FUNDAÇÃO NACIONAL DE SAÚDE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 25100.004170/2022-80

1. INTRODUÇÃO

1.1. Este Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. O presente documento visa oferecer subsídios à elaboração do Termo de Referência, estabelecer parâmetros para uma boa execução contratual e está alinhado com o disposto na Instrução Normativa nº 01, de 04 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia - SGD/ME.

2. DESCRIÇÃO DA NECESSIDADE

2.1. Descrição da Solução de Tecnologia da Informação

2.1.1. Trata-se de demanda da Coordenação-Geral de Modernização e Tecnologia da Informação - CGMTI para analisar a viabilidade de Contratação de empresa especializada no fornecimento de Solução de Segurança, Auditoria e Governança, contemplando instalação, treinamento e garantia da proteção dos dados da Fundação Nacional de Saúde por 12 meses.

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de segurança, auditoria e prevenção de ameaças	Contas do AD	3190
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	Serviço	1
3	Treinamento para 5 participantes	Turma	1

Tabela 1 – Descrição da Solução.

2.2. Motivação/Justificativa

2.2.1. A Fundação Nacional de Saúde (FUNASA), órgão executivo do Ministério da Saúde, é uma das instituições do Governo Federal responsável em promover a inclusão social por meio de ações de saneamento para prevenção e controle de doenças. É também a instituição responsável por formular e implementar ações de promoção e proteção à saúde relacionadas com as ações estabelecidas pelo Subsistema Nacional de Vigilância em Saúde Ambiental.

2.2.2. No que se refere à gestão de tecnologia da informação, os princípios e os fundamentos formulados pela FUNASA têm como sustentação a correta utilização de recursos de infraestrutura e o planejamento de informatizar seus processos, nesse sentido, existe a necessidade de um aporte tecnológico capaz de manter a integridade, confidencialidade e disponibilidade das informações.

2.2.3. Considerando as informações tratadas no âmbito da FUNASA, como ativos valiosos para a eficiente prestação dos serviços públicos e a necessidade de incrementar a segurança dos ativos, físicos e digitais, assim como a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pela instituição, assegurando sempre a qualidade dos serviços públicos e garantindo a segurança com relação à guarda de "dados sensíveis" pelo governo, através da adoção de medidas rigorosas de segurança para acesso dessas informações.

2.2.4. Partindo-se deste princípio, a contratação da solução proposta visa aprimorar a capacidade de segurança, auditoria e governança no que tange os recursos de dados não estruturados, assim como a proteção das credenciais de acesso privilegiadas e de alto valor, adequando a infraestrutura à crescente demanda por medidas protetivas modernas e gestão de ativos eficiente. Essa necessidade é reforçada no item 6.12, 6.13 e 6.14 da Política de Segurança da Informação e Comunicações POSIC da FUNASA.

2.2.5. Segundo o instituto de pesquisas técnicas e análises de tendências de TI – o *Gartner Group*, cerca de 80% dos dados estratégicos estão armazenados em base de dados não estruturadas ou semiestruturadas. Toda essa informação está distribuída em pastas (departamentais, setoriais e individuais) acessadas pelos diversos usuários da rede e gerenciadas por sistemas operacionais que proporcionam registro de eventos (*Log's*) custoso e pouquíssimo informativo e que não proporcionam a devida granularidade para pesquisas de auditoria referentes a quem, quando, onde e como um dado é utilizado.

2.2.6. A infraestrutura de TI da fundação é composta, de forma resumida, por equipamentos servidores destinados ao processamento e armazenamento de dados, estações de trabalho usadas pelos colaboradores além dos elementos de interconexão. A solução de segurança, auditoria e governança é de suma importância para garantir os princípios básicos de segurança e conformidade para os ativos e funcionários da FUNASA, assim como para o registro histórico das atividades ocorridas no ambiente tecnológico, auxiliando no monitoramento e investigação contra possíveis ameaças cibernéticas.

2.2.7. De acordo com o relatório de segurança da IBM, o Security X-Threat de 2022, o maior vetor de entrada a um ambiente foi através de seus usuários, que por métodos de invasão escalavam até um ataque de Ransomware em todo o ambiente tecnológico, sendo esse o tipo de ataque mais observado em 2021. Atualmente a FUNASA dispõem apenas dos sistemas operacionais para a geração e coleta de logs de auditoria, que são usados para rastrear ações indevidas e possíveis incidentes. Esse método vem tornando-se cada vez mais ineficiente, uma vez que o volume de eventos de auditoria cresce substancialmente sem nenhum tipo de tratamento ao dado, dificultando as pesquisas por fatos relevantes e onerando as mídias de armazenamento do órgão.

2.2.8. A identificação de usuários comprometidos, sejam eles comuns ou privilegiados, requer o uso de ferramentas capazes de avaliar o comportamento do usuário, normalmente através de *Machine Learning*. Um usuário comprometido é, normalmente, a porta de entrada para ataques como os citados. Por essa razão, a capacidade de conhecer o comportamento de cada usuário da rede e de verificar se esses estão ou não comprometidos é recurso essencial atualmente, onde há um crescente ataque às instituições e empresas.

2.2.9. A Funasa provê a seu corpo técnico de TIC soluções e tecnologias que permitem à Fundação executar seus serviços para a sociedade. A gestão dessas soluções demanda o constante acesso de analistas e técnicos a componentes críticos, que, por falta de medidas de controles eficientes, podem estar com suas credenciais comprometidas. Um exemplo observado em âmbito nacional foi o ataque ao ambiente do Superior Tribunal de Justiça, onde uma conta privilegiada foi comprometida e através dela foram iniciadas inúmeras ações maliciosas que passaram despercebidas pelos métodos convencionais de auditoria e controle. Tendo em vista a necessidade de rastrear e monitorar as ações dentro do ambiente de TIC, a Funasa levanta a necessidade de contratar uma solução capaz de auditar e alertas ações que fujam do comportamento padrão das credenciais que possuem alto nível de acesso ao ambiente.

2.2.10. A atual arquitetura da FUNASA é constituída por 2700 colaboradores que operam dispositivos de microinformática acessados por suas contas de usuário, manipulando diariamente arquivos e ativos digitais sensíveis, tanto em suas máquinas como em repositórios centrais. Para que os sistemas internos possam operar de forma devida são utilizadas em torno de 300 contas de serviços que orquestram e disponibilizam os recursos aos usuários através do *Active Directory* (AD). Um levantamento interno demonstra que metade do total de contas possuem um grau mais elevado de permissionamento no ambiente de TIC, sendo consideradas contas de com maior risco de impacto caso sejam comprometidas ou sequestradas por algum ator malicioso. Sendo assim, a FUNASA visa realizar um processo de segurança em camadas para a proteção dessas contas que tendem a ser mais visadas, entre elas as de presidente, secretários, diretores, coordenadores, contas de serviços críticos e colaboradores que detenham poder sobre ativos críticos para a fundação.

2.2.11. A fim de garantir a conformidade de acesso dos seus usuários, a integridade dos dados e capacidade de auditoria e segurança, a FUNASA visa adotar uma solução de segurança que traga maior agilidade para seus controles internos, possibilitando o monitoramento e conformidade para os repositórios de dados, serviços de base de usuários e estações de trabalho. Os principais benefícios desta aquisição serão a garantia da proteção das informações do ambiente tecnológico, visibilidade das estruturas, análise e correlação de eventos nos ativos digitais e físicos, e a capacidade de monitorar e prever possíveis ameaças ao ambiente da FUNASA, viabilizando inclusive a proteção das contas com acessos elevados a infraestrutura crítica do ambiente.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. A Fundação Nacional de Saúde (FUNASA), órgão executivo do Ministério da Saúde, é uma das instituições do Governo Federal responsável por promover a inclusão social por meio de ações de saneamento para prevenção e controle de doenças. É também a instituição responsável por formular e implementar ações de promoção e proteção à saúde relacionadas com as ações estabelecidas pelo Subsistema Nacional de Vigilância em Saúde Ambiental.

3.1.2. No que se refere à gestão de tecnologia da informação, os princípios e os fundamentos formulados pela FUNASA têm como sustentação a correta utilização de recursos de infraestrutura e o planejamento de aprimorar os processos de segurança, nesse sentido, existe a necessidade de uma aquisição (software) capaz de manter a integridade, confidencialidade e disponibilidade das informações.

3.1.3. Uma Solução de segurança, auditoria e prevenção de ameaças é componente fundamental para a Organização, pois garante a proteção dos colaboradores contra atores maliciosos, proporciona maior visibilidade dos ativos físicos e digitais e evita o abuso de poder por parte das credenciais com acesso a recursos críticos da CGMTI.

3.1.4. Hoje, é fundamental manter as áreas de negócio do órgão com recursos tecnológicos que garantam o acesso seguro e controlado às informações de sua propriedade ou sob sua custódia, protegendo-as de acessos não autorizados, conforme a Política de Segurança da Informação.

3.1.5. A contratação em tela visa atender às necessidades de segurança apresentadas na Política de Segurança da Informação e Comunicação da Funasa, como:

- Prover maior capacidade de classificação e governança das informações disponibilizadas pelos recursos centrais da Organização, compreendendo quais dados podem estar expostos;
- Monitoramento e auditoria continua dos acessos aos recursos centrais e estações de trabalho corporativas,
- Aproveitamento eficiente do espaço de armazenamento dos eventos de auditoria;
- Aprimorar a gestão de segurança da informação e comunicações.
- Mitigar o risco de ataques de *ransomware* e, caso ele ocorra, limitar seu efeito e consequente impacto;
- Atender às normas para auditoria e inventário:
  - Art. 4º a 9º da Instrução Normativa GSI Nº 3, de 28 de maio de 2021;
  - Guia do Framework de Segurança e CIS Controls v8;
  - Controle 1: Inventário e Controle de Ativos de Hardware;
  - Controle 2: Inventário e Controle de Ativos de Software;
  - ABNT NBR ISO/IEC 27002;
  - Gestão de Ativos Norma Complementar GSI nº 21/2014;
  - Guia do Framework de Segurança;
  - CIS Controle 6: Manutenção, Monitoramento e Análise de Logs de Auditoria;
  - Controle 08: Gestão de registros de auditoria;
  - ABNT NBR ISO/IEC 27002 - 12.4 Registros e Monitoramento.

3.1.6. Manter e modernizar todas essas questões relacionadas à infraestrutura de TI, para que o cerne desta atividade mantenha a estratégia de negócio e as necessidades institucionais da Funasa.

3.1.7. Esta contratação também possui o objetivo de atender as exigências sobre a proteção de dados apoiando demandas da Lei Geral de Proteção de Dados - LGPD.

3.1.8. O processo de auditoria e governança é parte dos procedimentos de Segurança da Informação que a CGMTI tem como obrigação de executar e garantir conforme especificado no item 6 - Diretrizes Específicas da Politica de Segurança da Informação e Comunicação devendo proporcionar maior controle dos ativos digitais e físicos da Funasa. Esclarece-se ainda que, por tratar-se de uma solução de apoio à gestão da política de segurança da informação e comunicação da FUNASA, existe o entendimento de que a operação desta infraestrutura deve ser considerada serviço contínuo, demandando.

3.1.9. O projeto em questão está em conformidade e encontra-se alinhada ao Plano Diretor de Tecnologia da Informação – PDTIC da FUNASA e proposta orçamentária de 2022, bem como ao Planejamento Institucional 2018 - 2023.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**OBJETIVOS ESTRATÉGICOS**
N4	Implantar e atualizar controles que promovam a Segurança da Informação e Comunicações
N9	Melhorar a prestação de serviços à sociedade através da transformação digital

Tabela 2 - Alinhamento aos Planos Estratégicos.

ALINHAMENTO AO PDTIC DA FUNASA			
ID	**META**	**ID**	**AÇÃO**
M4	Manter os serviços especializados de suporte ao usuário	A4.2	Contratar/Manter serviços especializados em Governança e Gestão (apoio)
M5	Implementar ações de Segurança da Informação e Proteção de Dados (adequação tecnológica à LGPD)	A5.3	Implementação de controles para conformidade com a LGPD

Tabela 3 – Alinhamento da Demanda ao PDTIC da Funasa

ALINHAMENTO AO PLANEJAMENTO INSTITUCIONAL 2018 - 2023		
ID	**CÓD. DA INICIATIVA**	**TÍTULO DA INICIATIVA**
OE11	IE11.3A	Implementar o Plano de Transformação Digital como Plano Estratégico, em consonância com a Política de Gestão da Informação

Tabela 4 – Alinhamento da Demanda ao Planejamento Institucional da Funasa.

ALINHAMENTO AO PAC 2022		
Nº ITEM	**TIPO DE ITEM**	**DESCRIÇÃO**
308	Soluções de TIC	SERVICO DE LICENCA PELO USO DE SOFTWARE

Tabela 5 – Alinhamento da Demanda ao PAC 2022 da Funasa.

ALINHAMENTO À ESTRATÉGIA DE GOVERNO DIGITAL
A presente aquisição também guarda alinhamento à Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, instituída pelo Decreto nº 10.332, de 28 de Abril de 2020, no tocante ao Objetivo Estratégico OE 16 "**Otimização das infraestruturas de tecnologia da informação**". Para alcance desse objetivo estratégico, a EGD enuncia como iniciativa (Iniciativa nº 16.1) a realização de, no mínimo, seis compras centralizadas de bens e serviços comuns de TIC, até 2022.

Tabela 6 - Alinhamento da demanda à Estratégia de Governo Digital.

3.2. **Requisitos Tecnológicos e Demais Requisitos**

3.2.1. **REQUISITOS DE CAPACITAÇÃO**

3.2.1.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução;

3.2.1.2. O treinamento será demando à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento;

3.2.1.3. O treinamento deverá ser em Brasília – DF, para a equipe técnica do CONTRATANTE;

3.2.1.4. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA;

3.2.1.5. O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida, englobando tanto os componentes de hardware quanto de software;

3.2.1.6. Deverá ser ofertada para 3 (três) pessoas e com carga horária mínima de 40 (quarenta) horas;

3.2.1.7. Deverá ser fornecido certificado de conclusão emitido pelo fabricante;

3.2.1.8. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde);

3.2.1.9. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.

3.2.2. **REQUISITOS LEGAIS**

3.2.3. A contratação do objeto deste Estudo tem amparo legal nos seguintes dispositivos legais:

3.2.4. Lei nº 8.666, de 21 de junho de 1993, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

3.2.5. Lei 12.349, altera as de 21 de junho de 1993, 8.958, de 20 de dezembro de 1994, e 10.973, de 2 de dezembro de 2004; e revoga o §1° do art. 2° da Lei no 11.273, de 6 de fevereiro de 2006.

3.2.6. Decreto nº 3.555, de 08 de agosto de 2000, que aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

3.2.7. Lei nº 10.520, de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

3.2.8. Decreto nº 5.450, de 31 de maio de 2005, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;

3.2.9. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da microempresa e da Empresa de Pequeno Porte, altera dispositivos das Leis nºs 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nºs 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de

3.2.10. Instrução Normativa nº 05 do MPOG, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

3.2.11. Instrução Normativa Nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

3.2.12. Instrução Normativa nº 73, de 5 de agosto de 2020, 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;

3.2.13. A referida contratação deve assegurar os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), descritos no Artigo 6º. da Lei. Toda informação trafegada, por meio dos equipamentos de tecnologia da informação e comunicação, que fazem parte do objeto de contratação devem atender às exigências da Lei Geral de Proteção de Dados Pessoais.

3.3. **REQUISITOS DE MANUTENÇÃO E GARANTIA**

3.3.1. A garantia de funcionamento das licenças adquiridas, bem como o suporte técnico serão pelo período de 12 meses.

3.3.2. O serviço de assistência técnica em GARANTIA deverá cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças, ajustes e reparos técnicos

em conformidade com manuais e normas técnicas especificadas pelo fabricante.

3.3.3. Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema;

3.3.4. Para efeitos de certificar a garantia, a CONTRATADA deve possuir recurso disponibilizado via web, site do próprio fabricante, que permita verificar a garantia do equipamento através da inserção do seu número de série;

3.3.5. A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia técnica do contrato;

3.3.6. Os serviços de suporte técnico abrangem:

3.3.6.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

3.3.6.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;

3.3.6.3. Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;

3.3.6.4. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

3.3.7. O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

3.3.8. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução;

3.3.9. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;

3.3.10. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

3.3.11. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

3.3.12. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

3.3.13. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

3.3.14. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web, E-mail, Central 0800 e/ou telefone fixo;

3.3.15. O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;

3.3.16. O recebimento dos equipamentos/serviços será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos/serviços e a forma definitiva será após a instalação, configuração e teste da solução.

3.4. REQUISITOS TEMPORAIS

3.4.1. O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência;

3.4.2. O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

3.4.3. Os equipamentos e as licenças de softwares devem ser entregues em Brasília, no endereço descrito na tabela abaixo:

UF	ENDEREÇO
DF	SAUS QUADRA 04 , BL- N. Cidade: Brasília. UF: Distrito Federal - DF. CEP: 70070040. - Brasília/DF - CEP: 70.719-040 - Telefone: (61) 3314-6466/6442 Fax: (61) 3314-6253

Tabela 7 - Endereço de entrega da solução.

3.4.4. A entrega dos equipamentos deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

3.4.5. Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

3.4.6. O recebimento dos equipamentos será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

3.5. REQUISITOS DE SEGURANÇA

3.5.1. A empresa CONTRATADA para prestação dos serviços deverá observar os seguintes requisitos quanto à Segurança da Informação e Comunicações:

3.5.1.1. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela FUNASA, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação e Comunicações e suas Normas Complementares, durante a execução dos serviços nas instalações da FUNASA;

3.5.1.2. Deverá ser garantida a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações inerentes ao contrato e seus serviços, podendo ser responsabilizado legalmente quem porventura causar perdas e danos à FUNASA e a terceiros;

3.5.1.3. Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes:

a) Término ou rompimento do Contrato; ou

b) Solicitação da FUNASA.

3.5.1.4. Devem ser utilizadas ferramentas de proteção e segurança de informações, a fim de evitar qualquer acesso não autorizado aos sistemas e softwares, seja em relação ao que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados a FUNASA, ainda que por meio de link;

3.5.1.5. Quando solicitado formalmente pela FUNASA, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado;

3.5.1.6. A CONTRATADA deverá informar à FUNASA, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;

3.5.1.7. Prestar os esclarecimentos necessários à FUNASA, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução;

3.5.1.8. Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos causados a FUNASA e a terceiros;

3.5.1.9. A empresa CONTRATADA não poderá divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na FUNASA, sem prévia autorização;

3.5.1.10. O acesso às instalações da CONTRATADA onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas;

3.5.1.11. A CONTRATADA deverá manter os seus profissionais identificados por crachás, quando em trabalho, devendo substituir imediatamente aquele que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da FUNASA;

3.5.1.12. A CONTRATADA deverá manter os seus profissionais informados quanto às normas disciplinares da FUNASA, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações;

3.5.1.13. Deverá ser celebrado TERMO DE COMPROMISSO entre a CONTRATADA e a FUNASA para garantir a segurança das informações da FUNASA, assim como, celebrado o TERMO DE CIÊNCIA a todos envolvidos na prestação dos serviços;

3.5.1.14. Não transferir a terceiros os serviços contratados;

3.5.1.15. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro da FUNASA.

3.6. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

3.6.1. Aderência aos padrões definidos pelo Modelo de Acessibilidade em Governo Eletrônico – e-MAG, conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007, quando houver necessidades de acessibilidade ao aplicativo para solicitações de suporte técnico;

3.6.2. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela Contratante; e

3.6.3. A Contratada deverá instruir os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pela Contratante, autorizando a participação desses em eventos de capacitação e sensibilização promovidos pela Contratante, quando for o caso.

3.7. REQUISITOS DE PAGAMENTO

3.7.1. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

3.7.1.1. As licenças forem entregues e instaladas pela CONTRATADA atendendo às especificações contidas no Termo de Referência;

3.7.1.2. O fornecedor emitir certificado de garantia de 12 meses para as licenças entregues;

3.7.1.3. A qualidade do serviço tiver sido avaliada e aceita pela CONTRATANTE.

3.7.2. O pagamento deverá ser efetuado mediante a apresentação de Nota Fiscal ou Fatura pela CONTRATADA, que deverá conter as informações necessárias à conferência do objeto fornecido, incluindo o prazo de validade, a data da emissão, os dados do contrato e do órgão contratante, o período de prestação dos serviços, o valor a pagar e eventual destaque do valor de retenções tributárias cabíveis.

3.7.3. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência, no prazo de até 05 (cinco) dias úteis.

3.7.4. Em até 15 (quinze) dias corridos após a emissão do Termo de Recebimento Provisório, salvo a inexistência de pendências a serem saneadas, sendo confirmada sua operação e desempenho a contento, nos termos do Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo;

3.7.5. Antes do pagamento, a CONTRATANTE verificará a regularidade fiscal da CONTRATADA através de consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores - SICAF, ou na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios oficiais.

3.7.6. À CONTRATANTE fica reservado o direito de retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis quando a CONTRATADA:

3.7.6.1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

3.7.6.2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade inferior à demandada.

3.8. REQUISITOS DE ACEITAÇÃO DO OBJETO

3.8.1. A aceitação do objeto ocorrerá apenas se a empresa vencedora apresentar todos os critérios de habilitação;

3.8.2. A descrição do objeto na Nota Fiscal deverá ser idêntica à descrição do edital e da Nota de Empenho, caso contrário o serviço executado deverá ser recusado para correção da documentação por parte da contratada.

3.9. DA INSTALAÇÃO E CONFIGURAÇÃO

3.9.1. A CONTRATADA deverá instalar a solução ofertada nas instalações da CONTRATANTE;

3.9.2. A empresa que realizar a implantação deverá ter técnicos treinados em toda a solução ofertada;

3.9.3. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI do local de instalação.

4. LEVANTAMENTO DAS ALTERNATIVAS

4.1. **IDENTIFICAÇÃO DAS POSSÍVEIS SOLUÇÕES**

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	Adoção de solução baseada em software livre.
2	Aquisição de solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint,* pelo período de 12 meses.

Tabela 8 - Descrição das soluções/cenários.

4.2. **ANÁLISE COMPARATIVA DAS SOLUÇÕES**

4.2.1. **SOLUÇÃO 1**

4.2.1.1. A primeira solução a ser avaliada consiste na adoção de software livre. Por “software livre” devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários, à grosso modo, isso significa que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software.

4.2.1.2. Ao mesmo tempo que tal fato pode ser encarado de forma positiva, há que se levar em consideração que este cenário apresenta uma grande fragilidade de segurança, tendo em vista que as customização são feitas livremente sem levar em consideração aspectos importantes de padronização, escalabilidade e consistência.

4.2.1.3. Outro ponto muito importante na adoção de software livre é que estes não possuem suporte ou garantia, ficando os dados desta FUNDAÇÃO, a mercê de comunidades livres, sem SLA ou qualquer tipo de garantia.

4.2.1.4. Pelas razões supracitadas, a equipe de planejamento da contratação não encontrou elementos objetivos que justifiquem a utilização desse cenário/solução.

4.3. **SOLUÇÃO 2**

4.3.1. A solução 2 consiste na contratação de nova solução de mercado compreendendo a contratação de empresa especializada no fornecimento de Solução de Segurança, Auditoria e Governança, contemplando instalação, treinamento e garantia da proteção dos dados da Fundação Nacional de Saúde por 12 meses.

4.4. Considerando o ambiente atual da Funasa, esta solução possibilitará o atendimento das necessidades atuais da fundação, com ganho em qualidade e eficiência, além de prover o atendimento aos requisitos de segurança da informação, garantindo a disponibilidade e continuidade dos serviços de TI, bem como para atender às constantes evoluções dos recursos de TIC.

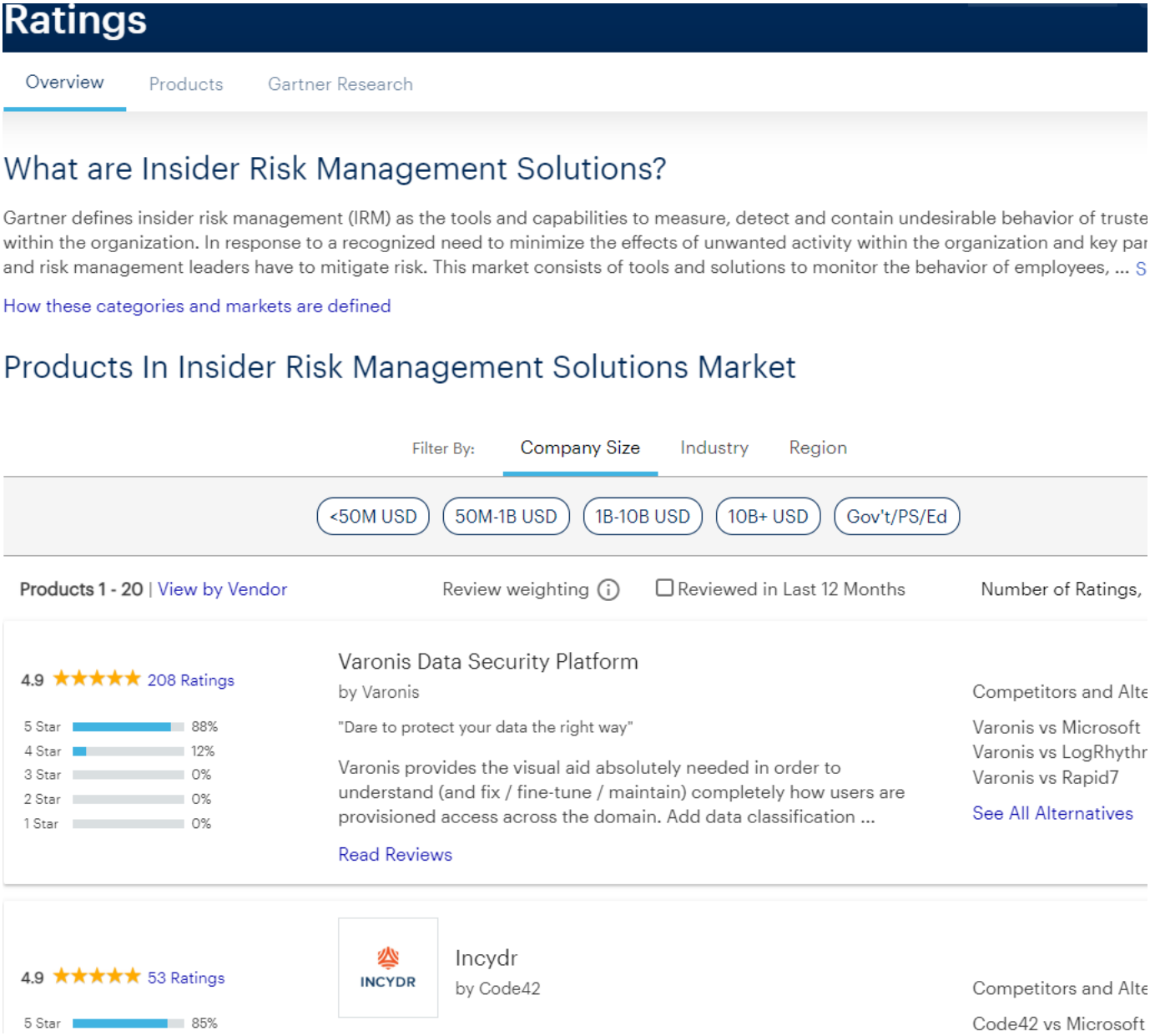
4.5. Por meio da aquisição da solução 2 será possível atender as necessidades da Funasa, com ganho em qualidade e eficiência, além de prover o atendimento aos requisitos de segurança da informação, garantindo a disponibilidade e continuidade dos serviços de TI, bem como para atender às constantes evoluções dos recursos de TIC.

4.6. Portanto, a equipe de planejamento da contratação não encontrou justificativa técnica ou econômica para não seguir o recomendado neste cenário.

4.7. **SOLUÇÕES DISPONÍVEIS NO MERCADO**

4.7.1. Para a solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*, não encontramos no mercado um único software que abrange toda a demanda. Existem softwares que atendem partes dos requisitos, alguns mais do que outros. No entanto, a demanda pode ser atendida se a contratação não focar em um produto único, mas em uma solução formada por mais de um software e fornecida ao Tribunal através de empresas integradoras, ou seja, por empresas que integram produtos de TIC e a entregam como uma solução.

4.7.2. Consoante análise de mercado realizada pelo Gartner (empresa com atuação no ramo de pesquisas, consultorias, eventos e prospecções acerca do mercado de TI), o mercado de soluções de segurança para prevenção contra vazamento de informaçõe**s** apresenta diversos fabricantes e soluções conforme pode ser visto em levantamento anual acerca de soluções Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados (análise comportamento de usuário).



Ratings

Overview Products Gartner Research

What are Insider Risk Management Solutions?

Gartner defines insider risk management (IRM) as the tools and capabilities to measure, detect and contain undesirable behavior of truste within the organization. In response to a recognized need to minimize the effects of unwanted activity within the organization and key par and risk management leaders have to mitigate risk. This market consists of tools and solutions to monitor the behavior of employees, ... S

How these categories and markets are defined

Products In Insider Risk Management Solutions Market

Filter By: Company Size Industry Region

<50M USD | 50M-1B USD | 1B-10B USD | 10B+ USD | Gov't/PS/Ed

Products 1 - 20 | View by Vendor Review weighting Reviewed in Last 12 Months Number of Ratings,

4.9 ★★★★★ 208 Ratings

5 Star 88%
4 Star 12%
3 Star 0%
2 Star 0%
1 Star 0%

Varonis Data Security Platform
by Varonis

"Dare to protect your data the right way"

Varonis provides the visual aid absolutely needed in order to understand (and fix / fine-tune / maintain) completely how users are provisioned access across the domain. Add data classification ...

Read Reviews

Competitors and Alte
Varonis vs Microsoft
Varonis vs LogRhythr
Varonis vs Rapid7
See All Alternatives

4.9 ★★★★★ 53 Ratings

5 Star 85%

INCYDR

Incydr
by Code42

Competitors and Alte
Code42 vs Microsoft

visibility and reporting with activity on our endpoints. For example, ...

Read Reviews

4.2 ★★★★☆ 50 Ratings

5 Star 28%
4 Star 66%
3 Star 4%
2 Star 2%
1 Star 0%

Advanced Threat Analytics (ATA)

by Microsoft

"ATA Review"

ATA is a great product to give you analytic insights into your organization. I love how it analyzes user logins and computer access. It is helpful to be able to see suspicious activity on your network and ...

Read Reviews

Competitors and Alte

Microsoft vs Forcepo
Microsoft vs Rapid7
Microsoft vs IBM

See All Alternatives

4.5 ★★★★½ 24 Ratings

5 Star 54%
4 Star 46%
3 Star 0%
2 Star 0%
1 Star 0%

InsightIDR

by Rapid7

"Excellent SIEM solution for in-house team"

InsightIDR has enabled us to bring the management of SIEM in-house with an easy to deploy and use product that we have full confidence in. The Rapid7 team were great throughout the entire process providing ...

Read Reviews

Competitors and Alte

Rapid7 vs LogRhythn
Rapid7 vs Microsoft
Rapid7 vs Varonis

See All Alternatives

4.3 ★★★★☆ 22 Ratings

5 Star 41%
4 Star 55%
3 Star 5%
2 Star 0%
1 Star 0%

Proofpoint Insider Threat Management

by Proofpoint

"ObserveIT, unobtrusive and discreet monitoring tool."

The solution scales well whether you are gearing up for a massive corporation or a smaller business. Deployment seemed to be very straight forward but I was not directly involved in it and am relying on ...

Read Reviews

Competitors and Alte

Proofpoint vs Micros
Proofpoint vs Forcep
Proofpoint vs Varonis

See All Alternatives

4.3 ★★★★☆ 18 Ratings

Quest Change Auditor for Active Directory

by Quest

Competitors and Alte

by Quest

5 Star 50%
4 Star 44%
3 Star 0%
2 Star 0%
1 Star 6%

"Change Auditor an essential tool for Active Directory Administrators"

My team uses Change Auditor weekly to help troubleshoot and resolve issues. The interface isn't fancy, but it does the job without throwing a bunch of stuff at you that you don't need. We routinely use it to ...

Read Reviews

Competitors and Alte

Quest vs Microsoft
Quest vs Proofpoint
Quest vs Varonis

See All Alternatives

4.5 ★★★★½ 14 Ratings

5 Star 50%
4 Star 36%
3 Star 14%
2 Star 0%
1 Star 0%

Securonix User and Entity Behavior Analytics (UEBA)

by Securonix

"Extremely knowledgable, pro-active and responsive"

The Securonix Team is very knowledgeable about Insider Threat principles and how to mitigate threats using their application. They are very pro-active and responsive to system problems and enhancing ...

Read Reviews

Competitors and Alte

Securonix vs Gurucu
Securonix vs Forcepo
Securonix vs LogRhy

See All Alternatives

---

5 ★★★★★ 12 Ratings

5 Star 100%
4 Star 0%
3 Star 0%
2 Star 0%
1 Star 0%

Micro Focus ArcSight Intelligence

by Micro Focus

"Efficient combination of Unsupervised machine learning and advanced correlation !!"

Best UEBA solution with true unsupervised Machine learning which can scale up as needed, best part is with out any human intervention we will get the risk profiling of the whole organization entities. We have ...

Read Reviews

Competitors and Alte

Micro Focus vs Secu
Micro Focus vs IBM
Micro Focus vs Micro

See All Alternatives

4.6 ★★★★½ 12 Ratings

5 Star 58%
4 Star 42%

DTEX InTERCEPT Workforce Cyber Security Platform

by Dtex Systems

"Strong solution for Insider Threat monitoring, detection and response"

Competitors and Alte

Dtex Systems vs Mic
Dtex Systems vs Proo

Read Reviews

4.7 ★★★★★ 11 Ratings

5 Star 55%
4 Star 45%
3 Star 0%
2 Star 0%
1 Star 0%

LogRhythm UEBA

by LogRhythm

"Amazing cybersecurity with the ability to solve your threats"

We've been using LogRhythm for nearly 2 years now and its just perfect for us. The ability to identify threats and giving you a solution on how to fix it for a minimum price, we had problems with cybersecurity that ...

Read Reviews

Competitors and Alte

LogRhythm vs IBM
LogRhythm vs Secur
LogRhythm vs Micros

See All Alternatives

3.9 ★★★★☆ 8 Ratings

5 Star 25%
4 Star 63%
3 Star 0%
2 Star 13%
1 Star 0%

QRadar User Behavior Analytics

by IBM

"Clean, solid, customizable and easily understood. Except when it finds something bad."

Solid product with a good level of integration to other tools. It can be a bit difficult to understand at times and produces a good amount of false positives so it needs constant tuning. Good product in general and ...

Read Reviews

Competitors and Alte

IBM vs Microsoft
IBM vs Proofpoint
IBM vs Forcepoint

See All Alternatives

5 ★★★★★ 7 Ratings

5 Star 100%
4 Star 0%
3 Star 0%
2 Star 0%
1 Star 0%

ActivTrak

by ActivTrak

"Try it. You will not be disappointed!"

Overall, our experience with ActivTrak has been great. The product is not cost prohibitive and has provides great information and tracking resources both when we were working from home and when we ...

Read Reviews

Competitors and Alte

ActivTrak vs Microsof
ActivTrak vs Teramin
ActivTrak vs Veriato

See All Alternatives

Elevate Platform

3 Star 0%
2 Star 0%
1 Star 0%

Using Elevate security Phishing simulator platform Reflex, we were able to mock a company-wide phishing campaign. Their team is easy to work with and can customize the products to suit the needs of our ...

Read Reviews

currently unavailable

See All Alternatives

4.8 ★★★★★ 3 Ratings

5 Star 33%
4 Star 67%
3 Star 0%
2 Star 0%
1 Star 0%

Gurucul Risk Analytics (GRA)

by Gurucul

"Fantastic Vendor to work with "

The vendor partners with us to enhance our capabilities and innovate our IAM roadmap. They are invested in forming a great partnership by always listening to feedback and improving our experience and our ...

Read Reviews

Competitors and Alte

Gurucul vs Securonix
Gurucul vs LogRhyth
Gurucul vs Veriato

See All Alternatives

2.8 ★★★☆☆ 3 Ratings

5 Star 0%
4 Star 33%
3 Star 0%
2 Star 67%
1 Star 0%

Recon (Legacy)

by Veriato

"Poweful tool, but not easy to use. Support can be sluggish and can't always solve issues."

Veriato captures everything, which is great. The Dashboard used to access the data, on the other hand, is not so great. It's confusing and takes quite a bit of practice to get used to.

Read Reviews

Competitors and Alte

Competitor or alternativ currently unavailable

See All Alternatives

---

4 ★★★★☆ 2 Ratings

5 Star 0%
4 Star 100%
3 Star 0%
2 Star 0%
1 Star 0%

Bottomline Technologies User Behavior Monitoring (Legacy)

by Bottomline Technologies

"Good solution but needs some maturity"

overall partnership good, maturity of product below expectations, still several project scope items TBD as we are still in phase 1

Read Reviews

Competitors and Alte

Bottomline Technolo

See All Alternatives

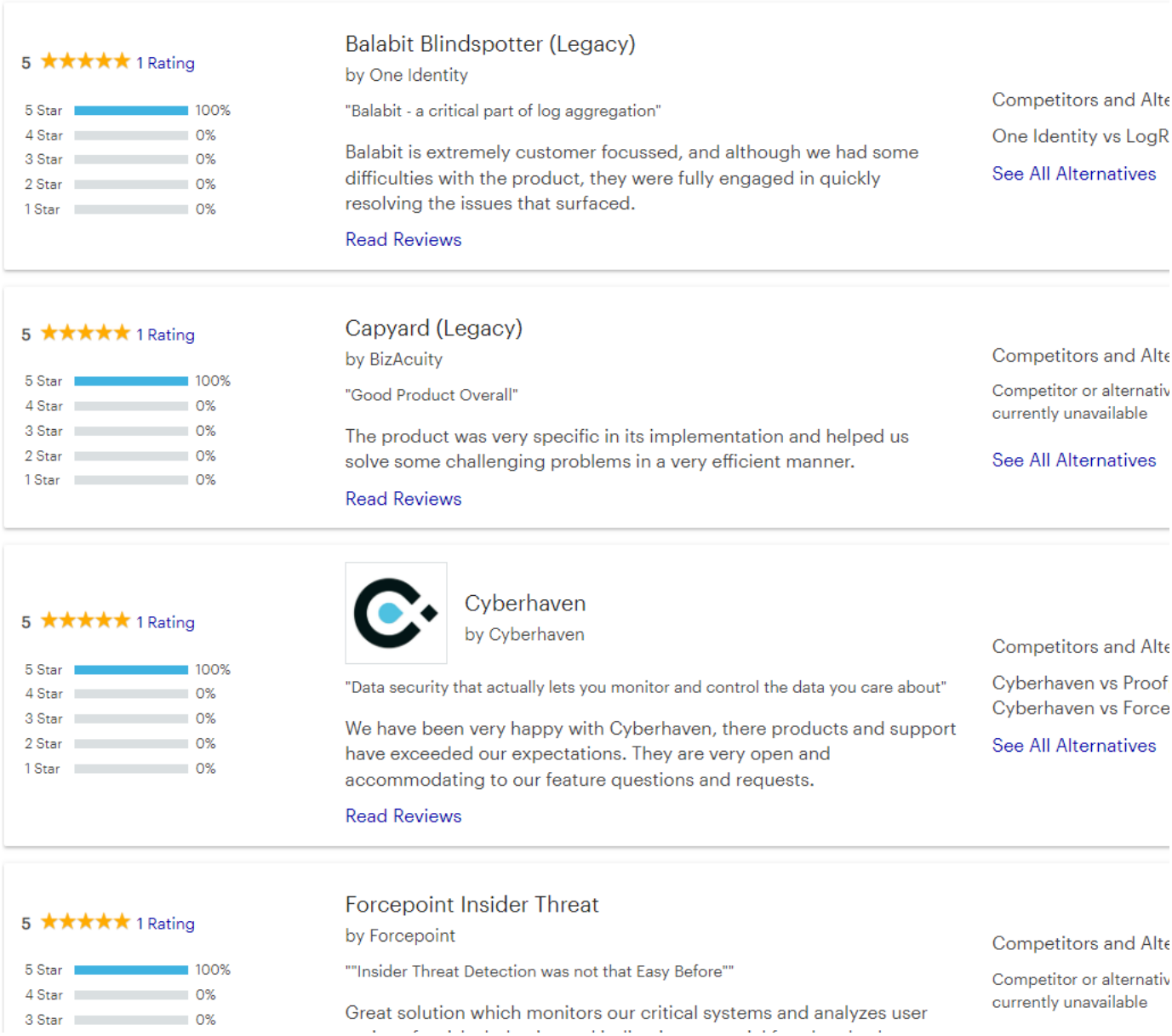


Imagem 1. Levantamento anual de solução UEBA realizado pelo Gartner.

Definição: Conjunto de tecnologias e técnicas de inspeção usadas para classificar o conteúdo de informações contido em um objeto – como um arquivo, e-mail, pacote, aplicativo ou armazenamento de dados – enquanto em repouso (em armazenamento), em uso (durante uma operação) ou em trânsito (através de uma rede). As ferramentas de análise comportamento de usuário também têm a capacidade de aplicar dinamicamente uma política — como registrar, relatar, classificar, realocar, marcar e criptografar — e/ou aplicar proteções de gerenciamento de direitos de dados corporativos.

4.7.3. O Gartner avalia soluções de análise comportamento de usuário que fornecem visibilidade do uso de dados em uma organização para um amplo conjunto de casos de uso e a aplicação dinâmica de políticas com base no conteúdo e contexto no momento de uma operação, abordando ameaças relacionadas a dados, incluindo os riscos de perda de dados inadvertida ou acidental, e a exposição de dados confidenciais usando monitoramento, filtragem, bloqueio e outros recursos de correção.

4.7.4. O estudo abaixo relaciona as alternativas existentes no mercado que se enquadram nas necessidades/benefícios elencadas pela Instituição

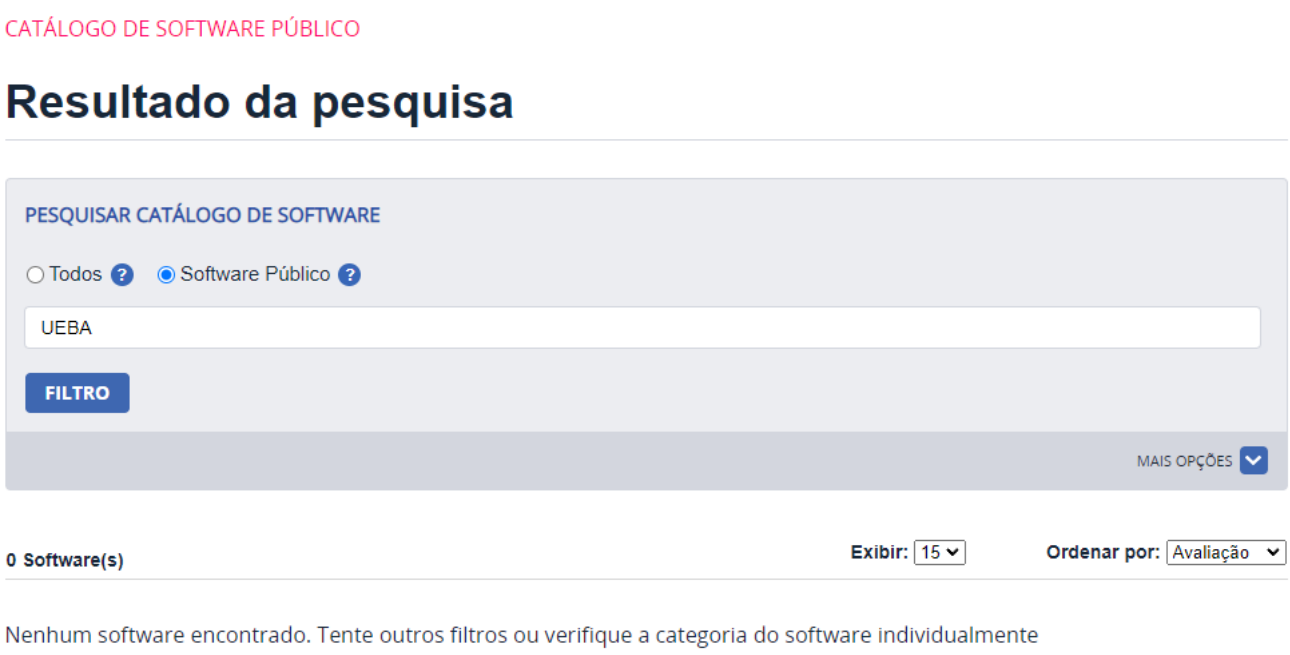
ESTUDO DE MERCADO	
Solução para Investigação e Prevenção Contra Ameaças	**SYMANTEC** • Proteção voltada para identidades do ambiente; • Monitoramento de malware e artefatos maliciosos espalhados através de e-mail; • Proteção dos dados contra vazamento ou roubo, com monitoramento externo; • Ampliação do alcance dos recursos de prevenção contra ataques monitoramento de pessoas; • Ambiente de testes para recriação e teste de ataques e artefatos maliciosos; • Auditoria para ambiente de mensageria; • Licenciamento por usuário e funcionalidade.
	TREND MICRO

	• Monitoramento de diversos dispositivos e ativos; • Recriação da cadeia de ataque; • Gerenciamento de direitos digitais com reconhecimento de conteúdo integrado; • Análise de ambiente e aprendizado automático para evidenciação de ameaças; • Detecção e resposta de comportamentos maliciosos nos dispositivos monitorados; • Diversos módulos necessários licenciados a parte.
	VARONIS • Auditoria e monitoramento de dados e identidades; • Mapeamento das estruturas e permissões das pastas e arquivos • Implementação de análise de comportamento de usuário baseado na auditoria coletada; • Criação e atualização automática de base de alertas conhecidamente maliciosos; • Resposta automática de contra alertas de comportamento maliciosos • Descobrir, identificar, classificar, indexar arquivos não estruturados a padrões como PII, PCI, SOX, GLBA e LGPD • Apresentação de métricas sobre conformidade e segurança dos dados; • Licenciamento por usuário, aderente a necessidade atual.

Tabela 9 – Estudo de Mercado.

4.7.5. **Da existência de software público brasileiro**

4.7.5.1. De acordo com a busca realizada no dia 20 de Janeiro de 2022, às 14:45, com as palavras chaves "Auditoria e segurança de dados não estruturados", o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.



CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

○ Todos ? ◉ Software Público ?

file system analysis

FILTRO

MAIS OPÇÕES

0 Software(s) **Exibir:** 15 **Ordenar por:** Avaliação

Nenhum software encontrado. Tente outros filtros ou verifique a categoria do software individualmente

CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

○ Todos ? ◉ Software Público ?

Análise de comportamento de usuários e entidades

FILTRO

MAIS OPÇÕES

14 Software(s) **Exibir:** 15 **Ordenar por:** Avaliação

★★★★★

Desde:
27 de Abril de 2012

tcn - Tucunaré

Desenvolvido para facilitar a instalação e configurações do sistema operacional em computadores desktop e Telecentros.

Categorias de Software: Administração Pesquisa e Desenvolvimento Educação

★★★★★

Desde:
19 de Outubro de 2011

SAELE

Sistema aberto de eleições eletrônicas que visa agilizar e melhorar o processo eleitoral em universidades.

Categorias de Software: Educação

Desde:
7 de Agosto de 2007

i3Geo

Interface integrada para internet de ferramentas de geoprocessamento

Categorias de Software: Comércio e Serviços Comunicações Energia Transportes Habitação Indústria Meio Ambiente Pesquisa e Desenvolvimento Saneamento Saúde Educação Agropecuária, Pesca e Extrativismo

---

Desde:
5 de Março de 2009

Amadeus LMS

Sistema de gestão de aprendizagem para educação a distância.

Categorias de Software: Educação

Desde:
20 de Janeiro de 2014

Citsmart ITSM Community

Ferramenta Web de Gerenciamento de Serviços de TI baseada nas melhores práticas da Biblioteca ITIL.

Categorias de Software: Administração Comunicações Energia Indústria Segurança e Ordem Pública Trabalho Saúde Software Educação Infraestrutura e Fomento Planejamento e Gestão

---

Desde:
28 de Abril de 2010

EducatuX

O aluno desenvolve habilidades jogando e a família e escola podem acompanhar seu desempenho através de centenas de ap

Categorias de Software: Educação

Guarux

Desde:
23 de Abril de 2013

Guarux é um sistema operacional baseado em software livre (Linux) voltada à educação especial.

Categorias de Software: Educação

Desde:
29 de Setembro de 2008

i-Educar

Modernize o processo de gestão escolar com o i-Educar.

Categorias de Software: Educação

Desde:
9 de Outubro de 2009

e-Cidade

O e-cidade destina-se a informatizar a gestão dos municípios brasileiros de forma integrada.

Categorias de Software: Administração Economia e Finanças Saúde Educação

---

Desde:
11 de Junho de 2010

EdiTom

Software de edição de partituras que permitindo que iniciantes possam ter uma ferramenta para criar sons.

Categorias de Software: Esporte e Lazer Educação

Desde:
17 de Junho de 2009

Linux Educacional

Imagem 2. Pesquisa de solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados (UEBA) no portal de software público.

4.7.5.2. Após análise dos resultados acima, verificou-se que nenhum software corresponde às especificações da solução proposta.

4.8. **Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública**

ID	SOLUÇÃO	ORGÃO/UNIDADE	Nº PREGÃO	UASG/UNIDADE
01	Escolha da proposta mais vantajosa para a contratação solução integrada de segurança para estação de trabalho e servidores em ambiente corporativo de acordo com as especificações, registro de preços, conforme condições, quantidades e exigências estabelecidas neste Edital e nos anexos.	TRIBUNAL SUPERIOR DO TRABALHO	58/2021	250110 COORDENAÇÃO GERAL DE MATERIAL E PATRIMÔNIO
02	Contratação de empresa para fornecimento e implantação de solução de auditoria e governança, baseado em software, para ambiente de diretórios de usuários, servidores de arquivos, monitoramento e prevenção de ameaças internas, identificação e classificação de informações sensíveis e busca de informação não estruturada corporativa, contemplando execução de serviços de apoio pós-implantação, de acordo com as especificações técnicas, condições, quantidades e exigências estabelecidas no Edital e seus anexos do Pregão em referência.	ESTADO DO ALAGOAS	05/2021	925473 TRIBUNAL DE CONTAS DO ESTADO DO ALAGOAS

Tabela 10 - Análise de Projetos Similares.

4.8.1. As soluções adquiridas em contratações recentes da Administração Pública utilizados como referência, possuem configurações aproximadas ou similares a aquisição pretendida pela Funasa. Portanto a contratação pode ser caracterizada como bem comum, pois as padronizações de suas configurações são comumente encontradas no mercado e em contrações da Administração Pública.

4.8.2. A tabela a seguir apresenta a análise quanto as políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis:

Requisito	Entidade	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1, 2	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1, 2		X	
A capacidade e alternativas do mercado, inclusive existência de software livre ou software público?	1, 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1, 2	X		
A Solução é aderente às regulamentações da ICP-Brasil? (Quando houver necessidade de certificação digital)	1, 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?	1, 2	X		
A Solução é aderente às necessidades técnicas do órgão?	1, 2	X		
A análise de projetos similares foi utilizada para realização do orçamento estimado?	1, 2	X		

Tabela 11 - Análise das Alternativas Existentes.

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. A **Solução de Id. 1** compreende o uso de solução baseada em software livre. Devido à falta de suporte técnico especializado, possuir código fonte, ausência de garantias e necessidade de composição com vários produtos para entrega aproximada da necessidade, fica evidente que esta solução não atenderia as necessidades da Funasa.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1. Bens e serviços que compõem a solução

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de segurança, auditoria e prevenção de ameaças	Contas do AD	3190
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	Serviço	1
3	Treinamento para 5 participantes	Turma	1

Tabela 12 - Bens e serviços que compõem a solução.

6.2. Justificativa da solução escolhida

6.3. A solução a ser contratada é a de **Id 02** que compreende a contratação de nova solução de mercado compreendendo a contratação de empresa especializada no fornecimento de Solução de Segurança, Auditoria e Governança, contemplando instalação, treinamento e garantia da proteção dos dados da Fundação Nacional de Saúde por 12 meses.

6.4. Como visto no estudo de mercado, não há um único produto de *software* que atenda sozinho todos os requisitos para a solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*. Sendo assim, a melhor forma de aquisição é a contratação de uma solução e não um produto específico. Essa solução será formada por dois ou mais produtos de *software* e caberá a uma empresa integradora de TIC, especializada em segurança da informação, ofertar, em processo licitatório, o melhor conjunto de produtos de *softwares* que estejam em acordo com o especificado no Termo de Referência

6.5. Através da referida contratação será possível atender as necessidades da Funasa, com ganho em qualidade e eficiência, além de prover o atendimento aos requisitos de segurança da informação, garantindo a disponibilidade e continuidade dos serviços de TI, bem como para atender às constantes evoluções dos recursos de TIC, desse modo, a contratação da solução escolhida irá fornecer o suporte adequado às necessidades do negócio desta FUNASA, que necessita de soluções de segurança que sejam proativas e inteligentes, buscando preservar um dos maiores ativos existentes atualmente nas organizações que é a informação.

6.6. A solução deverá ser adquirida pelo modelo de subscrição, no qual o direito de uso das licenças e a sua garantia e suporte são adquiridos como serviço por período (no caso em tela, 12 meses), considerando que o modelo de subscrição é mais abrangente, favorecendo a ampla concorrência.

6.7. A contratação será abordada com ampla concorrência de mercado e menor preço global, auferindo a proposta com o valor mais vantajoso para a administração, desde que atendam aos requisitos mínimos tecnológicos elencados no termo de referência.

7. ESTIMATIVA DE VOLUME DA DEMANDA

7.1. Item 1 - Aquisição de licenças de software de solução de segurança, auditoria e prevenção de ameaças

7.1.1. Atualmente há uma média de 3.034 contas ativas, e considerando as mudanças passíveis de ocorrem no cenário da Funasa e Superintendências Estaduais - SUEST's, no quadro de pessoal da Fundação, abarcando os servidores da casa, os terceirizados e estagiários, é necessária uma margem de segurança no quantitativo estimado. Deste modo, foi adicionada uma margem de 5% ao quantitativo mencionado (totalizando 3190).

7.1.2. Portanto, considerando que a solução pretendida possui seu licenciamento baseado em usuários que acessam o ambiente, o volume de licenciamento estimado para o item 1 é de **3190 licenças**.

7.2. Item 3 - Treinamento

7.2.1. O quantitativo do item 3 foi estimado em 1 Turma (de 5 participantes), com base no número de Técnicos da Funasa atualmente lotados na Coordenação Geral de Modernização e Tecnologia da Informação - CGMTI que possuem conhecimento das normas de Segurança da Informação da Fundação. Desta forma, para fins de formação da estimativa de custos, a pesquisa de preços para o item 3 (treinamento) foi realizada considerando o valor unitário por participante, para consolidação do valor final total para 1 turma de 5 participantes.

8. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

8.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

8.1.1. Para construção do TCO de cada um dos itens foi levado em consideração os seguintes itens:

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de segurança, auditoria e prevenção de ameaças	Contas do AD	3190
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	Serviço	1
3	Treinamento para 5 participantes	Turma	1

Tabela 13 - Itens considerados para construção do TCO.

8.2. CUSTO TOTAL DE PROPRIEDADE

8.2.1. Para realização deste TCO, realizou-se pesquisa de preço seguindo as orientações contidas na INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020, 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.

8.2.2. A pesquisa traz em sua cesta de preços valores nos parâmetro I, II e IV, conforme tabela a seguir. O detalhamento da pesquisa de preços consta da Nota Técnica (SEI nº 3990962).

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite (Média
1	Solução de segurança, auditoria e prevenção de ameaças	I	PREGÃO 05/2021 - TCE-AL	R$ 568,00	R$ 1.889,80	670,56	2.5
		II	PREGÃO 58/2021 - TST	R$ 2.121,00			
		IV	FORNECEDOR 1 - OMTV	R$ 2.437,84			
		IV	FORNECEDOR 2 - NTSEC	R$ 2.168,42			
		IV	FORNECEDOR 3 - ARVVO	R$ 2.153,75			
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	II	PREGÃO 58/2021 - TST	R$ 95.000,00	R$ 111.131,25	14.208,86	125.
		IV	FORNECEDOR 1 - OMTV	R$ 99.891,00			
		IV	FORNECEDOR 2 - NTSEC	R$ 129.634,00			
		IV	FORNECEDOR 3 - ARVVO	R$ 120.000,00			
3	Treinamento para 5 participantes	II	PREGÃO 58/2021 - TST	R$ 2.900,00	R$ 8.369,61	4.420,58	12.7
		IV	FORNECEDOR 1 - OMTV	R$ 6.999,23			
		IV	FORNECEDOR 2 - NTSEC	R$ 15.179,20			
		IV	FORNECEDOR 3 - ARVVO	R$ 8.400,00			

Tabela 14 - Preços coletados para os itens.

8.2.3. Após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta pelos seguintes valores considerados aceitáveis:

8.2.3.1. ANÁLISE DOS PREÇOS COLETADOS PARA O ITEM 1

8.2.3.2. Para o item 1, a pesquisa traz em sua cesta de preços 05 (cinco) valores, sendo 1 (um) no parâmetro I (painel de preços), 1 (um) no parâmetro II (contratações similares de outros entes públicos) e 03 (três) no parâmetro IV (fornecedores). Dessa forma, após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 4 (quatro) valores considerados aceitáveis.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Me
1	Solução de segurança, auditoria e prevenção de ameaças	II	PREGÃO 58/2021 - TST	R$ 2.121,00	R$ 2.220,25	R$ 2
		IV	FORNECEDOR 1 - OMTV	R$ 2.437,84		
		IV	FORNECEDOR 2 - NTSEC	R$ 2.168,42		
		IV	FORNECEDOR 3 - ARVVO	R$ 2.153,75		

Tabela 15 - Preços aceitáveis para o item 1.

8.2.3.3. ANÁLISE DOS PREÇOS COLETADOS PARA O ITEM 2

8.2.3.4. Para o item 2, a pesquisa traz em sua cesta de preços 04 (quatro) valores, sendo 1 (um) no parâmetro II e 3 (três) no parâmetro IV (Tabela 16). Dessa forma, após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 2 (dois) valores considerados aceitáveis.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Mediana	Menor Preço	Desv.Padr
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	IV	FORNECEDOR 1 - OMTV	R$ 99.891,00	R$ 109.945,50	R$ 109.945,50	R$ 99.891,00	10.054,5
		IV	FORNECEDOR 3 - ARVVO	R$ 120.000,00				

Tabela 16 - Preços aceitáveis para o item 2.

8.2.3.5. Desse modo, considerando que para a definição do indicador a ser adotado para utilização do preço de referência o cálculo deve incidir sobre um conjunto de três ou mais preços, utilizou-se como parâmetro a média dos 4 (quatro) preços coletados para o item 2, conforme discriminado na tabela a seguir.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite Superior (Média + Desvio)	Limite Inferi (Média -Desv
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	II	PREGÃO 58/2021 - TST	R$ 95.000,00	**R$ 111.131,25**	14.208,86	125.340,11	96.922,39
		IV	FORNECEDOR 1 - OMTV	R$ 99.891,00				
		IV	FORNECEDOR 2 - NTSEC	R$ 129.634,00				
		IV	FORNECEDOR 3 - ARVVO	R$ 120.000,00				

Tabela 17 - Média dos preços coletados para o item 2.

8.2.3.6. **ANÁLISE DOS PREÇOS COLETADOS PARA O ITEM 3**

8.2.3.7. A pesquisa de preços para o item 3 (treinamento) foi realizada **considerando o valor unitário por participante**, para consolidação do valor final para 1 turma de 5 participantes.

8.2.3.8. O valor do Pregão 58/2021 - TST (que correspondente ao item 3) apresenta um valor total para treinamento de 1 turma de até 10 participantes, desta forma, o valor total foi dividido por 10 para chegar ao valor unitário por participante. Já as propostas dos fornecedores apresentam o valor total para treinamento de 1 turma de até 5 pessoas, desse modo, o valor total foi dividido por 5 para chegar ao valor unitário por participante.

8.2.3.9. A pesquisa traz em sua cesta de preços 04 (quatro) valores, sendo 1 (um) no parâmetro II e 3 (três) no parâmetro IV. Dessa forma, após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 2 (dois) valores considerados aceitáveis.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Mediana	Menor Preço	Desv.Padr
3	Treinamento para 5 participantes	II	FORNECEDOR 1 - OMTV	R$ 6.999,23	R$ 7.699,62	R$ 7.699,62	R$ 6.999,23	700,39
		IV	FORNECEDOR 3 - ARVVO	R$ 8.400,00				

Tabela 18 - Preços aceitáveis para o item 3.

8.2.3.10. Considerando que para a definição do indicador a ser adotado para utilização do preço de referência o cálculo deve incidir sobre um conjunto de três ou mais preços, utilizou-se como parâmetro a média dos 4 (quatro) preços coletados para o item 2, conforme discriminado na tabela a seguir.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite Superior (Média + Desvio)	Limite Inferio (Média -Desvi
3	Treinamento para 5 participantes	II	PREGÃO 58/2021 - TST	R$ 2.900,00	R$ 8.369,61	4.420,58	12.790,18	3.949,03
		IV	FORNECEDOR 1 - OMTV	R$ 6.999,23				
		IV	FORNECEDOR 2 - NTSEC	R$ 15.179,20				
		IV	FORNECEDOR 3 - ARVVO	R$ 8.400,00				

Tabela 19 - Média dos preços coletados para o item 3.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

9.1. Com base em pesquisa elaborada de acordo com a INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020, 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, o custo total da contratação foi estimado em **R$ 7.235.576,80 (sete milhões, duzentos e trinta e cinco mil quinhentos e setenta e seis reais e oitenta centavos)** na forma como segue:

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de segurança, auditoria e prevenção de ameaças	3190	R$ 2.220,25	R$ 7.082.597,50
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	1	R$ 111.131,25	R$ 111.131,25
3	Treinamento para 5 participantes	5	R$ 8.369,61	R$ 41.848,05
Custo Estimado Total				**R$ 7.235.576,80**

Tabela 20 - Custo Estimado Total da Contratação.

9.2. O detalhamento da pesquisa de preços encontra-se na Nota Técnica de Elaboração de Pesquisa de Preços (SEI nº 3990962).

10. BENEFÍCIOS ESPERADOS

10.1. Os benefícios a serem alcançados com a pretensa contratação estão elencados no item 3.1.5 deste Estudo Técnico.

11. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

Não se aplica

12. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

12.1. Recursos Materiais

12.1.1. Os equipamentos e materiais utilizados, bem como a prestação dos serviços deverão estar rigorosamente dentro das normas vigentes e das especificações estabelecidas pela FUNASA, sendo que a inobservância desta condição implicará a sua recusa, bem como a sua devida adequação/substituição, sem que caiba à CONTRATADA qualquer tipo de reclamação ou indenização.

12.2. Recursos Humanos

12.2.1. O modelo de prestação de serviços prevê que a CONTRATADA seja integralmente responsável pela gestão de seu pessoal em todos os aspectos, sendo vedado à equipe da FUNASA, formal ou informalmente, qualquer tipo de ingerência ou influência sobre a administração da mesma, ou comando direto sobre seus empregados, fixando toda negociação na pessoa do preposto da CONTRATADA ou seu substituto.

12.2.2. Neste sentido, se torna indispensável a transferência de conhecimento à equipe técnica da FUNASA de todos os novos procedimentos e/ou serviços implantados ou modificados pela CONTRATADA, mediante documentação técnica em repositório adotado pela Fundação para esse fim, dando plena capacidade ao mesmo de acompanhar, executar e gerenciar os serviços contratados em caso de descontinuidade do contrato.

13. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

13.1. Requisitos de Continuidade Contratual

13.1.1. Haver falhas na legislação aplicada ou nas especificações/qualidade da solução:

13.1.1.1. **Ações de Contingência e seus respectivos responsáveis:** Ter certeza que a equipe de planejamento tenha capacidade e conhecimento do assunto técnico, bem como da parte administrativa e jurídica, estando tudo isso transcrito nos documentos – Equipe de Planejamento.

13.1.2. Questões Relacionadas a Defeitos e Reparações

13.1.2.1. **Ações de Contingência e seus respectivos responsáveis:** Caso a empresa CONTRATADA não providencie a troca ou reparação de algum produto com defeito, haverá a aplicação de advertência, multa, notificação, sanções, abatimento das custas do depósito em garantia. O custo do retrabalho dos serviços ocorrerá a expensas da empresa, o que poderá ser cobrado judicialmente– Comissão executora.

13.1.3. Serviço de Manutenção Fora do Prazo

13.1.3.1. **Ações de Contingência e seus respectivos responsáveis:** Caso a empresa CONTRATADA não providencie a instalação e/ou a manutenção em um prazo hábil estipulado, causando prejuízo ao Erário, haverá aplicação de advertência, multa, notificação, sanções, abatimento das custas do depósito em garantia – Comissão executora.

13.1.4. Garantia de Qualificação Econômico-Financeira

13.1.4.1. **Ações de Contingência e seus respectivos responsáveis:** A empresa CONTRATADA deverá apresentar qualificação econômico-financeira que minimize ocorrência do risco de insubsistência da empresa – Setor de compras.

13.2. Continuidade do fornecimento da solução de tecnologia da informação em eventual interrupção contratual

13.2.1. A futura transição contratual decorrente de nova contratação para o mesmo objeto e a eventual interrupção do contrato por qualquer motivo são riscos inerentes a pretendida contratação, para os quais concorrem como ações planejadas para favorecer a continuidade dos serviços, reduzir os impactos e prover maior segurança institucional;

13.2.2. A empresa CONTRATADA deverá apresentar, sempre que solicitado pela FUNASA, qualificação econômico-financeira que minimize o risco de insubsistência da mesma;

13.2.3. Também com o intuito de minimizar os impactos no caso de insubsistência/falência da CONTRATADA, todo material ou produto da FUNASA mantido, produzido ou atualizado pela CONTRATADA deverá estar sob total controle da Fundação;

13.2.4. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato;

13.2.5. A empresa CONTRATADA repassará à FUNASA, todo o conhecimento técnico e capacitação necessária para a manutenção e suporte técnico, visando manter a solução em funcionamento em caso de interrupção por transição contratual ou outro motivo, o termo de Direito de Propriedade Intelectual da FUNASA no que concerne à parte de customização desenvolvida com base nas definições de requisitos próprios da Fundação;

13.2.6. A CONTRATADA devolverá os recursos disponibilizados, terá os perfis que lhe foram atribuídos revogados, bem como a eliminação das caixas postais de correio eletrônico caso seja necessário.

13.3. Atividades de transição contratual e encerramento do contrato

13.3.1. A empresa CONTRATADA deverá apresentar periodicamente, qualificação econômico-financeira que minimize ocorrência do risco de insubsistência da empresa;

13.3.2. Em caso de venda da empresa CONTRATADA ou incorporação por novos controladores, a empresa CONTRATADA deverá assegurar a CONTRATANTE, mediante cláusula contratual, transferência de todas as obrigações contratuais ao sucessor;

13.3.3. No caso de interrupção contratual a empresa deverá devolver todos os equipamentos encontrados em sua posse. A CONTRATANTE poderá rescindir o contrato por razões supervenientes, assegurados os direitos da CONTRATADA. Nesse caso, a CONTRATANTE comunicará à CONTRATADA com antecedência de 90 (noventa) dias do término do contrato para que ela elabore o Plano de Transição e realize a passagem do contrato. Neste caso, a CONTRATADA deverá devolver os equipamentos encontrados em sua posse reparados e os serviços abertos do momento da comunicação de rescisão do contrato e não finalizadas devem ser finalizadas antes do término do contrato. Especialmente no encerramento do contrato, a Área Administrativa deverá assegurar-se da adequada liquidação de todas as obrigações contratuais.

13.3.4. A CONTRATADA deve devolver todos os recursos de propriedade da CONTRATANTE, tais como:

- Licenças de softwares;
- Manuais e documentos, classificados ou que devam permanecer com a CONTRATANTE.

13.4. A estratégia de independência da CONTRATANTE com relação à CONTRATADA

13.4.1. A estratégia de independência tem como garantia o Termo de Recebimento Provisório, o qual deverá ser assinado pelos respectivos fiscais técnico e requisitante, e o Termo de Recebimento Definitivo, o qual deverá ser assinado pelo fiscal requisitante e pelo Gestor, que irá subsidiar a emissão do Termo de

Encerramento do Contrato

13.5. **Transferência de conhecimento**

13.5.1. A transferência de conhecimento deve ser ofertada à equipe técnica da FUNASA, precisamente à equipe técnica da Informática. A referida transferência compreende, necessariamente, demonstração prática de cada funcionalidade dos equipamentos/produtos adquiridos, informações técnicas, em plena compatibilidade com o ambiente computacional da FUNASA e em conformidade com a proposta técnica previamente apresentada no Plano Executivo.

13.6. **Direitos de propriedade intelectual (LEI Nº. 9.610/1998)**

13.6.1. Os direitos de propriedade intelectual do software e projetos não necessitam ser transferidos ao contratante por tratar-se de solução proprietária e produtos de uso exclusivo para esta solução;

13.6.2. Entretanto, a entrega deverá incluir a licença de uso de todo o software fornecido para operacionalização do equipamento durante todo o seu período de atividade, independentemente da expiração da garantia e do contrato.

14. APROVAÇÃO E ASSINATURAS

14.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 5355, de 19 de outubro de 2022 (SEI nº 4185763).

14.2. Conforme o §2º do Art. 11 da IN SGD/ME nº 1, de 2019, o Estudo Técnico Preliminar da Contratação será aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

Integrante Requisitante	Integrante Técnico
André Wilson Pimenta Santana Coordenador-Geral de Modernização e de Tecnologia da Informação SIAPE: 1.347.001	**Gleicy Kellen dos Santos Faustino** Coordenador de Sistemas e Inovações SIAPE: 1.320.942

Tabela 21 - Equipe de Planejamento da Contratação.

14.3. **Aprovação da Autoridade Máxima da Área de TIC**

14.3.1. Conforme o §3º do Art. 11 da IN SGD/ME nº 1, de 2019, caso a autoridade máxima da Área de TIC venha a compor a Equipe de Planejamento da Contratação, a autoridade que assinará o Estudo Técnico Preliminar da Contratação será aquela superior à autoridade máxima da Área de TIC.

Autoridade Máxima da Área de TIC
ALAN OLIVEIRA LIMA Diretor do Departamento de Administração SIAPE 3.278.934

Tabela 22 - Autoridade Máxima da Área de TIC.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Integrante Requisitante**, em 19/10/2022, às 17:52, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gleicy Kellen dos Santos Faustino**, **Integrante Técnico**, em 20/10/2022, às 14:50, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Haroldo Rodrigues da Silva**, **Pregoeiro(a)**, em 20/10/2022, às 15:18, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Alan Oliveira Lima**, **Diretor do Departamento de Administração**, em 20/10/2022, às 16:05, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **3947632** e o código CRC **F3B39504**.