes justificativas técnicas, conforme análises descritas nas seções anteriores deste documento:

14.1.1 Atendimento adequado das necessidades técnicas e tecnológicas da Fundacentro relativas ao gerenciamento, prevenção e tratamento de incidentes causadas por malwares em redes computacionais, uma vez que não há relatos de proliferação em série de malwares em sistemas e computadores da Fundacentro que não tenham sido tratadas e contidas pela solução nos últimos anos e, além disso, tem qualidade técnica aferida por institutos independentes de tecnologia da informação, que pode ser comprovada por meio do posicionamento atual da McAfee/Trellix no quadrante de líderes do “Quadrante Mágico para Plataformas de Proteção de Endpoints” do Gartner e por meio do selo “Top Product Aprovado for Corporate Endpoint Protection - Windows” nos resultados dos testes de qualidade efetuados pela organização internacional “AV-Test.org” (<https://www.av-test.org/en/>).

14.1.2 Baixa probabilidade de indisponibilidade de estações de trabalho, sistemas e serviços de TI críticos ao público interno e externo que podem causar prejuízos no cumprimento da missão institucional, imagem e reputação da Fundacentro, tais como MonitorIBUTG, SSTFácil, Sistema Eletrônico de Informações (SEI), Aleph/Primo (sistemas da biblioteca), entre outros, em oposição ao elevado risco de indisponibilidade na eventual realização de troca da ferramenta, pois a solução McAfee encontra-se totalmente compatibilizada, estável e integrada aos diversos sistemas e serviços de TI internos e externos da Fundacentro;

14.1.3 Manutenção do conhecimento técnico adquirido pela equipe técnica na solução McAfee durante os anos de sua operação na Fundacentro, que permitiu que ela atingisse um elevado nível de estabilidade de funcionamento e proteção integrada às várias plataformas e tecnologias da informação que compõem o ambiente computacional da Fundacentro não possuindo uma longa curva de aprendizado pela equipe técnica quando comparada à realização da eventual troca da solução.

15. Justificativa econômica da escolha da solução

Como pode ser averiguado na seção 11 deste estudo - ANÁLISE COMPARATIVA DOS CUSTOS (TCO) – esta solução promove maior economicidade à Fundacentro dentre as estratégias viáveis tecnicamente, uma vez que o valor global para adquirir uma nova solução é maior quando comparado ao valor global para atualizar a solução existente.

Ressalta-se ainda que esta economia estimada nos custos diretos com a adoção da estratégia de renovação da solução atual quando comparada aos custos diretos da estratégia de troca da solução deverá ainda ser maior se forem adicionados os custos indiretos que serão originados se adotada pela equipe a estratégia pela troca da solução da Fundacentro conforme detalhado na

referida seção 12 deste estudo (abertura de chamados relacionados à incidentes, interrupções de serviços, necessidades de novas customizações, parametrizações, entre outros, decorrentes da concretização de riscos operacionais existentes na troca da solução do ambiente computacional).

Por fim, com a adoção da estratégia de renovação com atualização da atual solução McAfee da Fundacentro, haverá o melhor aproveitamento do capital investido nela relativos à sua implantação, parametrização e customização para pleno funcionamento ao ambiente computacional da Fundacentro desde a sua adoção e utilização no órgão ao longo dos anos.

16. Benefícios a serem alcançados com a contratação

- Continuidade de proteção cibernética aplicada diretamente nos endpoints contra ataques cibernéticos variados que envolvem execução de malwares em computadores;
- Modernização dos mecanismos de proteção cibernética aplicados nos endpoints para controle de códigos maliciosos executados no parque computacional;
- Redução dos riscos cibernéticos associados à segurança das informações da Fundacentro;
- Economicidade na contratação frente à alternativa de realização de troca da solução;
- Manter a disponibilidade, a integridade e a confiabilidade dos dados e a continuidade dos serviços prestados pela Fundacentro;
- Com a atualização tecnológica da solução antivírus, evita-se o reinício de todo o processo de instalação, configuração, treinamento e curva de aprendizado dos recursos de outra ferramenta de solução de segurança;
- Economicidade e eficiência;
- Manutenção do gerenciamento centralizado da solução de segurança das estações de trabalho e servidores institucionais;
- Manutenção e elaboração de políticas e controles globais de acesso e uso de recursos de rede, efetuadas em nível de dispositivo;
- Melhoria na proteção das informações e dados pessoais e corporativos, atendendo as exigências do Programa de Privacidade e Segurança da Informação (PPSI) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

17. Providências a serem Adotadas

Não serão necessárias adequações no ambiente da Fundacentro ou capacitação para a gestão e fiscalização do contrato pelos servidores que serão incumbidos dessa atividade na Instituição.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A contratação proposta neste Estudo, qual seja, a atualização tecnológica da solução de segurança de endpoints McAfee/Trellix, com garantia de atualizações de versões e suporte técnico do fabricante por 24 (vinte e quatro) meses, prorrogáveis por iguais e sucessivos períodos, até o limite previsto na Lei 14.133/2021, é viável considerando o exposto neste ETP. Em cumprimento ao disposto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e em conformidade com a Lei nº 14.133/2021, o presente documento segue assinado pelos Integrantes Requisitante e Técnico da Equipe de Planejamento da Contratação, designada pelo documento de Instituição da Equipe de Planejamento da Contratação (Portaria nº 1292/2024 - SEI 0261654)

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: Portaria Fundacentro nº 1292, de 01 de março de 2024

NORISVALDO FERRAZ JUNIOR

Membro da comissão de contratação



Assinou eletronicamente em 01/04/2024 às 12:01:38.

Despacho: Portaria Fundacentro nº 1292, de 01 de março de 2024

DIEGO RICARDI DOS ANJOS

Membro da comissão de contratação



Assinou eletronicamente em 02/04/2024 às 10:38:56.

Despacho: Portaria Fundacentro nº 1292, de 01 de março de 2024

MANUEL PEREIRA TEIXEIRA

Membro da comissão de contratação



Assinou eletronicamente em 01/04/2024 às 15:22:38.