Ministério da Educação
Secretaria Executiva
Subsecretaria de Tecnologia da Informação e Comunicação

Processo de Contratação de Soluções de TIC

Estudo Técnico Preliminar

Instrução Normativa n° 01, de 04 de abril de 2019, Secretaria de Governo Digital

Processo SEI n° 23000.010862/2022-60

Solução de monitoramento de atividades em bancos de dados e mascaramento de dados

Brasília/DF, 26 de setembro de 2022.

Índice

1 Introdução 1

2 Descrição da demanda 2

2.1 Análise do cenário atual 2
2.2 Identificação das necessidades de negócio 3
2.3 Identificação das necessidades tecnológicas 4
2.4 Identificação dos requisitos necessários e suficientes à escolha da solução 8
2.5 Estimativa do volume de bens e/ou serviços da demanda 8
2.6 Alinhamento estratégico da demanda 12

3 Identificação e análise de soluções 12

3.1 Análise comparativa das alternativas para o atendimento da demanda 12

3.1.1 Solução de monitoramento de atividades em bancos de dados 12
3.1.2 Solução de mascaramento e anonimização de dados 15

4 Análise comparativa de custos 15

4.1 Memória de cálculo das soluções viáveis 15

4.1.1 Alternativa B – Contratação de Solução de monitoramento de atividades em bancos de dados 15

4.2 Registro das soluções inviáveis 15

5 Escolha da solução 15

5.1 Composição da solução escolhida 15

5.1.1 Justificativas da escolha da solução 16
5.1.2 Forma de seleção do fornecedor 18
5.1.3 Benefícios identificados 22
5.1.4 Alinhamento legal e normativo 22

5.2 Estimativa do custo total da contratação 24
5.3 Análise de necessidades de adequação do ambiente 24

5.3.1 Identificação de recursos tecnológicos e materiais necessários à execução do objeto 24
5.3.2 Identificação de recursos humanos necessários à execução do objeto 25

5.4 Análise da estratégia de continuidade 25

6 Declaração de viabilidade da contratação 25

7 Aprovação 26

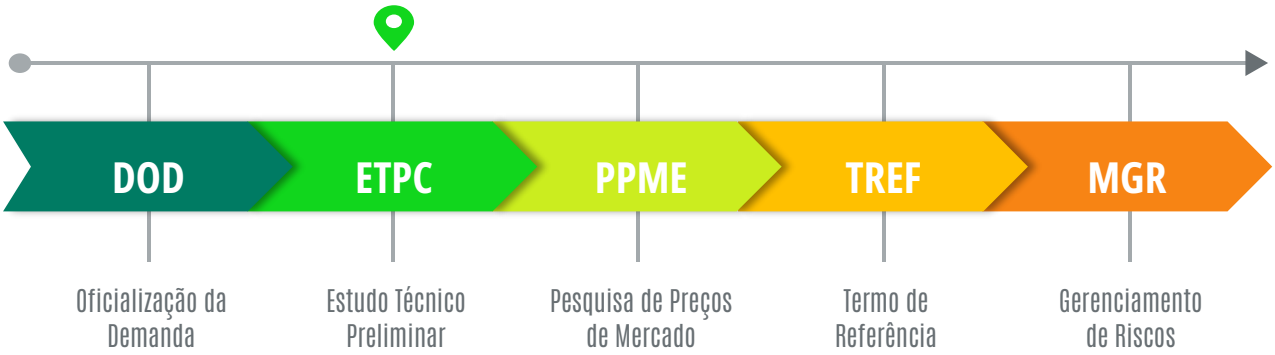
Anexos

APÊNDICE 01 Análise comparativa das alternativas identificadas 27
APÊNDICE 02 Catálogo de Aplicações de Software 28
APÊNDICE 03 Especificação técnica prévia da solução 36
APÊNDICE 04 Resumo da estimativa de preços da contratação 51

1 Introdução

O Estudo Técnico Preliminar da Contratação é o "documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação" – conforme regulamentado pela Instrução Normativa n° 01, de 04 de abril de 2019[1], da Secretaria de Governo Digital do Ministério da Economia (IN-01/2019/SGD/ME).

O processo de planejamento da contratação de soluções de TIC, na forma na IN-01/2019/SGD/ME, é composto pelas seguintes fases:



Na definição apresentada pelo Decreto n° 10.024/2019 (inc. IV do art. 3°), Estudo Técnico Preliminar é o "documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a melhor solução ao problema a ser resolvido e que, na hipótese de conclusão pela viabilidade da contratação, fundamenta o termo de referência".

Em sentido geral, a necessidade de realizar estudos técnicos preliminares, como etapa fundamental do planejamento de uma contratação, decorre antes de tudo dos princípios consagrados no artigo 37 da Constituição Federal:

> *Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...] (BRASIL, 1988).*

Eficiência pode ser entendida como a maximização da capacidade dos recursos disponíveis, isto é, obter o melhor resultado com menos recursos, visando qualificar o gasto público sem se descuidar dos demais princípios constitucionais.

Assim, no presente documento, a EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (EPC) – ora designada pela PORTARIA Nº 26, DE 06 DE MAIO DE 2022 (3295207) – aqui representada por seus integrantes técnico e requisitante, na forma do art. 11 da IN-01/2019/SGD/ME– dedica-se a analisar aspectos fundamentais relacionados à demanda em questão, tais como: adequação técnica; funcionalidades e requisitos; adequação às normas vigentes; modelos de execução; capacidade do mercado; estimativa preliminar de custos e viabilidade econômico-financeira do objeto.

Versionamento

VERSÕES	DESCRIÇÃO	DATA
1.0	Versão preliminar consolidada pela EPC na fase de Planejamento da Contratação	07/10/2021
1.1	Versão preliminar consolidada pela EPC na fase de Planejamento da Contratação	27/04/2022
1.2	Versão preliminar consolidada pela EPC na fase de Planejamento da Contratação	29/04/2022
1.3	Versão preliminar consolidada pela EPC na fase de Planejamento da Contratação (após Pesquisa de Preços)	16/05/2022
1.4	Versão preliminar consolidada pela EPC na fase de planejamento, encaminhada para análise jurídica.	08/06/2022
1.5	Versão consolidada pela EPC na fase de planejamento, após análise do Parecer Jurídico	26/09/2022

[1] Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019-versao-compilada

2 Descrição da demanda

Trata-se de demanda da Coordenação-Geral de Infraestrutura e Segurança – CGIS, com vistas à contratação de Solução de monitoramento de atividades em bancos de dados e mascaramento de dados, incluindo serviço de suporte técnico e garantia, com o intuito de atender às necessidades e demandas de TIC do MEC, conforme detalhado no Documento de Oficialização da Demanda (SEI nº3268209), Processo 23000.010862/2022-60, que elenca as seguintes duas necessidades a serem atendidas:

a) Provimento de solução de monitoração de atividades em bancos de dados (Database Activity Monitoring – DAM) e serviços agregados, para implantação de controles críticos de segurança da informação em bancos de dados; e
b) Provimento de Solução de mascaramento e anonimização de dados e serviços agregados, para atendimento aos requisitos da Lei Geral de Proteção de Dados – LGPD.

2.1 Análise do cenário atual

Atualmente o Ministério da Educação não dispõe de uma ferramenta capaz de prover as informações necessárias para analisar em tempo real a estrutura de dados nos bancos de dados e auditá-las. Assim, por vezes, acessos direto, LEGÍTIMOS, a Banco de Dados ocorrem por demanda da equipe de sistemas para que possam sustentar e desenvolver melhorias nos sistemas. Esses acessos apresentam as bases de dados como elas são incluindo os dados reais. Essa exibição proporciona uma falha grave de segurança da informação, pois dados sensíveis não poderiam ser acessados por qualquer pessoa, mesmo essas pessoas fazendo parte das equipes técnicas do MEC. Além disso, acessos não legítimos podem ocorrer a qualquer tempo por meio da ação de atacantes que tem como objetivo obter acesso às informações sensíveis e/ou danificar a base de dados.

O uso da Tecnologia da Informação e Comunicação como recurso para a otimização dos serviços públicos possibilita a Administração Pública prover medidas que torne seus procedimentos cada vez mais ágeis, seguros, integrados, eficientes e, sobretudo, acessíveis à toda a população brasileira.

Os dados sensíveis dos bancos de dados no Ministério da Educação estão sendo condensados na infraestrutura de SGBD (Gerenciamento de Banco de Dados ou *Database Management System* - DBMS), porém a capacidade nativa de segurança destes SGBD é insuficiente para gerir os riscos crescentes de ameaças, sejam elas internas e externas. De acordo com o GARTNER[2], 96% dos registros de violação de dados se deram em resultado de servidores de banco de dados comprometidos. Além disso, a gestão de SGBD cria um aumento da complexidade do gerenciamento de riscos para toda a estrutura organizacional de segurança da informação.

Devido a não homogeneidade da estrutura de banco de dados atual do Ministério da Educação, e em parte porque os controles nativos dos SGBD utilizados não oferecerem suporte ou capacidade de gerenciamento centralizado para outros SGBD, entendemos haver situação de potencial fragilidade nessas estruturas – em termos de capacidades de auditoria e de segurança, levando a risco de falhas potencialmente críticas na estratégia de segurança de banco de dados heterogêneos. Ademais muitas funcionalidades nativas dos SGBD não possuem algumas das mais importantes funcionalidades e dispositivos de segurança, tal como políticas de segurança para auditoria de acessos suspeitos.

Unificar os SGBD não seria uma solução, haja visto que as diversas tecnologias utilizadas estão alinhadas a necessidades de negócio atendidas com particularidades de cada arquitetura aplicada. Logo, essa não é uma alternativa para a questão.

Assim, a presente demanda objetiva ao atendimento dos requisitos de rastreabilidade, auditoria, mascaramento e acesso à dados no ambiente tecnológico do MEC – de forma agnóstica à arquitetura e/ou do SGBD. De forma complementar a nova solução deverá ser capaz de otimizar o uso de armazenamento em cópias (clones) de Banco de Dados visando fazer o uso racional dos recursos tecnológicos de armazenamento.

Em suma, é necessário garantir o contínuo aprimoramento dos controles críticos de segurança em dados tanto para implementar compliance regulatório quanto para assegurar os requisitos de segurança da informação - pois possíveis ataques de roubo de dados, acessos não autorizados e a ação de malwares podem implicar na indisponibilidade de diversos sistemas, impactando diretamente os sistemas críticos, bem como em toda a infraestrutura do MEC.

Por tais razões, a área requisitante entende que o atendimento da demanda em tela é indispensável para a efetivação das atividades finalísticas do MEC, permitindo que este Ministério continue cumprindo com seu papel institucional de provedor de políticas educacionais e entregando à sociedade sistemas e programas com qualidade e disponibilidade, preservando a integridade dos dados e o grau de sigilo necessários. Além disso, proporcionará que os dados armazenados nas bases de dados dos sistemas do MEC estejam em constante auditoria.

[2] As referências a conteúdos Gartner são feitas mediante licenciamento, conforme Contrato nº 28/2020-STIC. Em virtude dos termos de uso, não autorizamos a replicação de conteúdo licenciado.

2.2 Identificação das necessidades de negócio

A contratação em tela visa atender à necessidade de implementar uma camada de segurança na infraestrutura de bancos de dados do Ministério da Educação, permitindo:

a) Analisar a Infraestrutura de dados dos bancos de dados em tempo real;
b) Identificar dados confidenciais e classificá-los conforme sua criticidade;
c) Proteger os dados conforme interesse do Ministério da Educação;
d) Avaliar e analisar todas as atividades nos bancos de dados;
e) Possibilitar auditoria em valores nas tabelas de bancos de dados;
f) Disponibilizar dados para testes, auditorias e treinamentos sem que eles sejam compartilhados em sua versão autêntica, garantindo conformidade com as normas e Leis de proteção aos dados;
g) Mascarar e/ou *tokenizar* dados nos bancos de dados com o objetivo de garantir a confidencialidade das informações; e
h) Gerenciar o mascaramento e/ou a *tokenização* dos dados nos bancos de dados.

Diante dos desafios criados pelos processos de transformação digital das organizações públicas e pelos desafios de dependência tecnológica impostos pela Covid-19 o que acabou por forçar às organizações a expandir seu ambiente de trabalho em regime remoto. Desse modo, os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações - a exemplo o expressivo aumento dos casos de *ransomware* – requerendo que as corporações ampliem sua capacidade em gestão de segurança.

Os órgãos de controle também têm atuado na linha de monitorar as capacidades em gestão de segurança. Por exemplo, o Tribunal de Contas da União, por meio do TC 001.873/2020-2, registrou levantamento com o objetivo de conhecer a macroestrutura de governança e gestão de segurança da informação e de segurança cibernética na Administração Pública Federal (APF), incluindo aspectos referentes a legislação, políticas, normativos, atores, papéis e responsabilidades atinentes a essas áreas. O acompanhamento de controles críticos de Segurança Cibernética (SegCiber) das organizações públicas federais realizado pelo TCU baseia-se nas boas práticas do *framework* do **Center for Internet Security (CIS)** – que embora não seja diretamente recepcionado no regramento jurídico aplicável, tem sido bastante aceito com boa prática em controles críticos.

De acordo com o Relatório de Investigações de Violação de Dados de 2009 da Verizon Business - com base em dados analisados do número de casos de 90 violações confirmadas da Verizon Business envolvendo 285 milhões de registros comprometidos durante 2008 - 75% de todos os registros violados vieram de servidores de banco de dados comprometidos.

Nessa linha, o controle **CIS 8 - 03 Proteção de Dados** contempla a necessidade de se desenvolver processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados. Manter os dados custodiados pelo MEC implica dizer que todas as bases de dados dos sistemas internos e externos necessitam possuir controle de acesso, privacidade. Temos visto muitas ações que ocorrem em outras organizações onde os atacantes (hackers) obtém acesso a redes e aos sistemas com a finalidade de extrair esses dados sensíveis. O MEC tem caminhado no sentido de acompanhar a legislação vigente, porém sem uma ferramenta adequada torna-se impossível manter esses dados em segurança.

O controle **CIS 8 - 08 Gestão de registros de auditoria** reforça a necessidade de se coletar, analisar e reter logs de auditoria de eventos que podem ajudar a detectar, compreender ou se recuperar de um ataque. Nesse quesito devem ser considerados as possibilidades diversas de armazenamento dos logs de diferentes aplicações e sistemas.

O acesso dos usuários privilegiados é uma das principais preocupações de segurança da informação para auditoria. Usualmente a configuração padrão para SGBD é conceder aos DBA o acesso completo aos dados que, por sua, concedem os níveis de privilégios para os usuários. Contas privilegiadas incrementam os riscos de uso indevido, fraude ou ataques direcionados, portanto os reguladores precisam possuir um acompanhamento detalhado e acesso aos dados de auditoria das contas de privilégio elevado.

A prevenção ou bloqueio dos usuários privilegiados é uma tarefa complexa e ineficiente do ponto de vista do dinamismo e segurança da informação, visto a complexidade na diferenciação de um acesso legítimo do usuário privilegiado das atividades maliciosas ou enganadas. Logo, a obrigação de cumprir com diversos regulamentos destacou uma série de preocupações de segurança para auditores, como:

a) Identificar dados sensíveis;
b) Avaliação de vulnerabilidades e conformidade com os padrões de configuração de segurança;
c) Gerenciar os privilégios de desenvolvedores para impedir o acesso a campos de dados sensíveis ou colunas através de sistemas de produção;
d) Ser capaz de auditar mudanças em configurações e patchs dos próprios SGBD;
e) Avaliar os direitos de acesso dos usuários altamente privilegiados, tais como DBA, usuários de aplicação e administradores de sistema.
f) Monitoramento de acesso inadequado ou excessivo às bases de dados por usuários de aplicação.

No que se refere à necessidade de mascaramento e anonimização de dados, os regulamentos continuam a ser um dos principais fatores para a adoção de produtos de segurança de banco de dados relativos as informações pessoalmente identificáveis (PII), informações de

saúde protegidas (PHI), e informações de cartão de crédito e de financeiras, desta forma a Descoberta e Classificação de Dados é uma ferramenta de vital importância para o cenário atual quando vivemos ainda sob a Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709, de 14 de agosto de 2018. Mascarar os dados tem um papel crucial neste cenário, visto que os recursos de proteção de dados serão utilizados para acessar dados armazenados ou em produção.

Mascaramento pode ser aplicado para manter a estrutura do banco de dados, permitindo simultaneamente a funcionalidade de pesquisa. Mascaramento de dados também pode ser aplicada para proteger os dados subjacentes, substituindo-os com dados fictícios. No entanto fornecendo dados significativos para desenvolvedores e administradores durante as atividades de desenvolvimento ou homologação. É preciso que a solução objeto deste estudo permita a entrega de dados protegidos, tanto pelo método de anonimização, como pelo método de pseudonimização, em aderência à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

É notório a real necessidade da proteção em tempo real e visibilidade das atividades realizadas nos bancos de dados no Ministério da Educação, cobrindo e garantindo uma maior visibilidade e transparência em importantes sistemas e programas educacionais, tais como: ENEM, SISU, ProUNI, SIMEC, E-Mec e FIES, dentre outros.

Com uma base de dados complexa, heterogênea e de tamanho absoluto, automatizar os processos de descoberta e classificação trará ao Ministério da Educação a capacidade de descobrir e classificar de forma dinâmica as instâncias de bancos de dados novas ou modificadas que contém dados confidenciais, mesmo que previamente desconhecidos. Não obstante aos termos técnicos, vemos a necessidade de que toda a implementação da solução seja realizada de forma planejada, por profissionais altamente qualificados e que haja a operação assistida para ajustes detalhados da solução após a sua instalação.

Em razão dos fatos relatados, faz-se necessário a contratação de uma solução que tenha capacidade de identificar dados sensíveis, mascará-los para garantir sua anonimização e segurança, identificar os usuários que acessam aos dados e detectar usuários compartilhados no nível do sistema operacional e realizar todo o processo de auditoria sobre os dados contidos. Permitindo a realização de tratamento de dados pessoais garantindo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em atendimento à Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Por outro lado, existem no MEC a necessidade de utilização de armazenamento para as cópias das bases de dados do ambiente de produção. Essas cópias necessitam que sejam disponibilizados os recursos de armazenamentos iguais aos utilizados em ambiente de produção para que possam refletir com grau de fidelidade as condições normais de operação em produção. Dessa forma a ocupação tende a ser crescente sempre que se necessita criar bases CLONE para ambientes de desenvolvimento, homologação e testes além de demais outras necessidades. Sendo assim é preciso que a solução a ser contratada possibilite lidar com o uso de espaço em disco de forma otimizada, não impactando na capacidade de armazenamento da infraestrutura do MEC.

Além do exposto, objetiva-se atender à necessidade elencada no PDTIC 2021-2023 do MEC: "STIC.ACP-20 - Implantação de ferramenta de mascaramento de dados e a previsão contida no plano anual de compras para 2022 (item 257 - Contratação de solução de gerenciamento de segurança da informação).

2.3 Identificação das necessidades tecnológicas

No que se refere à solução de Database Activity Monitoring (DAM), temos que o monitoramento de atividades em bancos de dados (também conhecido como auditoria de banco de dados empresarial e proteção em tempo real) é uma tecnologia de segurança de banco de dados para monitorar e analisar a atividade do banco de dados. As soluções de DAM pode combinar dados de monitoramento baseado em rede e informações de auditoria nativas para fornecer uma imagem abrangente da atividade do banco de dados. Os dados coletados são usados para analisar e relatar a atividade do banco de dados, dar suporte a investigações de violação e alertar sobre anomalias – uma vez que normalmente é executado continuamente e em tempo real.

Globalmente, o monitoramento e prevenção de atividades de banco de dados (DAMP) é uma extensão do DAM que vai além do monitoramento e alerta para também bloquear atividades não autorizadas. O DAM ajuda as organizações a atender a exigências de conformidade regulatória, como o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), a Lei Sarbanes-Oxley (SOX), regulamentos do governo dos EUA, como NIST 800-53, e regulamentos da UE.

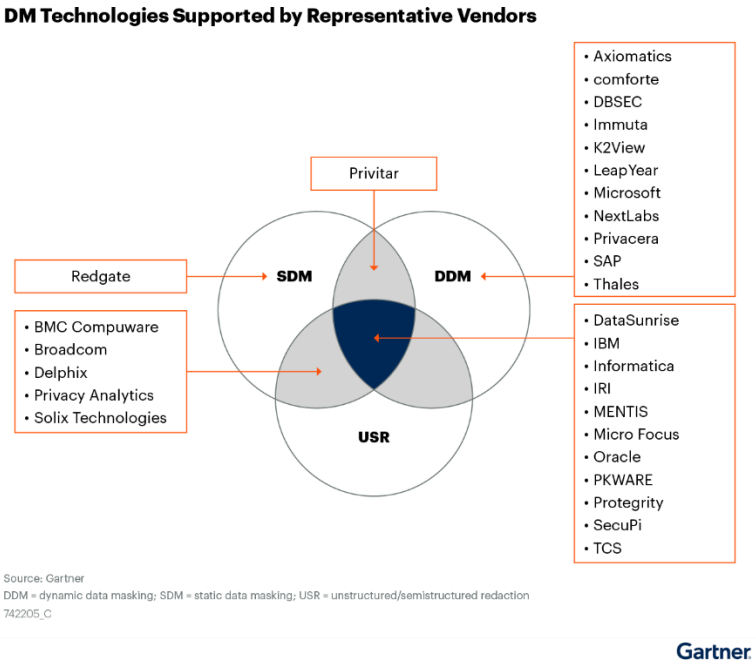
De acordo com o Gartner, "o DAM fornece monitoramento de acesso privilegiado de usuários e aplicativos que é independente do registro de banco de dados nativo e das funções de auditoria. Ele pode funcionar como um controle de compensação para problemas de separação de funções de usuários privilegiados, monitorando a atividade do administrador. A tecnologia também melhora a segurança do banco de dados ao detectar atividades incomuns de leitura e atualização do banco de dados da camada do aplicativo. A agregação, correlação e geração de relatórios de eventos de banco de dados fornecem um recurso de auditoria de banco de dados sem a necessidade de habilitar funções de auditoria de banco de dados nativas (que se tornam intensivas em recursos à medida que o nível de auditoria aumenta).".

No que se refere à necessidade de mascaramento e anonimização de dados é importante destacar que durante a fase de planejamento da contratação, foi realizada pesquisa no portal Gartner Peer Insights (https://www.gartner.com/reviews/home) na qual foi possível encontrar uma variada gama de soluções referentes aos casos de uso *Data Masking* e *Data Virtualization*, sendo possível constatar, inclusive, a existência de fabricantes e soluções que atendem a ambos os casos de uso. Existem soluções de mercado que atendem tanto ao caso de uso de mascaramento de dados quanto ao de disponibilização de cópias virtuais de dados.

No documento "Market Guide for Data Masking", publicado pelo Gartner em novembro de 2019, consta que o mascaramento de dados frequentemente é fornecido através de uma camada de replicação de dados ou cópia de virtualização, resultando em um conjunto de dados estaticamente mascarado no ambiente de destino. Este documento também informa que a virtualização de dados de teste é uma tecnologia cada vez mais popular quando usada em combinação com o mascaramento de dados, para acelerar o provisionamento e atualizações para ambientes-alvo, além de reduzir significativamente a quantidade de armazenamento exigida por esses ambientes. Informa ainda que existem diversos exemplos de fornecedores de mascaramento de dados que combinam ambas as tecnologias

Do mesmo documento, extrai-se as classificações e conceitos a seguir:

a) **Static Data Masking - SDM**: O SDM é usado para mascarar um conjunto de dados que é usado em um aplicativo, em vez dos dados reais. Os dados são mascarados antes de seu uso. Portanto, os dados são protegidos em repouso e em uso ou propagação subsequente. Na maioria das vezes, é implementado como um processo em lote iniciado manualmente, de forma programada ou orientado por um aplicativo, mas há variações arquitetônicas que se alinham aos modelos de dados de entrega modernos. Por exemplo, o SDM também pode ser entregue por meio de uma camada de replicação de dados ou de virtualização de cópia, resultando em um conjunto de dados estaticamente mascarado no ambiente de destino.
b) **Dynamic Data Masking - DDM**: O DDM aplica operações de mascaramento em tempo real quando um aplicativo ou uma pessoa acessa dados com base em direitos. Os dados confidenciais originais residem no repositório e podem ser acessados por um aplicativo quando autorizados pela política. Os usuários e aplicativos que não estão autorizados a acessar as informações confidenciais recebem dados mascarados. O DDM não altera os dados no repositório subjacente.
c) **Unstructured/Semistructured redaction - USR**: As organizações podem proteger conteúdo sensível não estruturado (PDF, arquivos Excel, arquivos de texto, arquivos de log etc.) e semiestruturado (XML, JSON etc.) com tecnologia de redação de dados. A demanda por USR e redação de dados semiestruturados de fornecedores de DM não é tão forte quanto a demanda por SDM e DDM para plataformas relacionais e de big data.



Como não é possível fazer uma comparação entre soluções considerando a totalidade das características técnicas e todos os requisitos previamente definidos, até porque o processo licitatório em tela não tem por objetivo restringir somente à um fabricante ou a uma só solução possível, a comparação entre soluções de mercado se deu considerando o atendimento das premissas definidas, conforme podemos verificar na tabela abaixo:

Fabricante	Licenciamento	Fornecimento	Métrica	Características	Limitações
Micro Focus	Perpétuo e Subscrição	On premise e Cloud	Sem informações	Suporta diversas plataformas de dados; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não realiza identificação e localização de dados sensíveis com base no domínio dos dados;
Delphix	Subscrição	On premise e Cloud	Por volume (Terabyte)	Suporta diversas plataformas de dados; Capacidade de identificar dados sensíveis de forma automatizada (inspeção); APIs REST para todos os fluxos; Modelo de implementação não intrusivo; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não implementa o Mascaramento de Dados Dinâmico (DDM);
IBM	Perpétuo e Subscrição	On premise e Cloud	Sem informações	Suporte a diversas plataformas de dados; Usuários desenvolvem seus próprios algoritmos, particulares para cada fonte de dados;	Requer desenvolvedores e DBAs especificamente qualificados para implementar e manter; Requer hardware dedicado, diversos componentes de software e staging; Gerenciamento manual de relacionamentos para identificação de dados sensíveis;
Oracle	Perpétuo e Subscrição	On premise e Cloud	Por core (núcleo de processamento)	Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados;	Suporta apenas os bancos de dados Oracle; Não tem identificação automática de dados sensíveis (inspeção); Não tem algoritmos determinístico pré-configurado; Requer desenvolvedores e DBAs altamente qualificados para implementar e manter; Depende de outros produtos da mesma plataforma; Não possui integração via APIs REST;
Informática	Perpétuo e Subscrição	On premise e Cloud	Por fontes de dados (métrica chamada de Data Stores)	Suporta diversas plataformas de dados; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados.	Requer produtos adicionais para identificação de dados sensíveis (inspeção); Depende de outros produtos da mesma plataforma; Interface de usuário é uma interface de programação ETL (depende de conhecimento técnico para utilizar).

Fabricante	Licenciamento	Fornecimento	Métrica	Características	Limitações
Imperva	Perpétuo e Subscrição	On premise e Cloud	Sem informações	Suporta diversas plataformas de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não implementa o Mascaramento de Dados Dinâmico (DDM); Não tem identificação automática de dados sensíveis (inspeção); Depende de outros produtos da mesma plataforma.

Quanto a análise dos modelos de licenciamento, segue o que foi considerado, conforme a tabela abaixo:

Licenciamento[3]	Vantagens	Desvantagens
Perpétuo	Fácil de gerenciar, uma vez que não tem renovações Não tem limitação de uso pelo tempo; Um só pagamento, sem a recorrência de pagamentos futuros; Pode ser contabilizado como capital, uma vez que se integra com os bens dos clientes.	Exige um desembolso financeiro maior inicial maior em relação ao licenciamento por subscrição; Aumenta o risco de desperdício em caso de descontinuidade do projeto; Dificuldade de gerenciar atualizações; Maior exposição a falhas de segurança; Sem a contratação de manutenção associada, existe a tendência ao uso de versão muito antiga.
Subscrição (assinatura) O uso da licença é renovável, geralmente anual, incluindo suporte de software e atualizações durante o período de cobertura. A licença é encerrada automaticamente, a menos que seja renovada	Exige um desembolso financeiro menor em comparação ao licenciamento perpétuo; Como exige uma decisão de renovação a cada período, existe uma redução do valor da subscrição por conta da pressão por receita do fabricante; Reduz o risco de desperdício dos recursos públicos em caso de descontinuidade do projeto; A política e as condições de licenciamento podem ser alteradas no momento da renovação; Possibilita ajustes quanto à quantitativos e erros de estimativa de uso, em caso de superdimensionamento inicial; Permite o pagamento anual, com recursos relacionados aos exercícios financeiros; Permite redução de custos operacionais em caso de necessidade de contingenciamento financeiro, uma vez que pode não ser renovada; Incentiva o relacionamento cliente/fornecedor de forma positiva, uma vez que o fornecedor tem total interesse na continuidade dos resultados pretendidos pela contratação.	Maior sobrecarga de gerenciamento de licenças, uma vez que requer processos de renovação anual; Requer manutenção de registros precisos para gerenciar o ciclo de vida das licenças.

A solução deve ter a capacidade de identificar dados sensíveis, mascará-los para garantir sua anonimização e segurança, identificar os usuários que acessam aos dados e detectar usuários compartilhados no nível do sistema operacional e realizar todo o processo de auditoria sobre os dados contidos, em aderência à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Deverão ser observadas as leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção ao Decreto Federal n° 3.505/2000, à Instrução Normativa GSI/PR n° 01/2008, e suas normas complementares.

Deverão ser observadas as normas e diretrizes contidas na Política de Segurança da Informação e Comunicações (POSIN) do MEC, e suas normas complementares, bem como as diretrizes do Plano Diretor de Segurança da Informação e Comunicações (PDSIC).

A solução não deve ser um obstáculo à adoção de Padrões de Interoperabilidade de Governo Eletrônico. Os sistemas e serviços de TI do MEC devem estar de acordo com normas de acessibilidade (e-Mag) e interoperabilidade do Governo Eletrônico (e-Ping), incluindo os padrões de governança.

A contratada deverá atender no que couber, os critérios de sustentabilidade ambiental. Destaca-se, as recomendações contidas no Capítulo III, Dos Bens e Serviços, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MPOG, bem como, o Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos, no que couber.

Todas as funcionalidades devem ser fornecidas integralmente pela solução, sem a necessidade de aquisições avulsas de funcionalidades, permitindo o acesso irrestrito e ilimitado do Ministério da Educação à solução, independentemente da quantidade de usuários internos necessários para sua operação ou uso.

Cada produto ou serviço entregue terá garantia mínima de 12 (doze) meses a contar da data do aceite definitivo. A garantia da solução contempla o fornecimento da solução de monitoramento de atividades em bancos de dados e mascaramento de dados. O suporte técnico deve contemplar a abertura de chamados técnicos para resolução de problemas eventualmente encontrados no uso do produto, aplicação de patches de correção e intervenções para manutenção em caso de falhas.

2.4 Identificação dos requisitos necessários e suficientes à escolha da solução

Consiste na contratação de soluções de monitoramento de atividades em bancos de dados e mascaramento de dados, contemplando instalação, configuração, suporte técnico, treinamento e transferência de conhecimentos.

O modelo adotado para contratação da presente Solução de TIC será no formato de contratação de licenciamento de software no formato de subscrição e de prestação de serviços aferidos e pagos mensalmente. O escopo dessa contratação consiste no licenciamento dos direitos do software (subscrição) de solução de DAM – Monitoramento de Atividades em Banco de Dados e de Mascaramento de Dados, por período determinado. O licenciado possui somente o direito de uso do software, não sendo autorizado a transferir, comercializar, doar, arrendar, alienar ou sublicenciar o software. As subscrições devem ser fornecidas pelo período mínimo de 12 (doze) meses (período de cobertura contratual), nos quantitativos previstos na sequência.

A presente solução contempla, ainda, os seguintes requisitos:

a) Serviços de implantação, instalação e configuração das soluções de Monitoramento de Atividades em Bancos de Dados e da solução de Mascaramento de Dados a ser fornecido no escopo desta contratação;
b) Suporte Técnico e atualização tecnológica;
c) Serviços de Operação Assistida composto por: serviço Técnico Especializado **sob demanda**, contemplando customização de configuração, ajustes de parâmetros e atividades relacionadas às necessidades do Ministério da Educação, visando a completa utilização das ferramentas; e provimento de treinamento para capacitação técnica da(s) equipe(s) interna(s) e transferência de conhecimento acerca das soluções a serem adquiridas no escopo desta contratação.

2.5 Estimativa do volume de bens e/ou serviços da demanda

A infraestrutura de banco de dados do Ministério da Educação é composta de bancos de dados MySQL, SQL Server, Postgree e Oracle, sendo:

SGBD/versão	SRVs/Cores físicos	SRVs/Cores lógicos
POSTGRES 9.4.8	4	16
POSTGRES 9.4.10	10	80
POSTGRES 11.8	2	4
POSTGRES 9.4.6	4	16
POSTGRES 9.4.10	8	32
POSTGRES 11.8	4	8
POSTGRES 9.4.12.21	2	8
POSTGRES 9.4.6	4	16
POSTGRES 9.6.15	2	16
POSTGRES 9.4.19	4	32

SGBD/versão	SRVs/Cores físicos	SRVs/Cores lógicos
POSTGRES 9.4.4	4	16
POSTGRES 11.8	2	8
POSTGRES 9.3.6	4	16
POSTGRES 9.4.12.21	10	80
POSTGRES 9.4.12	2	8
POSTGRES 9.2.24	2	16
POSTGRES 9.2.24	2	16
POSTGRES 11.8	2	8
POSTGRES 11.8	2	8
POSTGRES 9.3.5	4	16
POSTGRES 9.4.4	4	16
POSTGRES 9.4.1	10	80
POSTGRES 9.4.4	2	4
POSTGRES 9.2.1.3	2	8
POSTGRES 11.8	4	8
POSTGRES 9.2.1.3	2	8
POSTGRES 9.4.4	4	16
POSTGRES 9.3.24	4	16
POSTGRES 9.4.21	5	20
POSTGRES 9.4.12.21	2	10
POSTGRES 11.8	2	4
POSTGRES 9.4.4	4	16
POSTGRES 11.8	4	8
POSTGRES 9.4.6	8	32
POSTGRES 9.4.4	2	4
POSTGRES 11.8	4	8
POSTGRES 8.4.1	4	16
POSTGRES 9.4.2	2	8
POSTGRES 10.10	1	2

SGBD/versão	SRVs/Cores físicos	SRVs/Cores lógicos
POSTGRES 10.10	1	8
POSTGRES 9.2.4	2	8
POSTGRES 8.1.8	1	4
POSTGRES 8.3.1	2	4
POSTGRES 8.4.1	4	16
POSTGRES 8.4.1	4	16
POSTGRES 8.4.7	4	16
POSTGRES 8.4.4	4	16
POSTGRES 8.4.10	4	16
POSTGRES 8.4.4	4	8
POSTGRES 10.10	1	8
SUBTOTAL POSTGRES	179	824
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	16	
ORACLE DATABASE 12c - exam**********.mec.gov.br	16	
ORACLE DATABASE 12c - exam**********.mec.gov.br	16	
ORACLE DATABASE 12c - exam**********.mec.gov.br	16	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
ORACLE DATABASE 12c - exam**********.mec.gov.br	4	
SUBTOTAL ORACLE	96	
MySQL 5.6.35	2	4
MySQL 5.6.35	4	4
MySQL 4.1.11	1	1
MySQL 5.0.51	4	8

SGBD/versão	SRVs/Cores físicos	SRVs/Cores lógicos
MySQL 5.0.32	16	16
MySQL 5.7.8	2	4
MySQL 5.5.61	8	8
MySQL 5.6.41	8	8
MySQL 5.7.8	16	32
MySQL 5.7.8	16	32
MySQL 5.7.11	2	4
MySQL 5.7.6	2	4
SUBTOTAL SQL SERVER	81	125
SQL Server 2008 R2	2	4
SQL Server 2012 / 2014	6	8
SQL Server 2017	10	20
SQL Server 2012 / 2016	3	6
SQL Server 2014	138	276
SQL Server 2014	18	36
SQL Server 2014	16	32
SQL Server 2012	120	240
SQL Server 2012	68	136
SQL Server 2008 R2	16	32
SQL Server 2008 R2	8	16
SQL Server 2008 R2	2	4
SQL Server 2012	16	32
SQL Server 2016	10	20
SQL Server 2000	12	12
SUBTOTAL SQL SERVER	445	874
MariaDB 10.2.15	12	24
MariaDB 10.2.8	8	16
SUBTOTAL MARIADB	20	40

Para subsidiar este levantamento, as informações foram extraídas a partir dos principais sistemas gerenciadores de banco de dados do MEC (Oracle, MS SQL Server e PostgreSQL), considerando somente as requisições recebidas no período de 2020 a 2021. Para contabilizar o volume foram utilizadas queries contra as seguintes tabelas de sistema de acordo com o SGBD:

SGBD	Tabela de Sistema
Oracle	dba_segments
MS SQL Server	SYS.DATABASE_FILES
PostgreSQL	pg_database

Por meio dessas informações, foi verificado que as diversas solicitações de cópias de base de dados oriundas do ambiente de produção para outros ambientes totalizam um volume de 15.050 GB. Não fizeram parte do levantamento outros SGBD's como MySQL, que basicamente é utilizado para alguns Portais do MEC.

Assim, para atendimento da necessidade, entendemos adequado que a contratação seja ser composta pelos serviços descritos na tabela a seguir:

Estimativa do volume de bens e/ou serviços

LOTE	ITEM	DESCRIÇÃO DO ITEM	BEM/SERVIÇO	UNIDADE	QUANTIDADE ESTIMADA
1	1	Solução de software de segurança e monitoração de atividades em banco de dados (Database Activity Monitoring - DAM), contemplando instalação, configuração, suporte técnico, treinamento e transferência de conhecimentos - conforme requisitos especificados no Termo de Referência	Serviço	Subscrição Anual – Bancos de Dados	100
	2	Serviço de operação assistida	Serviço	Horas	2.016
2	3	Solução de software de disponibilização, acesso e controle de cópias virtuais de dados e mascaramento (anonimização e pseudonimização), contemplando instalação, configuração, suporte técnico, treinamento e transferência de conhecimentos - conforme requisitos especificados no Termo de Referência	Serviço	Subscrição Anual - Terabyte	10
	4	Serviço de operação assistida	Serviço	Horas	2.016

2.6 Alinhamento estratégico da demanda

A presente contratação está alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação vigente (PDTICMEC 2021-2023) Portal MEC - PDTIC, conforme detalhado no respectivo DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA (DOD). Assim como encontra-se devidamente registrada no PLANO ANUAL DE CONTRATAÇÕES DE TIC do Ministério da Educação para o ano de 2022.

3 Identificação e análise de soluções

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-01/2019/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

3.1 Análise comparativa das alternativas para o atendimento da demanda

3.1.1 Solução de monitoramento de atividades em bancos de dados

Para essa necessidade, como destacado na descrição da demanda, o MEC não possui nenhuma ferramenta, solução e/ou serviço compatível com o escopo da demanda. Nesse caso a melhor alternativa é realizar a contratação de uma solução no mercado que atenda aos requisitos negociais e técnicos da demanda:

Mapa comparativo das alternativas identificadas

Fabricante	Licenciamento	Fornecimento	Métrica	Características	Limitações
Micro Focus	Perpétuo e Subscrição	On-premise e Cloud	Sem informações	Suporta diversas plataformas de dados; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não realiza identificação e localização de dados sensíveis com base no domínio dos dados;
Delphix	Subscrição	On-premise e Cloud	Por volume (Terabyte)	Suporta diversas plataformas de dados; Capacidade de identificar dados sensíveis de forma automatizada (inspeção); APIs REST para todos os fluxos; Modelo de implementação não intrusivo; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não implementa o Mascaramento de Dados Dinâmico (DDM);
IBM	Perpétuo e Subscrição	On-premise e Cloud	Sem informações	Suporte a diversas plataformas de dados; Usuários desenvolvem seus próprios algoritmos, particulares para cada fonte de dados;	Requer desenvolvedores e DBAs especificamente qualificados para implementar e manter; Requer hardware dedicado, diversos componentes de software e staging; Gerenciamento manual de relacionamentos para identificação de dados sensíveis.
Oracle	Perpétuo e Subscrição	On-premise e Cloud	Por core (núcleo de processamento)	Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados.	Suporta apenas os bancos de dados Oracle; Não tem identificação automática de dados sensíveis (inspeção); Não tem algoritmos determinístico pré-configurado; Requer desenvolvedores e DBAs altamente qualificados para implementar e manter; Depende de outros produtos da mesma plataforma; Não possui integração via APIs REST;
Informática	Perpétuo e Subscrição	On-premise e Cloud	Por fontes de dados (métrica chamada de Data Stores)	Suporta diversas plataformas de dados; Funcionalidade de mascaramento integrado à funcionalidade de replicação / virtualização de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Requer produtos adicionais para identificação de dados sensíveis (inspeção); Depende de outros produtos da mesma plataforma; Interface de usuário é uma interface de programação ETL (depende de conhecimento técnico para utilizar).

Mapa comparativo das alternativas identificadas

Fabricante	Licenciamento	Fornecimento	Métrica	Características	Limitações
Imperva	Perpétuo e Subscrição	On-premise e Cloud	Sem informações	Suporta diversas plataformas de dados; Mantém a integridade referencial do dado mascarado em diversas tabelas e diferentes bases de dados;	Não implementa o Mascaramento de Dados Dinâmico (DDM); Não tem identificação automática de dados sensíveis (inspeção); Depende de outros produtos da mesma plataforma.

Quanto ao formato de contratação, as soluções mapeadas são comercializadas basicamente em duas modalidades:

ALTERNATIVA	DESCRIÇÃO DA ALTERNATIVA OU CENÁRIO IDENTIFICADO	ITEM
A	Aquisição de solução de monitoramento de atividades em bancos de dados (DAM) por licenciamento perpétuo	3.1.1
B	Aquisição de solução de monitoramento de atividades em bancos de dados (DAM) por subscrição de uso	3.1.2

Essas distintas modalidades de licenciamento geralmente são recomendadas nos seguintes cenários:

a) Licenciamento Perpétuo: Em soluções de software bem conhecidas e maduras no mercado, como suítes gráficas ou suítes de produtividade, sistemas operacionais e outras aplicações específicas com baixa risco de obsolescência e baixo risco de descontinuidade do projeto em face de prioridade ou patrocínio institucional; e
b) Licenciamento Por Subscrição: Em soluções de software que estão sendo testadas no ambiente e fazem parte de projetos inovadores e inéditos dentro das organizações. Em projetos que apresentam soluções de alto risco de obsolescência em virtude da acelerada inovação tecnológica e em projetos de alto risco de descontinuidade por conta de mudanças de prioridade ou patrocínio institucional.

Nos itens a seguir analisamos cada uma delas individualmente.

3.1.1.1 Alternativa A – Aquisição de solução na modalidade licenciamento perpétuo

Trata-se de aquisição da solução na modalidade perpétua, para esta alternativa considera-se:

a) Alto custo de investimento na aquisição das licenças perpétuas;
b) Aquisição do quantitativo fechado, sem a possibilidade de redução posterior;
c) Equipe interna deverá estar atenta e disponível para executar às atualizações liberadas;
d) Menor flexibilidade no uso das licenças; e
e) Garantia de suporte e atualização somente enquanto durar o prazo da garantia.

Destaca-se o fato da solução perpétua tende a transformar a Administração em um refém do fabricante durante o período contratado, nesse caso 60 (sessenta) meses, e após esse período ou o MEC adquire o serviço de manutenção e suporte anual para garantir as atualizações e suporte ou mantém a solução em uso sem atualização e suporte ou, até mesmo, opta pelo desuso da solução em detrimento do investimento já realizado.

As licenças perpétuas envolvem um pagamento único para a compra permanente do software, isso geralmente resulta em um custo inicial maior. O benefício é que, com essa alternativa a solução poderá ser usada ao longo de vários anos. Contudo, deve-se considerar a depreciação da solução ao longo do tempo, bem como, a rapidez com que a área de TIC precisa se atualizar, os volumes de dados aumentam, as ameaças on-line evoluem e as tecnologias avançam, softwares perpetuamente licenciados podem não oferecer a flexibilidade necessária.

Quanto a esse tipo de licenciamento também é importante pontuar que as licenças perpétuas demandas recursos de capital (CAPEX), por gerarem impacto patrimonial ao adquirente.

Em vista disso, atualmente o mercado está cada vez mais substituindo a licença de compra única para o produto por assinaturas baseadas em nuvem.

3.1.1.2 Alternativa B – Contratação de solução na modalidade subscrição de uso

Trata-se de contratação no modelo subscrição de direitos de uso, para esta alternativa considera-se:

a) Baixo custo se comparado a aquisição das licenças perpétuas;
b) Flexibilidade na contratação podendo ocorrer dimensionamentos ao longo do tempo (ano a ano);
c) Por se tratar de uma contratação na modalidade subscrição a empresa contratada irá tratar das atualizações; e

d) Facilidade de se aferir o uso e dimensionamento.

O custo inicial é menor que uma licença perpétua. Além disso, a contratação inclui automaticamente atualizações de software e suporte técnico, não havendo necessidade de um plano de manutenção, proporcionando a proteção mais atual para os dados e sistemas do MEC. Os recursos orçamentários para aquisição de licenças de subscrição de direitos de uso são carimbados como "custeio" (OPEX), através de contratos continuados.

3.1.2 Solução de mascaramento e anonimização de dados

Quanto à essa demanda, identificamos a possibilidade de que possa ser ao menos parcialmente atendida por soluções da Plataforma Microsoft Azure já disponíveis no ambiente do MEC – sendo necessário aprofundar a análise técnica para identificação da aderência à demanda e da efetividade necessidade e do escopo de uma eventual futura contratação.

Portanto, para esse item, recomendamos que seja realizada primeiramente a análise das soluções Microsoft para que, a partir das conclusões obtidas, possa ser retomada a avaliação de necessidade de uma contratação específica.

4 Análise comparativa de custos

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-01/2019/SGD, e inclui:

a) comparação de custos totais de propriedade (*Total Cost Ownership* – TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção; e

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

Considerando que a demanda prosseguirá apenas para atendimento da necessidade de provimento de solução de monitoramento de atividades em bancos de dados, temos que a alternativa considerada viável para análise comparativa de custos é a seguinte:

ID SOLUÇÃO	DESCRIÇÃO DA ALTERNATIVA OU CENÁRIO IDENTIFICADO	TCO GLOBAL
B	Contratação de solução na modalidade subscrição de uso	R$9.772.819,00

O detalhamento dos cálculos realizados está contido no documento de pesquisa de preços, que segue incorporado ao processo administrativo nº 23000.010862/2022-60, sendo também referenciado no ANEXO D, deste estudo.

4.1 Memória de cálculo das soluções viáveis

4.1.1 Alternativa B – Contratação de Solução de monitoramento de atividades em bancos de dados

O quadro abaixo apresenta a tabela resumo da pesquisa de preços realizada com o TCO para a alternativa viável em análise:

LOTE	ITEM	DESCRIÇÃO DO ITEM	BEM/SERVIÇO	UNIDADE	QUANTIDADE ESTIMADA	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	1	Subscrição de solução de software de segurança e monitoração de atividades em banco de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados	Serviço	Subscrição Anual - Banco de Dados	100	R$89.825,47	R$8.982.547,00
	2	Serviços agregados de operação assistida para a solução de segurança e monitoração de atividades em bancos de dados ((*Database Activity Monitoring* - DAM), conforme requisitos especificados	Serviço	Horas	2.016	R$392,00	R$790.272,00

4.2 Registro das soluções inviáveis

De acordo com o presente estudo, em que pese o cálculo do respectivo custo total de propriedade, conforme previsão contida no inciso III, art. 11 da Instrução Normativa nº 01, de 04 de abril de 2019, a ALTERNATIVA A foi considerada inviável, tendo em vista os riscos apontados na análise técnica, além de não ser usualmente utilizada pela Administração Pública, apresenta restrições técnicas, econômicas e ausência completa de parâmetros confiáveis de custos.

5 Escolha da solução

5.1 Composição da solução escolhida

Após a análise comparativa das Soluções, identificadas a alternativa viável, economicamente mais vantajosa para a Administração a Equipe de Planejamento da Contratação recomenda a escolha da alternativa "B" (Contratação de solução de monitoramento de atividades em bancos de dados mediante subscrição de direitos de uso, com serviços agregados), estruturada da seguinte forma:

Lote	Item	Descrição do item	Catser	Unidade	Quantidade estimada
1	1	Subscrição de solução de software de segurança e monitoração de atividades em banco de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados.	24333	Subscrição Anual - (Banco de dados)	100
	2	Serviços agregados de operação assistida para a solução de segurança e monitoração de atividades em bancos de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados.	27260	Horas de Serviço Técnico	2.016

A demanda será atendida mediante a contratação de subscrição de direitos de uso de solução de software com serviços agregados de instalação, configuração, consultoria, transferência de conhecimento e operação assistida – necessários à plena operação da solução. A execução dos serviços de planejamento, instalação e configuração da solução, bem como sua integração à rede e as alterações que ocorrerão no contexto do Projeto de Implementação, cujas etapas e atividades mínimas deverão ser descritas no Termo de Referência.

5.1.1 Justificativas da escolha da solução

O monitoramento de atividades em bancos de dados (Database Activity Monitoring - DAM, também conhecido como auditoria de banco de dados empresarial e proteção em tempo real) é uma tecnologia de segurança de banco de dados para monitorar e analisar a atividade do banco de dados. As soluções de DAM pode combinar dados de monitoramento baseado em rede e informações de auditoria nativas para fornecer uma imagem abrangente da atividade do banco de dados. Os dados coletados são usados para analisar e relatar a atividade do banco de dados, dar suporte a investigações de violação e alertar sobre anomalias – uma vez que normalmente é executado continuamente e em tempo real.

Globalmente, o monitoramento e prevenção de atividades de banco de dados (DAMP) é uma extensão do DAM que vai além do monitoramento e alerta para também bloquear atividades não autorizadas. O DAM ajuda as organizações a atender a exigências de conformidade regulatória, como o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), a Lei Sarbanes-Oxley (SOX), regulamentos do governo dos EUA, como NIST 800-53, e regulamentos da UE.

DAM também é uma tecnologia importante para proteger bancos de dados confidenciais de ataques externos de cibercriminosos. De acordo com o Relatório de Investigações de Violação de Dados de 2009 da Verizon Business - com base em dados analisados do número de casos de 90 violações confirmadas da *Verizon Business* envolvendo 285 milhões de registros comprometidos durante 2008 - 75% de todos os registros violados vieram de servidores de banco de dados comprometidos.

De acordo com o Gartner, "o DAM fornece monitoramento de acesso privilegiado de usuários e aplicativos que é independente do registro de banco de dados nativo e das funções de auditoria. Ele pode funcionar como um controle de compensação para problemas de separação de funções de usuários privilegiados, monitorando a atividade do administrador. A tecnologia também melhora a segurança do banco de dados ao detectar atividades incomuns de leitura e atualização do banco de dados da camada do aplicativo. A agregação, correlação e geração de relatórios de eventos de banco de dados fornecem um recurso de auditoria de banco de dados sem a necessidade de habilitar funções de auditoria de banco de dados nativas (que se tornam intensivas em recursos à medida que o nível de auditoria aumenta)."

5.1.1.1 Justificativa técnica

Considerando que a área requisitante não possui ferramentas capazes de atender a demanda pleiteada, nem mesmo de forma parcial, o modelo de subscrição de solução de monitoramento de atividades em bancos de dados, com garantia, suporte técnico e operação assistida, é a solução mais viável para o atendimento dos padrões de qualidade exigidos, com ganho na eficiência, eficácia e economicidade para a Administração Pública.

Com relação aos requisitos técnicos, a solução foi especificada tanto para prover as funcionalidades mínimas para atendimento das necessidades como para se adequar ao ambiente tecnológico do MEC – que é bastante heterogêneo, principalmente se considerarmos as multitecnologias de Banco de Dados atualmente em uso (Oracle, MS SQLServer, PostgreSQL, entre outros).

Por outro lado, considerando a capacidade própria, não seria suficiente apenas contratar o licenciamento da solução – vez que sua instalação, configuração e adaptação demanda conhecimentos técnicos especializados. Desse modo, é tecnicamente necessário que também sejam contratados serviços agregados para implantação da solução no ambiente computacional do MEC.

Além disso, considerando os ciclos dos processos seletivos de acesso ao ensino superior e demais atividades de caráter crítico e cíclico, momento em que há uma forte curva de aumento de demandas sob o ambiente e a equipe própria, também consideramos adequado assegurar a disponibilidade de serviços agregados de operação assistida sob demanda para atender a essas necessidades.

A especificação do objeto também considerou os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Governo Digital do Ministério da Economia e no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.

5.1.1.2 Justificativa econômica

Conforme evidenciado neste Estudo, a contratação da solução pela modalidade subscrição de direitos de uso é a opção mais adequada do ponto de vista econômico – por permitir o enquadramento da despesa como "custeio" (OPEX) e estar alinhada ao direcionador estratégico "3 – Tecnologia adaptativa", contido no PDTIC-MEC 2021-2023.

Esse modelo responde mais adequadamente à flutuação de demandas e possui menor custo de entrada em relação à opção de licenciamento perpétuo – além de garantir o provimento de uma solução sempre atualizada e com o necessário suporte técnico.

5.1.1.3 Enquadramento legal e normativo

A natureza do objeto a ser adquirido enquadra-se na classificação de serviços comuns, de caráter continuado e sem fornecimento de mão de obra em regime de dedicação exclusiva, nos termos do parágrafo único, do art. 1°, da Lei nº10.520, de 2002, c/c art. 3º, II do Decreto nº 10.024/2019. Classifica-se o objeto deste Termo de Referência, também, como bens ou serviços de informática, nos termos do Decreto nº 7.174/2010, para fins de definição dos critérios de sua aceitação quando da fase externa da licitação.

A instrução Normativa n° 01, de 4 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia (IN SGD/ME n° 01/2019), disciplina o processo de contratação de soluções de tecnologia da informação e comunicação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo federal.

Suas definições derivam de todo o arcabouço legal acerca de contratações públicas, tais como a Lei 8.666/1993 e o Decreto n° 7174/2010 que "regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União" que, em seu art. 2° estabelece a obrigatoriedade de realizar o planejamento;

> Art. 2º A aquisição de bens e serviços de tecnologia da informação e automação deverá ser precedida da elaboração de planejamento da contratação, incluindo projeto básico ou termo de referência contendo as especificações do objeto a ser contratado, vedando-se as especificações que:
> I - direcionem ou favoreçam a contratação de um fornecedor específico;
> II - não representem a real demanda de desempenho do órgão ou entidade; e
> III - não explicitem métodos objetivos de mensuração do desempenho dos bens e serviços de informática e automação.

5.1.1.4 Modelo de execução

Considerando as características de cada lote da contratação, a respectiva vigência contratual inicial será de **12 (doze) meses**, contados da data da sua assinatura, podendo ser prorrogado por interesse das partes, por iguais e sucessivos períodos até o limite de **48 (quarenta e oito) meses** observado o limite estabelecido no inciso II, do art. 57, da Lei n° 8.666/1993.

5.1.1.5 Justificativa do quantitativo a ser contratado

Conforme apontado na fase de estimativa de demanda (item 2.5), a infraestrutura de banco de dados do Ministério da Educação é composta de servidores PostGree, Oracle, SQL Server, MySQL e MariaDB, totalizando:

a) 50 Postgree;
b) 12 Oracle;
c) 15 SQL Servers;
d) 12 MySQL; e
e) 2 MariaDB.

Em complemento efetuamos o levantamento da lista e da quantidade de sistemas disponibilizados pela infraestrutura do MEC e que por consequência devem estar cobertos pela presente contratação. Hoje o MEC possui em sua infraestrutura um total de 209 sistemas. Convém destacar que desse total de 109 sistemas/módulos fazem parte do SIMEC e que para efeitos de contabilização de licenças deve-se considerar, nesse caso, esses 109 módulos como 1 (um) sistema. Dessa forma, para efeitos de dimensionamento do parque de sistemas do MEC é seguro utilizar o quantitativo de 101 (cento e um) sistemas. A relação completa dos sistemas está presente no ANEXO B. Além dos recorrentes pedidos de acesso à informação apresentados por meio da Lei de Acesso à Informação (LAI), existe um número considerável de demandas registradas com a finalidade de transposição de cópias de ambiente de produção para outros ambientes.

5.1.1.6 Parcelamento ou não parcelamento da solução

Considerando a natureza complementar e interdependente dos itens da contratação, entendemos que a solução não é divisível, ou seja, não há viabilidade técnica e econômica em seu parcelamento. Os serviços de operação assistida (Item 1) dizem respeito

exclusivamente à solução de software licenciada (Item 1), devendo serem necessariamente providos pelo mesmo fornecedor responsável pelo projeto, implementação e configuração da solução de software devido à sua interdependência técnica – com vistas a assegurar a entrega dos resultados pretendidos.

Na forma do ANEXO I da Instrução Normativa SGD/ME n° 01/2019 "serviços agregados são aqueles relacionados ao licenciamento de software, tais como os serviços de atualização de versão, manutenção e suporte técnico". Assim, na fase de análise da demanda, verificamos a necessidade de incluir o serviço de operação assistida da solução, no entanto, tal item difere dos serviços agregados que compõem o item 1 por possuir característica de requisição sob demanda – disso, visando a economicidade, julgamos adequado separá-los em um item com faturamento unitário, sob demanda.

Em complemento também atestamos que não foram identificados serviços alternativos que viabilizassem o atendimento dessa necessidade. Assim como atestamos que não haverá fornecimento condicionado desse item ao item 1, não podendo o fornecer em nenhuma hipótese vincular a utilização da solução à contratação de serviços de operação assistida.

Portanto, a decomposição do objeto não é tecnicamente viável, assim como não resultaria em melhor aproveitamento do mercado e nem ampliaria a competitividade do certame – trazendo, ainda, a possibilidade de risco ao conjunto do objeto pretendido. Portanto, não há razão para fragmentar inadequadamente os serviços a serem contratados.

5.1.1.7 Escolha do regime de execução

A equipe de planejamento da contratação entende ser a EMPREITADA POR PREÇO GLOBAL o regime de execução mais adequado para o objeto pretendido e o tipo e critério de julgamento da futura licitação, o MENOR PREÇO por lote, para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratações de bens e serviços de informática.

De acordo com o Art.1º do Decreto nº10.024/2019, a futura licitação deverá ser realizada na modalidade de Pregão, preferencialmente na sua forma eletrônica, com julgamento pelo critério de menor preço por lote. A fundamentação pauta-se na premissa de que a aquisição dos bens e a prestação dos serviços elencados neste estudo, baseiam-se em padrões de desempenho e qualidade claramente definidos por meio de especificações usuais de mercado, havendo diversos fornecedores capazes de fornecê-los e prestá-los, caracterizando-os como "bens e serviços comuns", de acordo com a previsão contida no Art. 9º, §2º do Decreto 7.174/2010.

O processo licitatório NÃO será destinado exclusivamente à participação de microempresas e empresas de pequeno porte, conforme preceitua o art. 6º do Decreto nº 8.538, de 6 de outubro de 2015, que regulamenta o tratamento favorecido, diferenciado e simplificado para estas entidades, pois o valor estimado para o lote pretendido é superior a R$ 80.000,00 (oitenta mil reais), também não aplicando-se o benefício referente à cota exclusiva para microempresas e empresas de pequeno porte, pois o lote se trata de uma única solução, sendo impossível subdividi-la, devido à necessidade de compatibilização de todos os seus componentes/serviços, de acordo com as previsões contidas neste estudo.

5.1.1.8 Classificação dos bens e/ou serviços a serem contratados

No que concerne os bens e serviços que compõe a solução, em conformidade com o art. 1° da LEI N° 10.520/2002, para fins de avaliação da aplicabilidade do DECRETO N° 10.024/2019, o objeto pretendido enquadra-se como SERVIÇO COMUM por apresentar, independentemente de sua complexidade, "padrões de desempenho e qualidade objetivamente definidos em edital, por meio de especificações usuais no mercado".

De acordo com os entendimentos estabelecidos na Nota Técnica n° 02/2008 SEFTI/TCU, "devido à padronização existente no mercado, os bens e serviços de tecnologia da informação geralmente atendem a protocolos, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado. Logo, geralmente, esses bens e serviços devem ser considerados comuns para fins de utilização da modalidade Pregão"

> [...] "Em geral, nem a complexidade dos bens ou serviços de tecnologia da informação nem o fato de eles serem críticos para a consecução das atividades dos entes da Administração descaracterizam a padronização com que tais objetos são usualmente comercializados no mercado. Logo, nem essa complexidade nem a relevância desses bens e serviços justificam o afastamento da obrigatoriedade de se licitar pela modalidade Pregão".

5.1.2 Forma de seleção do fornecedor

Considerando a natureza dos bens e/ou serviços pretendidos, o disposto no §1° do art. 1° do DECRETO N° 10.024/2019 e o disposto no § único do art. 26 da INSTRUÇÃO NORMATIVA SGD/ME N° 01, de 04 de abril de 2019, a licitação será realizada na modalidade PREGÃO ELETRÔNICO do tipo MENOR PREÇO GLOBAL observando, como critério de julgamento, o valor por LOTE. Quanto aos modos de disputa, assim define o art. 31 do Decreto n° 10.024/2019:

> Art. 31. Serão adotados para o envio de lances no pregão eletrônico os seguintes modos de disputa:
> I - aberto - os licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado no edital; ou
> II - aberto e fechado - os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado, conforme o critério de julgamento adotado no edital.

> Parágrafo único. No modo de disputa aberto, o edital preverá intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

Assim, embora ressalvada a competência da área administrativa para decidir sobre tal ponto, recomendamos que seja adotado o modo de disputa aberto, uma vez que em nossa visão este propicia maior grau de disputa:

> Art. 32. No modo de disputa aberto, de que trata o inciso I do caput do art. 31, a etapa de envio de lances na sessão pública durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.
> § 1º A prorrogação automática da etapa de envio de lances, de que trata o caput, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.
> § 2º Na hipótese de não haver novos lances na forma estabelecida no caput e no § 1º, a sessão pública será encerrada automaticamente.
> § 3º Encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no § 1º, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço disposto no parágrafo único do art. 7º, mediante justificativa.

5.1.2.1 Modalidade e tipo de licitação

O Decreto nº 10.024/2019, que "regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns", em seus parágrafos 1º e 4º do artigo 1º, define:

> Art. 1º [...]
> § 1º A utilização da **modalidade de pregão, na forma eletrônica**, pelos órgãos da administração pública federal direta, pelas autarquias, pelas fundações e pelos fundos especiais é obrigatória.
> [...]
> § 4º Será admitida, excepcionalmente, mediante prévia justificativa da autoridade competente, a utilização da forma de pregão presencial nas licitações de que trata o caput ou a não adoção do sistema de dispensa eletrônica, desde que fique comprovada a inviabilidade técnica ou a desvantagem para a administração na realização da forma eletrônica.

Por conseguinte, a IN-01/2019/SGD/ME corrobora essa determinação em seu artigo 25:

> Art. 25. [...]
> Parágrafo único. É obrigatória a utilização da modalidade Pregão para as contratações de que trata esta Instrução Normativa sempre que a solução de TIC for enquadrada como bem ou serviço comum, conforme o disposto no § 1º, art. 9º do Decreto nº 7.174, de 2010.

Em suma, as licitações de bens e serviços de TIC para aquisição de bens e serviços comuns, regidas pela IN SGD/ME nº 1/2019, utilizam o pregão eletrônico, instituído pela Lei nº 10.520/2002.

Aplica-se a adoção do Sistema de Registro de Preços, à luz do princípio da eficiência, o SRP tem por escopo instrumentalizar meios para aquisição parcelada de bens e serviços na Administração Pública, sendo, portanto, compatível com a Lei do Pregão nº 10.520/02.

Desta forma, a adoção do SRP, enquadra-se nas hipóteses previstas no Decreto nº 7.892/2013:

> Art. 3- O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:
> I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
> II – quando o for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
> III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo: ou
> IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Em função dos aspectos técnicos e requisitos que envolvem a execução dos serviços e considerando o grau de interação do conjunto de serviço técnico descrito no presente estudo, natureza específica, caráter contínuo, características de especificidade, aliada a criticidade e complexidade que envolve a prestação de serviço desta contratação, e em virtude da ausência de estrutura administrativa satisfatória para fins de gerenciamento de demandas advindas de outros órgãos interessados na contratação, bem como pela necessidade de realização e conclusão célere deste procedimento licitatório, opta-se pela não divulgação da Intenção de Registro de Preços - IRP.

5.1.2.2 Requisitos de qualificação técnica do fornecedor

Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de serviços em características e quantidades compatíveis com a presente

licitação, mediante apresentação de um ou mais ATESTADO (S) DE CAPACIDADE TÉCNICA que deverão comprovar o atendimento aos seguintes requisitos mínimos:

Requisitos de capacidade técnica	
LOTE / REQUISITO	Requisito detalhado
1-A	Fornecimento de solução de TIC compatível com o objeto da pretensão contratual em volume correspondente a, no mínimo, cerca de 30% do quantitativo individual previsto para o item 1[3].
1-B	Execução de serviços de projeto, implantação, operação assistida e suporte técnico-operacional (ou serviços agregados similares) compatíveis com o objeto da pretensão contratual.

Os ATESTADOS DE CAPACIDADE TÉCNICA devem atender, ainda, ao seguinte:

a) Os ATESTADOS devem evidenciar explicitamente a execução de objeto compatível ao objeto da presente licitação - contendo descrição adequada, clara e suficiente do(s) serviço(s) executado(s) ou em execução;
b) Os ATESTADOS devem conter a identificação do(s) contrato(s) vinculado(s) e do(s) período(s) a que se referem os serviços executados, podendo considerar contratos já executados ou em execução[4];
c) Os ATESTADOS deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificada no contrato social vigente do LICITANTE; e
d) Será admitido o somatório de ATESTADOS para comprovar a capacidade técnico-operacional do LICITANTE.

Visando garantir a razoabilidade e a ampliação da competitividade do certame serão admitidos atestados em outras unidades de medida (tais como PF, UST e outras), desde que demonstrada e comprovada a correlação entre a métrica e a quantidade de horas de trabalho empreendidas na execução contratual, resultando no inequívoco atendimento à exigência mínima acima descrita[5]. Assim como poderão ser aceitos ATESTADOS cujas atividades executadas não estejam listadas de forma idêntica àquelas acima previstas – desde que o objeto da contratação e os serviços executados sejam compatíveis com o da presente contratação, devendo tal compatibilidade restar suficientemente clara nos ATESTADOS e/ou nos seus documentos complementares.

A critério do CONTRATANTE, nas situações em que julgar necessário, poderão ser realizadas inspeções e diligências com a finalidade de entender, esclarecer e/ou comprovar as informações contidas no(s) ATESTADO(S) DE CAPACIDADE TÉCNICA entregue(s) – nos termos do §3°do art. 43 da Lei n° 8.666/1993. Assim como poderão ser solicitadas cópias de documentos complementares como contratos, notas fiscais e notas de empenho. Porém, não serão executadas diligências para acrescentar informações obrigatórias ausentes no(s) atestado(s) apresentado(s).

A eventual recusa do(s) emitente(s) do(s) ATESTADO(S) em prestar esclarecimentos e/ou fornecer documentos comprobatórios, ou sofrer diligências, ou a constatada inexatidão das informações atestadas, desconstituirá o(s) ATESTADO(S) – o que poderá, inclusive, configurar prática criminosa, ensejando comunicação ao Ministério Público Federal e abertura de Processo Administrativo Disciplinar, conforme o caso, para fins de apuração de responsabilidades.

No caso de atestados emitidos por empresas privadas, não serão admitidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial[6] da empresa proponente. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da CONTRATADA proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente. Ainda, com respeito aos ATESTADOS DE CAPACIDADE TÉCNICA:

a) Devem estar relacionados ao objeto da licitação;
b) Devem ser pertinentes e compatíveis às características, quantidades e prazos exigidos na licitação;
c) Poderão ser fornecidos por pessoas jurídicas de direito público ou privado, com correta identificação do emissor;
d) Devem ser emitidos sem rasuras, acréscimos ou entrelinhas;

[3] Para o item 1 (solução de software) será exigida a comprovação de fornecimento, instalação, configuração e manutenção de solução compatível com o objeto pretendido com capacidade mínima de 30 (trinta) hosts/bancos de dados – o que corresponde a 30% do volume previsto para o item.

[4] Tal exigência visa a evitar que o somatório de atestados acumulados durante longo período atinja o quantitativo mínimo exigido, não resultando, porém, na comprovação da efetiva capacidade logística e operacional do LICITANTE para executar o objeto (Acórdãos TCU n° 2.048:2006-Plenário e 1.287:2008-Plenário).

[5] Para atestados em Ponto de Função as licitantes deverão basear-se na produtividade média definida no respectiva Contrato e/ou no Guia de Métrica adotado na Contratação. Quando a contratação não contiver produtividade média, poderá ser utilizada a referência do Guia de Métricas de Software do SISP ou o padrão de 10 HH/PF utilizado pelo Contratante em seu Estudo Técnico Preliminar.

[6] Grupo de empresas mantido sob a direção, controle ou administração de outra, embora tendo, cada uma delas, personalidade jurídica própria e autonomia individual, constituindo grupo industrial, comercial ou de qualquer outra atividade econômica.

e) Devem estar assinados por quem tenha competência para expedi-los, tais como representantes legais do órgão/empresa, diretores, gerentes e representantes formais das áreas técnica ou demandante (sem se limitar a esses);

f) Devem conter identificação clara e suficiente do Atestante;

g) Devem apresentar redação clara, sucinta e objetiva que demonstre de forma inequívoca o atendimento ao objeto da requisição.

Convém destacar que, na análise dos atestados de capacidade técnica, o CONTRATANTE primará pela finalidade precípua da exigência, qual seja: a demonstração de que os licitantes possuem condições técnicas para executar o objeto pretendido pela Administração caso venha a sagrar-se vencedor da licitação. Assim, preservada a aderência aos ditames legais e constitucionais fundamentais, o exame documental balizar-se-á nos princípios da razoabilidade, da proporcionalidade e do formalismo moderado – o que, por óbvio, não significa que serão admitidos quaisquer informalismos.

5.1.2.3 Requisitos da garantia contratual

O adjudicatário prestará GARANTIA DE EXECUÇÃO DO CONTRATO, nos moldes do art. 56 da Lei nº 8.666/1993, com validade durante a execução do CONTRATO e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (CINCO POR CENTO) do valor total do CONTRATO.

No prazo máximo de 10 (DEZ) DIAS ÚTEIS, prorrogáveis por igual período, a critério do CONTRATANTE, contados da assinatura do CONTRATO, a CONTRATADA deverá apresentar comprovante de prestação de GARANTIA, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

A inobservância do prazo fixado para apresentação da GARANTIA acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autoriza a ADMINISTRAÇÃO CONTRATANTE a promover a rescisão do CONTRATO por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

A validade da GARANTIA, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017. A GARANTIA assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do CONTRATO e do não adimplemento das demais obrigações nele previstas;
b) prejuízos diretos causados à ADMINISTRAÇÃO CONTRATANTE decorrentes de culpa ou dolo durante a execução do CONTRATO;
c) multas moratórias e punitivas aplicadas pela ADMINISTRAÇÃO CONTRATANTE à CONTRATADA; e
d) obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

A modalidade SEGURO-GARANTIA somente será aceita se contemplar todos os eventos indicados acima, observada a legislação que rege a matéria. A GARANTIA em dinheiro deverá ser efetuada em favor da CONTRATANTE, em conta específica na CAIXA ECONÔMICA FEDERAL, com correção monetária.

Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo BANCO CENTRAL DO BRASIL, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

No caso de alteração do valor do CONTRATO, ou prorrogação de sua vigência, a GARANTIA deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

Se o valor da GARANTIA for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (DEZ) DIAS ÚTEIS, contados da data em que for notificada. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

Será considerada extinta a GARANTIA:

a) com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do CONTRATO;
b) no prazo de 90 (noventa) dias após o término da vigência do CONTRATO, caso a ADMINISTRAÇÃO não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada. A CONTRATADA autoriza a contratante a reter, a qualquer tempo, a GARANTIA, na forma prevista no EDITAL e no CONTRATO.

5.1.3 Benefícios identificados

Os benefícios/resultados a serem alcançados com a presente contratação são:

a) Executar as ações previstas no Plano Orçamentário do PDTIC vigente;
b) Atendimento à Lei Geral de Proteção de Dados Pessoais (LGPD), que veda o tratamento de informações pessoais sem o devido consentimento e sem a devida garantia da prevenção à fraude e à segurança do titular das informações;
c) Reduzir significativamente a despesa no acesso aos dados, evitando que os usuários requisitantes de dados abram ordens de serviço para execução de operações de gerenciamento de dados, bem como o custo de manutenção de ambientes de homologação e do armazenamento de dados;
d) Permitir que os usuários obtenham os dados de que precisam, quando precisam, e, ao mesmo tempo, fornecer aos administradores os controles necessários para garantir que os recursos sejam contabilizados adequadamente;
e) Aumentar a produtividade no desenvolvimento de projetos que consomem dados, com redução do retrabalho, eficiência na alocação de recursos críticos bem como na criação de ambientes de desenvolvimento, homologação e testes;
f) Propiciar a segurança na movimentação de dados, evitando o acesso a dados de informações pessoais por desenvolvedores ou demais usuários com acesso privilegiado;
g) Suportar as iniciativas e entregas estratégicas das áreas finalísticas do Ministério, bem como as que virão a fazer parte do novo planejamento estratégico do MEC.
h) Atender aos requisitos de Segurança da Informação e adequação das leis e normativos relacionadas à privacidade dos dados;
i) Aderência ao CIS v.8 em consonância com o acompanhamento de controles críticos de segurança cibernética das organizações públicas federais.

5.1.4 Alinhamento legal e normativo

Na elaboração deste documento foram observadas as seguintes fontes legais e normativas:

a) Lei Federal n° 8.666/1993: institui normas gerais para licitações e contratos na Administração Pública e dá outras providências;
b) Lei Federal nº 10.520/2002: institui a modalidade de licitação denominada pregão eletrônico para aquisição de bens e serviços comuns e dá outras providências;
c) Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;
d) Lei Complementar n° 123/2006: institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;
e) Decreto nº 7.174/2010: regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
f) Decreto n° 7.579/2011: dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;
g) Decreto 7.746/2012: regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;
h) Decreto n° 7.903/2013: estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de equipamentos de tecnologia da informação e comunicação que menciona;
i) Decreto n° 8.4202015: regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências;
j) Decreto nº 9.507/2018: dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
k) Decreto nº 9.739/2019: estabelece medidas de eficiência organizacional para o aprimoramento da administração pública federal direta, autárquica e fundacional, estabelece normas sobre concursos públicos e dispõe sobre o Sistema de Organização e Inovação Institucional do Governo Federal – SIORG;
l) Instrução Normativa SLTI/MP nº 05, de 27 de junho de 2014: dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral e suas alterações;

m) Instrução Normativa SEGES/MP n° 05, de 26 de maio de 2017: 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;

n) Instrução Normativa SEGES/ME n° 01, de 10 de janeiro de 2019: dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações;

o) Instrução Normativa SGD/ME nº 01, 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; e

p) Instrução Normativa SGD/ME n° 02, de 4 de abril de 2019: Regulamenta o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013, e dispõe sobre a composição e as competências do Colegiado Interno de Referencial Técnico.

5.1.4.1 Aplicabilidade de normas específicas

5.1.4.1.1 Instrução Normativa SGD n° 05, de 11 de janeiro de 2021

A Instrução Normativa SGD/ME n° 05 de 11 de janeiro de 2021, que atualizou a IN-SGD/ME n° 02/2019, de 04 de abril de 2019[7], "regulamenta o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013, e dispõe sobre a composição e as competências do Colegiado Interno de Referencial Técnico" e regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, relativos a bens e serviços de tecnologia da informação e comunicação – TIC.

A norma, em seu art. 2°, estabelece o seguinte:

> Art. 2º Os órgãos e as entidades previstos no art. 1º deverão submeter à Secretaria de Governo Digital do Ministério da Economia solicitação para aprovação de:
> I - contratações relativas a bens e serviços de TIC, para efeito do disposto no art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, com valor global estimado do objeto superior a 20 (vinte) vezes o previsto no art. 23, inciso II, alínea "c", da Lei nº 8.666, de 21 de junho de 1993; e
> II - formação de atas de registro de preços de serviços de TIC passíveis de adesão por parte de órgãos ou entidades não participantes, para efeito do disposto no art. 22, §10, inciso II, do Decreto nº 7.892, de 23 de janeiro de 2013.
> § 1º Para contratações no sistema de registro de preços, o valor global estimado que trata o inciso I deverá contemplar o montante das demandas dos órgãos participantes da licitação, incluindo os volumes previstos para possíveis utilizações da ata de registro de preços por órgão ou entidade não participante, e considerar a revisão dos valores na forma do art. 120 da Lei nº 8.666, de 1993.
> § 2º Para efeitos do valor referenciado no inciso I considerar-se-ão os valores estimados para a primeira vigência do(s) contrato(s).

Por sua vez, a alínea "c" do inc. II do art. 23 da Lei 8.666/1993 estabelece:

> Art. 23. As modalidades de licitação a que se referem os incisos I a III do artigo anterior serão determinadas em função dos seguintes limites, tendo em vista o valor estimado da contratação: [...]
> II - Para compras e serviços não referidos no inciso anterior: [...]
> c) concorrência - acima de R$ 650.000,00 (seiscentos e cinquenta mil reais).

Ocorre que esses valores foram atualizados pelo Decreto n° 9.412/2018, da seguinte forma:

> Art. 1º Os valores estabelecidos nos incisos I e II do caput do art. 23 da Lei nº 8.666, de 21 de junho de 1993, ficam atualizados nos seguintes termos: [...]
> I - Para obras e serviços de engenharia: [...]
> II - Para compras e serviços não incluídos no inciso I: [...]
> na modalidade concorrência - acima de R$ 1.430.000,00 (um milhão, quatrocentos e trinta mil reais).

Ou seja, devem ser submetidas à apreciação da Secretaria de Governo Digital as contratações de TIC cujo valor estimado do objeto seja superior a R$ 28.600.000,00 (vinte e oito milhões e seiscentos mil reais) e os processos licitatórios que resultem em formação de atas de registro de preços (ARP) que permitam adesão cujo valor estimado seja superior a R$ 9.533.333,33 (nove milhões, quinhentos e trinta e três mil trezentos e trinta e três reais e trinta e três centavos).

Quanto a esses critérios temos que:

a) O valor global estimado da contratação é de R$11.136.326,97;

[7] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=05/04/2019&jornal=515&pagina=58

b) O processo licitatório resultará na formação de Ata de Registro de Preços, porém não será admitida adesão por órgãos não participantes.

Logo, consideramos que a contratação não se enquadra nas hipóteses de submissão aos colegiados previstos na referida norma.

5.1.4.1.2 Portaria STI nº 6.432, de 11 de julho de 2018

A Portaria STI n° 6.432, de 11 de julho de 2018[8], "dispõe sobre a aplicação do Índice de Custos de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências". Considerando a aplicabilidade, o índice de reajuste a ser adotado para o CONTRATO será o ICTI - Índice de Custos de Tecnologia da Informação.

5.1.4.1.3 Portaria STI n° 04, de 6 de março de 2017

A Portaria STI n° 04, de 6 de março de 2017[9], "dispõe sobre recomendações técnicas para mensuração de software ou de resultados de serviços de desenvolvimento, manutenção e sustentação de software no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, e dá outras providências. A contratação em questão não envolve serviços de desenvolvimento e/ou manutenção de software, logo não se aplica o normativo supracitado.

5.1.4.1.4 Portaria STI nº 20, de 14 de junho de 2016

A Portaria STI n° 20, de 14 de junho de 2016[10], "dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências". Considerando a aplicabilidade, a contratação está precedida pelo processo de planejamento alinhado ao Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) do MEC, sendo observados os guias, manuais e modelos publicados pelo Órgão Central do SISP.

5.2 Estimativa do custo total da contratação

A estimativa do custo total da contratação foi elaborada com base nas definições da Instrução Normativa SEGES n° 73, de 5 de agosto de 2020[11], e nas disposições aplicáveis às soluções de Tecnologia da Informação e Comunicação contidas na Instrução Normativa SGD n° 01, de 04 de abril de 2019, cujo resultado encontra-se consolidado no documento PESQUISA DE PREÇOS, anexo à este ESTUDO TÉCNICO PRELIMINAR.

Estimativa de custos da contratação

OBJETO:		Solução de monitoramento de banco de dados					
FONTE DE RECURSOS:		A ser definida quando da efetivação da contratação					
GRUPO	ITEM	DESCRIÇÃO DO ITEM	CATSER	UNIDADE	QUANTIDADE ESTIMADA	VALORES MÁXIMOS ESTIMADOS	
						UNITÁRIO	TOTAL POR ITEM
1	1	Subscrição de solução de software de segurança e monitoração de atividades em banco de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados	24333	Subscrição Anual - Banco de Dados	100	R$89.825,47	R$8.982.547,00
	2	Serviços agregados de operação assistida para a solução de segurança e monitoração de atividades em bancos de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados	27260	Horas de Serviço Técnico	2.016	R$392,00	R$790.272,00
VALOR GLOBAL ESTIMADO:							**R$9.772.819,00**

5.3 Análise de necessidades de adequação do ambiente

5.3.1 Identificação de recursos tecnológicos e materiais necessários à execução do objeto

Para viabilizar a execução contratual será necessária a realização das seguintes adequações ambientais:

[8] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=13/07/2018&jornal=515&pagina=96

[9] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=08/03/2017&pagina=147

[10] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=15/06/2016&pagina=52

[11] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/08/2020&jornal=515&pagina=19

a) Disponibilização de mobiliário (mesas e cadeiras) para a equipe de implantação da solução.

5.3.2 Identificação de recursos humanos necessários à execução do objeto

Para cumprir as atividades de gestão e fiscalização do CONTRATO o CONTRATANTE deverá dispor de servidores (titulares e substitutos) para executar os seguintes papéis:

a) Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;
b) Fiscal Técnico: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;
c) Fiscal Requisitante: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação; e
d) Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

Atualmente, a área requisitante dispõe de servidores em quantidade e capacidade suficientes para a fiscalização de todos os controles, acompanhamento processual e demais atividades necessárias à aferição das exigências contratuais.

5.4 Análise da estratégia de continuidade

Recomenda-se que a vigência do CONTRATO seja fixada em 12 (doze) MESES, podendo ser prorrogado por períodos sucessivos de 12 (doze) meses até o limite de 60 (sessenta) meses, conforme disciplinado no art. 57 da Lei nº 8.666/1993. Com relação à manutenção das condições iniciais de habilitação técnica, a equipe de fiscalização deve atentar-se ao cumprimento do disposto no inc. V do art. 33 da IN-01/2019/SGD:

> Art. 33 O monitoramento da execução deverá observar o disposto no Modelo de Gestão do Contrato, e consiste em: [...]
> V - Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, a cargo dos Fiscais Administrativo e Técnico do Contrato.

A área requisitante deverá realizar contínuo monitoramento da execução contratual, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada. Além disso, deverá atuar no sentido de manter sob seu controle o conhecimento do serviço e dos processos de execução de modo a reduzir o risco de dependência em relação ao fornecedor. Todos os eventos da execução contratual deverão ser apontados em registro histórico adequado. Os RISCOS mapeados estão listados no MAPA DE GERENCIAMENTO DE RISCOS.

6 Declaração de viabilidade da contratação

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICO e REQUISITANTE em harmonia com o disposto no art. 11 da Instrução Normativa nº 01/2019/SGD/ME, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO – uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da contratação exclusivamente para a necessidade de provimento de solução de monitoramento de atividades em bancos de dados (*Database Activity Monitoring* – DAM), portanto a necessidade de provimento de solução de mascaramento e anonimização de dados requer aprofundamento da análise técnica das alternativas já existentes no MEC.

7 Aprovação

Nos termos do §2° do art. 11 da IN-01/2019/SGD, o presente Estudo TÉCNICO PRELIMINAR da Contratação é aprovado e assinado pelos Integrantes TÉCNICO e REQUISITANTE da Equipe de Planejamento da Contratação e pela AUTORIDADE MÁXIMA da Área de TIC.

Brasília/DF, 26 de setembro de 2022.

INTEGRANTE(S) REQUISITANTE(S)	INTEGRANTE(S) TÉCNICO(S)
Titular: Álvaro da Costa Rondon Neto Matrícula SIAPE nº 177484	Titular: Delson Pereira da Silva Matrícula SIAPE nº 2775068
Substituto: Irismar Furtado da Silva Matrícula SIAPE nº 50157	Substituto: Bruno Correa Miranda Matrícula SIAPE nº 2274801

AUTORIDADE DE TIC

André Henrique dos Santos Castro
Subsecretário de Tecnologia da Informação e Comunicação

Documento assinado digitalmente
gov.br
DELSON PEREIRA DA SILVA
Data: 27/09/2022 15:52:18-0300
Verifique em https://verificador.iti.br

Documento assinado digitalmente
gov.br
ANDRE HENRIQUE DOS SANTOS CASTRO
Data: 29/09/2022 10:00:36-0300
Verifique em https://verificador.iti.br

APÊNDICE 01 ANÁLISE COMPARATIVA DAS ALTERNATIVAS IDENTIFICADAS

Análise comparativa das alternativas identificadas

SOLUÇÃO [ALTERNATIVA DE MERCADO]	ADOÇÃO E/OU DISPONIBILIDADE EM OUTROS ÓRGÃOS	ADOÇÃO E/OU DISPONIBILIDADE NO PORTAL DO SOFTWARE PÚBLICO	ADERÊNCIA ÀS POLÍTICAS, PADRÕES E MODELOS DE GOVERNO	NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE	ESPECIFICAÇÃO, COMPOSIÇÃO E/OU CARACTERÍSTICAS	FORMA DE AQUISIÇÃO
Alternativa A – (Item 3.1.1)	Sim	Não se aplica	Não se aplica	Não há necessidade de adequação	Solução composta por aquisição de produtos e serviços	Nova contratação (Licitação)
Alternativa B – (Item 3.1.2)	Sim	Não se aplica	Não se aplica	Há necessidade de adequação	Solução composta por serviços	Nova contratação (Licitação)

APÊNDICE 02 CATÁLOGO DE APLICAÇÕES DE SOFTWARE

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
CEBAS		Sistema WEB Monolítico	Walquíria Freitas de Assis	SERES	PHP 5.2	
SIMEC-Formação Escola da Terra 2.0	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP 5.5	
ABACO	SIGLAS	Sistema WEB (Back+Front)		SE/STIC	JAVA	
apigatewayolinda		WS/API		SE/STIC/CGSTI		
App - Clique Escola		Aplicativo Mobile App	Antonio Ricardo de Morais	SEB/DICAP		
App - e-Proinfo		Aplicativo Mobile App	Antonio Ricardo de Morais	SEB		
App - Educacao Conectada		Aplicativo Mobile App	Antonio Ricardo de Morais	SEB/DARE		
App - IAE		Aplicativo Mobile App	Antonio Ricardo de Morais	SESU		
App - Isf Aluno		Aplicativo Mobile App	Antonio Ricardo de Morais	SESU		
App - ISF Gestão		Aplicativo Mobile App	Antonio Ricardo de Morais	SESU		
App - Mosquito Não		Aplicativo Mobile App	Antonio Ricardo de Morais	SESU		
ASPARLEGIS		Projeto	Murilo Rosa Assunção	GM/ASPAR	PHP 7.1	(PostgreSQL)
bCPF		WS/API	Wisley Alves do Couto	SE/STIC	JAVA	(PostgreSQL)
BIOE		Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB/DARE	JAVA	(PostgreSQL)
BNCC-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SETEC	JOOMLA	
Carolina Bori-Portal		Sítio/Portal Estático	Antonio Ricardo de Morais	SESU	HTML	
CCM-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEALF	JOOMLA	
CEBAS-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SERES	JOOMLA	
CEP		WS/API		SE/STIC/CGS		(PostgreSQL)
CNCT	SISTEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	JAVA	(PostgreSQL 11)
CNRMS		Sistema WEB Monolítico		SESU	PHP	
Dados Abertos-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SE/STIC	JOOMLA	
Diploma Digital-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SESU	JOOMLA	
Dirigentes FNDE / PAR 4	SIMEC-PAR 4	WS/API	Wallace Cardoso Pereira	SE/STIC/CGS	PHP	(PostgreSQL)
E-MEC		Sistema WEB Monolítico	Walquíria Freitas de Assis	SERES	PHP 5.5	(PostgreSQL)
Educação Conectada-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
EnergIF-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SETEC	JOOMLA	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
Étnico Racial-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEMESP	JOOMLA	
FIES-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SESU	JOOMLA	
FIES-Seleção Aluno		Sistema WEB Monolítico	Abda Gouveia de Albuquerque	SESU	PHP 5.6	
FIES-Sistema Oferta		Sistema WEB Monolítico	Abda Gouveia de Albuquerque	SESU	PHP 5.5	
FNE-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
IAE-Portal		Sítio/Portal Estático	Antonio Ricardo de Morais	SESU	HTML	
Intramec		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	GM/ACS	JOOMLA	
ISF Aluno		Sistema WEB Monolítico		SESU	PHP	(Oracle 12c)
ISF Gestão		Sistema WEB Monolítico		SESU	PHP	(Oracle 12c)
ISF-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SESU	JOOMLA	
Machado de Assis-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
MailerMEC		WS/API	Wisley Alves do Couto	SE/STIC/CGS	PHP 7.4	
NovoPepb		Projeto	Keyla Cristina dos Santos	SEB	PHP 7.1	
Novos Caminhos-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SETEC	JOOMLA	
NOVOSISTEC		Projeto	Shirlane Maria de Sousa Pereira	SETEC	JAVA	
novowsmec		WS/API	Wisley Alves do Couto	SE/STIC/CGS	PHP 7.4	
Olinda	apigatewayolinda	Cliente/Servidor		SE/STIC/CGS		
Pacto Ensino Médio-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
PDDE Campo e Água na Escola	PDDE Interativo	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEB	PHP	(PostgreSQL)
PDDE Interativo		Sistema WEB Monolítico	Gabriela Miranda dos Santos	SEB	PHP 5.5	(PostgreSQL)
PDDE Interativo-Administrativo	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-BNCC	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-Educação Conectada PIEC	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
PDDE Interativo-Escola Acessível	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
PDDE Interativo-formularios	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-Gestão Escolar	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-Livro	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
PDDE Interativo-Mais Alfabetização	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
PDDE Interativo-Melhores Receitas	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-Novo Ensino Médio	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
PDDE Interativo-Novo Mais Educacao	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
PDDE Interativo-PDDE Interativo 2012	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-PDDE Interativo 2013	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-PDDE Interativo 2014	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-PDDE Interativo 2015/2016	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
PDDE Interativo-ProEMI	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-REUNI	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE Interativo-SIS	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDDE-Sala de Recursos	PDDE Interativo	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
PDE Escola-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
PEC-G		Sistema WEB Monolítico		SESU	PHP 5.6	
PEC-G 2.0		Projeto		SESU		
PGD.MEC	PGD.MEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGGP	DOT.NET	(SQL Server 2017)
Plano de Carreira-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
Plataforma Carolina Bori		Sistema WEB Monolítico		SESU	PHP 5.4	(Oracle)
PNA-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEALF	JOOMLA	
PNE-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SE	JOOMLA	
PNLD Avaliação		Projeto	Keyla Cristina dos Santos	SEB	PHP 7.1	
PNP	SISTEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	JAVA	(PostgreSQL)
PNP-Portal		Sítio/Portal Estático	Antonio Ricardo de Morais	SETEC	HTML	
Portal MEC		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	GM/ACS	JOOMLA	
PPB-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEB	JOOMLA	
Presença		Sistema WEB Monolítico	Gabriela Miranda dos Santos	SEB	PHP 5.5	(SQL Server)
ProExt-Portal		Sítio/Portal Estático	Antonio Ricardo de Morais	SESU	HTML	
Pronacampo-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SEMESP	JOOMLA	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
ProUni-Gestão		Sistema WEB Monolítico	Alexandre Feijó Valente	SESU	PHP 7.1	
ProUni-Inscrição		Sistema WEB Monolítico	Alexandre Feijó Valente	SESU	PHP 7.1	
Prouni-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SESU	JOOMLA	
RAMEC		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SE/STIC	JOOMLA	
REUNI-Portal		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	SESU	JOOMLA	
SAE		Sistema WEB Monolítico	Murilo Rosa Assunção	SE	PHP 5.5	(PostgreSQL 9.4)
SEI		Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA	PHP 5.6	(SQL Server 2012)
SGC		Projeto	Murilo Rosa Assunção	SE/STIC	PHP	
SICMERCOSUL		Sítio/Portal Dinâmico	Antonio Ricardo de Morais	GM	JOOMLA	
SIGLAS		Sistema WEB Monolítico	Wagner de Paula Pereira	SE/STIC/CGS	DOT.NET	(SQL Server 2017)
SIGPET		Sistema WEB Monolítico		SESU	PHP 5.2	(PostgreSQL)
SIMEC		Sistema WEB Monolítico	Geraldo Afonso da Cruz	SE/STIC	PHP 5.5	(PostgreSQL)
SIMEC-+PNE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Agenda GM	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-ApiObrasVistoria	SIMEC	WS/API	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-ASPAR	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM/ASPAR	PHP	
SIMEC-Assessoria Internacional	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-Brasil Profissionalizado	SIMEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	PHP	
SIMEC-CAP	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-Catálogo Curso	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Catálogo Curso 2013	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-CONJUR	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM/CONJUR	PHP	
SIMEC-CONJUR V2	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM/CONJUR	PHP	
SIMEC-Contrato Gestão	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA	PHP	
SIMEC-CTEL	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA	PHP	
SIMEC-Demandas	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SIMEC-Demandas SE	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE	PHP	
SIMEC-E.I Manutenção Proinfância	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
SIMEC-Educação Conectada	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB/DARE	PHP 5.5	
SIMEC-EJA Novas Turmas	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SIMEC-Emendas	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM/ASPAR	PHP	
SIMEC-EMTI	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SIMEC-Ensino Médio Inovador	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Ensino Médio Inovador(antigo)	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Escola	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Escolas Exterior	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Exames do MEC / INEP	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	INEP	PHP	
SIMEC-Fábrica	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP 5.5	
SIMEC-Formação Escola da Terra 2014	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-Formação Escola da Terra 2015	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-Formação Escola da Terra 2016	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-Formação Escola da Terra 2017	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-Gerência de Projetos	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SIMEC-Gestão de Demandas SERES	SIMEC	Sistema WEB Monolítico	Walquíria Freitas de Assis	SERES	PHP	
SIMEC-Gestão de Tarefas	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SIMEC-Gestão Gabinete	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-Livros	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB/DARE	PHP 5.5	
SIMEC-Mais Cultura	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Mais Médicos	SIMEC	Sistema WEB Monolítico		SESU	PHP	
SIMEC-MM-Avaliação	SIMEC	Sistema WEB Monolítico		SESU	PHP	
SIMEC-Monitoramento de Obras 2.0	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-Obras 2.0	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-Pacto Universitário	SIMEC	Sistema WEB Monolítico		SESU	PHP	
SIMEC-PAR - Plano de Metas	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-PAR 2	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-PAR 3	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
SIMEC-PAR 4	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SIMEC-PDE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PDU	SIMEC	Sistema WEB Monolítico		SESU	PHP	
SIMEC-Planejamento e Monitoramento Estratégico	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-PNBE TEMÁTICO	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PNLD	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PRIL	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Projetos Especiais	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-ProJovem Campo	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SIMEC-ProJovem Urbano	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SIMEC-ProjovemCampoE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-ProjovemUrbanoE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PROJUR / INEP	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	INEP	PHP	
SIMEC-PROVA	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PSE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-PTO	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	INEP	PHP	
SIMEC-Publicidade	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	GM	PHP	
SIMEC-RAIZ	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SIMEC-Receitas Orçamentárias v2	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP	
SIMEC-REHUF	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	EBSERH	PHP	
SIMEC-REUNI	SIMEC	Sistema WEB Monolítico		SESU	PHP	
SIMEC-RSC	SIMEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	PHP	
SIMEC-SAP	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA	PHP	
SIMEC-SASE	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SCA	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA	PHP	
SIMEC-SIC	SIMEC	Sistema WEB Monolítico	Walquíria Freitas de Assis	SERES	PHP 5.5	
SIMEC-SIGEPE	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGGP	PHP	
SIMEC-SIS	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
SIMEC-SIS V2	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SIMEC-SISCAP	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGGP	PHP	
SIMEC-SISFOR	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP 5.5	
SIMEC-SISFOR V2	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-Sisindígena	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP 5.5	
SIMEC-SISIndígena 2014	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-SISIndígena 2015	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-SISIndígena 2016	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-SISIndígena 2018	SIMEC	Sistema WEB Monolítico	Ivania de Souza e Silva Sena	SEMESP	PHP	
SIMEC-SISMédio	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISPACTO 2013	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISPACTO 2014	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISPACTO 2015	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISPACTO 2016	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISPACTO 2017	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SISREQ	SIMEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	PHP	
SIMEC-Sistema Administrativo (Compras / Eventos / Contratos)	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGLC	PHP 5.5	
SIMEC-Sistema de Capacitação para Servidores do MEC	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGGP	PHP 5.5	
SIMEC-Sistema de Gestao de Pessoas	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SAA/CGGP	PHP 5.5	
SIMEC-Sistema de Monitoramento de Obras	SIMEC	Sistema WEB Monolítico	Maria Tereza Matos Bezerra	FNDE	PHP 5.5	
SIMEC-Sistema de Seguranca	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE	PHP 5.5	
SIMEC-Sistema Painel de Controle	SIMEC	Sistema WEB Monolítico	Walquíria Freitas de Assis	SE/SPO	PHP 5.5	
SIMEC-Sistema Rede Federal	SIMEC	Sistema WEB Monolítico		SESU	PHP 5.5	
SIMEC-SNF	SIMEC	Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP	
SIMEC-SPO - Execução Orçamentária	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP	
SIMEC-SPO - Limites Orçamentários	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP	
SIMEC-SPO - Painel de Controle	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP	
SIMEC-SPO - PPA-Monitoramento e Avaliação	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP	

Sistema	Sistema Relacionado	Tipo	Gerente	Área Gestora	Tecnologia	Banco de Dados
SIMEC-SPO - Proposta Orçamentária	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP	
SIMEC-SPO Acompanhamento Orcamentário	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO Emendas Parlamentares	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO Planejamento Orcamentario	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO Programacao Financeira	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO Receitas Orcamentarias	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO SICAJ Acoes Judiciais	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-SPO TED	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/SPO	PHP 5.5	
SIMEC-Treinamento	SIMEC	Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	PHP	
SINAR		Sistema WEB Monolítico		SESU	PHP 5.5	(Oracle)
SIPI		Sistema WEB Monolítico	Keyla Cristina dos Santos	SEB	PHP 5.5	
SISALFA		Sistema WEB (Back+Front)	Ivania de Souza e Silva Sena	SEALF	PHP 7.1	(PostgreSQL)
SISBP		Sistema WEB Monolítico		SESU	PHP 5.6	
SISCEBAS3	CEBAS	Projeto	Walquíria Freitas de Assis	SERES	PHP 7.1	
SisCNRM		Sistema WEB Monolítico		SESU	PHP 5.5	
SisFundApoio		Sistema WEB (Back+Front)		SESU	JAVA	
SISTEC	SISTEC	Sistema WEB Monolítico	Shirlane Maria de Sousa Pereira	SETEC	PHP 5.6	(PostgreSQL)
SISU-Gestao		Sistema WEB Monolítico		SESU	PHP 5.6	(Oracle)
SISU-Inscricao		Sistema WEB Monolítico		SESU	PHP 7.1	
SISU-Portal		Sítio/Portal Dinâmico		SESU	JOOMLA	
SSD		Sistema WEB Monolítico	Murilo Rosa Assunção	SE/STIC	JAVA	(PostgreSQL)

APÊNDICE 03 ESPECIFICAÇÃO TÉCNICA PRÉVIA DA SOLUÇÃO

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1	REQUISITOS ESPECÍFICOS
1.1	Deve ser nova, do último modelo disponível, em linha de fabricação na data da entrega e deve pertencer à última geração na respectiva linha de produtos do fabricante.
1.2	A solução deve estar licenciada para monitorar e proteger pelo menos 100 (cem) bancos de dados, suportando SQL Server, MySQL, Postgre, MariaDB e Oracle.
1.3	A solução será composta de equipamentos baseados em uma plataforma de appliances (hardware e software de propósito específico ou servidores virtuais) do mesmo fabricante e a solução deve incluir funcionalidades de auditoria e proteção de dados (firewall ou bloqueio). Esses recursos devem ser fornecidos sem a necessidade de instalação de software e / ou hardware em qualquer equipamento adicional que não faça parte da solução.
1.4	Para as soluções que são baseadas em servidores virtuais, de modo a não violar as restrições de arquitetura de TI do Ministério da Educação, a Contratada deverá fornecer a infraestrutura de servidores necessária com sistema operacional compatível, instalado e devidamente licenciado, devendo-se observar a necessidade do fornecimento conjunto do suporte para o período do contrato.
1.5	A solução oferecida deve ter o suporte correspondente do fabricante, para serviços de garantia de hardware, manutenção de software e suporte técnico.
1.6	O equipamento oferecido deve ser um aparelho de finalidade específica para DBF, projetado e fabricado para o setor empresarial.
Características mínimas do equipamento	
1.7	Deve ser capaz de executar todas as funções de aprendizagem, análise e proteção do tráfego SQL considerando pelo menos uma capacidade de processamento de 5.000 SQLHits /s ou TPS (transações por segundo) (O fabricante deve fornecer documentação de apoio por folha de especificações técnicas oficiais de fábrica e caractere público que indica a capacidade de processamento do tráfego SQL do appliance de DBF proposto, incluindo tarefas de aprendizado e de estresse).
1.8	Deverá possuir 16GB de RAM por dispositivo (em casos de appliances físicos).
1.9	Deverá possuir discos e fontes de alimentação redundantes (em casos de appliances físicos).
1.10	Deve ter pelo menos 4 interfaces de cobre de 1 Gbps, com a opção de ativar 4 interfaces de fibra de 1 Gbps ou 2 interfaces de fibra de 10 Gbps, todas com capacidade de falha de abertura (bypass) (em casos de appliance físico).
1.11	Deve ter uma interface de console (tipo RJ45) para administração (em caso de appliance físico).
1.12	Deve ter duas interfaces de 1Gbps para administração de rede IP (em caso de appliance físico).

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.13	Deve ter uma porta USB (em caso de appliance físico).
Implantação da solução	
1.14	Em caso de fornecimento de Appliance Físico a implantação da solução deverá ser feita no modo Bridge 2 da camada para Auditoria e Bloqueio e implantação de agentes nos servidores base somente para auditório local. A plataforma deve ter a possibilidade de alterar o modo de implementação de rede se for necessário que a entidade no futuro seja capaz de integrar a rede no modo bridge (camada 2 do Modelo OSI, as interfaces não requerem um endereço IP) e as interfaces devem incluir o bypass / failopen / failclose integrado ao Appliance e configurável para falhas de hardware e software.
1.15	A solução deve ter um impacto no nível de sub-milissegundo ou milissegundo na latência da rede.
1.16	O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM).
1.17	As equipes devem suportar o protocolo de gerenciamento de rede SNMP e SYSLOG a ser monitorado por ferramentas de terceiros e e-mails, se necessário.
Funcionalidades de monitoração e segurança	
1.18	A solução deve ter tecnologia de autoaprendizagem, o processo deve ser constante e deve aprender estrutura de bancos de dados, incluindo esquemas, objetos, tabelas; sistemas, aplicações, campos, diretórios, bem como o comportamento de cada usuário; tudo isso para o estabelecimento de um monitoramento e segurança de linha de base.
1.19	O modo de aprendizagem pode ser ativado e desativado manualmente para estender o tempo de reconhecimento dos padrões de comportamento.
1.20	A solução deve fornecer proteção por meio de bloqueios e alertas contra violações de segurança devido a ataques conhecidos, atividades suspeitas ou qualquer atividade específica a ser definida.
1.21	A solução deve ter a capacidade de suportar os mecanismos de banco de dados disponíveis para a entidade e os mecanismos de banco de dados comerciais, entre os quais no mínimo: MS-SQL, MySQL, Oracle, Postgresql.
1.22	A solução deve gerar relatórios e tendências em tempo real, bem como permitir a modificação e customização dos mesmos.
1.23	O appliance de gateway, em primeira instância, executará as funções de proteção de banco de dados, mas é exigida pela entidade que o mesmo appliance suporte no futuro as funcionalidades de proteção de arquivos e aplicativos da Web com integração nativa do mesmo fabricante da solução. Para ativar essas funcionalidades, a entidade deve exigir apenas o provisionamento do software de licenciamento que permite ativar as funções de proteção de aplicativos da Web e arquivos.
1.24	A solução deve ter instalações ou ferramentas analíticas para a realização de análise forense quando um incidente é relatado.
1.25	A solução não deve instalar apenas agentes leves de software nos servidores a serem monitorados para executar as funções de firewall do banco de dados.
1.26	A solução deve ser transparente para o banco de dados e / ou para os aplicativos que o acessam, ou seja, não exigirá alterações na programação, configuração ou operação (gatilhos, procedimentos armazenados, etc.) de nenhum deles.
1.27	O repositório para o registro da atividade no dispositivo não deve ser acessível por nenhum outro mecanismo além da interação através da GUI (interface gráfica) fornecida pelo fabricante ou por meios administrativos devidamente assegurados.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.28	A solução deve ser capaz de descobrir servidores de banco de dados e realizar análises de vulnerabilidades no software de gerenciamento de banco de dados, através de um único agente leve instalado no servidor pelo protocolo de comunicação e configuração de segurança, independentemente do sistema operacional no qual eles estão instalados.
1.29	A solução deve realizar uma avaliação de risco abrangente da infraestrutura de destino em diferentes níveis / camadas da infraestrutura de banco de dados, incluindo:
1.29.1	Problemas de configuração da plataforma, incluindo a configuração do sistema operacional dos servidores que suportam o software de banco de dados.
1.29.2	Problemas de configuração do banco de dados, como nível de correção, configuração de contas de usuário, avaliação da força das senhas, validade das senhas.
1.30	A solução deve fazer descobertas automatizadas na rede para identificar novos bancos de dados que estão sendo habilitados, no nível do servidor ou portas ativadas em servidores conhecidos.
1.31	A solução deve ter a capacidade de analisar e classificar os tipos de dados nos bancos de dados de acordo com as políticas de negócios. As definições de tipo de dados devem poder ser criadas de maneira flexível e granular.
1.32	A solução deve fornecer um serviço de proteção para o software de banco de dados através da aplicação de patches virtuais que permitem atacar as vulnerabilidades encontradas no referido software, independentemente da liberação da correção ou atualização do fabricante.
1.33	A solução deve apoiar os esforços de análise de vulnerabilidades, configuração de segurança, comportamento / desempenho de aplicativos e controle de alterações.
1.34	O módulo de gerenciamento do ciclo de vida da vulnerabilidade será acessado a partir do mesmo console de administração do sistema, sem necessidade de produtos ou consoles adicionais para essa finalidade.
1.35	A solução deve monitorar toda a atividade dos bancos de dados e deve armazenar os comandos SQL da maneira como foram escritos pelo usuário ou pelo aplicativo, incluindo os comandos DDL, DML e DCL.
1.36	A solução deve monitorar e interagir com a atividade do banco de dados, independentemente do ponto de entrada, seja conexões diretas, servidores de aplicativos, acesso direto ao banco de dados, links, procedimentos armazenados, entre outros.
1.37	A solução deve analisar e auditar todo o tráfego em tempo real, independentemente do volume de tráfego.
1.38	A solução deve ter a capacidade de monitorar o tráfego mascarado e/ou tokenizado para os bancos de dados.
1.39	A solução deve fornecer detalhes sobre alertas, sejam eles falsos ou negativos, e deve ter a facilidade de alterar uma política do alerta.
1.40	A solução deve lidar com regras e políticas tão amplas ou detalhadas quanto necessário e deve poder ser construída automaticamente ou manualmente e deve poder ser atualizada, manual ou automaticamente.
1.41	As políticas granulares para controle de acesso ou geração de alertas devem ter os seguintes critérios para a validação da atividade no aplicativo Banco de Dados. Os critérios devem ser usados em qualquer número e qualquer combinação:
1.41.1	Número de registros a serem retornados pela consulta (Consulta SQL)
1.41.2	Número de registros afetados

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
Tipo de dados acessado	
1.42	Acesso aos dados marcados como sensíveis
1.43	Banco de dados, esquema, instância, tabela e coluna acessados
Status de autenticação da sessão	
1.44	Usuário e / ou grupo de usuários do banco de dados conectado
1.45	Logins, Logout, Consultas
IPS de origem e destino	
1.46	Origem do nome do host, usuário assinado na origem do host
1.47	Aplicativo usado para conexão com o banco de dado
1.48	Tempo de resposta / processamento de consultas
Erros no driver do SQL	
1.49	Número de ocorrências em intervalos de tempo definidos
1.50	Por operações básicas (Select, Insert, Update, Delete)
1.51	Por operações privilegiadas (Criar, Alterar, Derrubar, Conceder, Revogar, Truncar, Exportar)
1.52	Por procedimento armazenado ou função usada
1.53	Se houver um ticket atribuído para mudanças
Hora do dia	
1.54	A solução deve identificar individualmente os usuários finais que realizam atividades por meio de aplicativos, mesmo que usem mecanismos de comunicação comuns entre o aplicativo e o banco de dados; essa atividade não deve envolver a modificação do aplicativo e / ou do banco de dados.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.55	A solução deve permitir análises históricas e em tempo real sob demanda, ou seja, sem ter que passar por um processo em lote anterior.
1.56	A solução deve associar e correlacionar eventos que individualmente não constituam um risco, mas que, juntos, são indicativos de uma possível violação de segurança.
1.57	A solução deve proteger contra-ataques SQL e não SQL (como estouro de buffer)
1.58	Consideração de emergência por possíveis violações das informações que incluem, mas não se limitam a:
1.58.1	Alto volume de acesso a dados sensíveis além do usual.
1.58.2	Acesso a dados incomuns para uma determinada hora do dia.
1.58.3	Acesso a dados de um local desconhecido (físico).
1.58.4	Acesso a dados usando aplicativos / ferramentas não autorizadas.
1.59	A solução deve lidar com uma auditoria sobre si mesma, mantendo um controle de alterações nas políticas e configurações autorizadas.
1.60	A solução deve ter recursos para arquivamento de informações históricas e de auditoria, com flexibilidade de protocolo ou opções de mídia (como SAN ou via FTP, HTTP, NFS, SCP).
1.61	A solução deve ter a capacidade de exportar dados e eventos, como alertas, eventos de sistema e banco de dados, informações / administração de segurança, entre outros, para outras ferramentas de administração através dos protocolos SNMP e Syslog.
1.62	A solução deve ter a capacidade de monitorar usuários de banco de dados que tenham acesso por meio de aplicativos da Web, oferecendo visibilidade, segurança e controle do usuário da Web ao banco de dados sem alterar a arquitetura dos aplicativos ou as bases de dados.
1.63	A solução deve ter um serviço de pesquisa sobre vulnerabilidades e ameaças de computador, para o qual deve apresentar a respectiva documentação na descoberta do mesmo sem que a entidade tenha que investir em software adicional para ter essa funcionalidade.
1.64	A solução deve ter um módulo de gerenciamento de vulnerabilidades para os sistemas e não deve exigir a instalação de um segundo agente nos servidores de banco de dados para essa funcionalidade.
1.65	A solução deve analisar os eventos gerados a partir de diferentes bancos de dados.
1.66	A solução deve permitir o gerenciamento de alarmes e notificações - em tempo real - para os eventos de correlação aos critérios de análise.
Critérios para análise dos eventos	
1.67	Deve mostrar o número de eventos que ocorreram, o número de usuários suspeitos e / ou os sistemas comprometidos.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.68	Deve ter um sistema de correlação baseado na direção dos ataques. Você deve determinar se os ataques vêm de dentro ou de fora da organização.
1.69	Deve executar uma correlação automática e em tempo real de eventos, vulnerabilidades e bancos de dados.
1.70	Deve executar uma correlação que permita identificar usuários de aplicativos associados a consultas - e determinadas atividades - em bancos de dados específicos, sem a necessidade de alterar aplicativos ou instalar APIs.
1.71	Deve correlacionar eventos, como o número de erros incomuns de instruções SQL ou ao efetuar login em bancos de dados.
Modelo de segurança	
1.72	A solução deve suportar e aplicar simultaneamente um modelo de segurança positivo e negativo.
1.73	O modelo de segurança negativo define explicitamente as assinaturas de ataques conhecidos, e deve atender às seguintes especificações:
1.73.1	Bloquear transações que tenham conteúdo que corresponda a assinaturas de ataque conhecida.
1.73.2	Incluir uma lista pré-configurada e detalhada de assinaturas de ataque.
1.73.3	Permitir a modificação ou adição de assinaturas pelo administrador.
1.73.4	Permitir a atualização automática do banco de dados de assinatura, garantindo proteção completa contra as ameaças de aplicativos mais recentes.
1.73.5	Detectar ataques conhecidos em vários níveis, incluindo a rede, sistemas operacionais, software de servidor da Web e ataques em nível de aplicativo.
1.74	A solução deve contemplar mecanismos que permitam facilmente o retorno de uma política de segurança implementada em um aplicativo.
1.75	Para as funcionalidades de Bloqueio, é necessário que os requisitos sejam processados na memória e não no disco, pois este último modo de operação gera latência no serviço de consulta ao banco de dados, a latência gerada pela operação de proteção deve ser menor que 5 mil segundos.
1.76	Para funcionalidades de bloqueio, a solução nunca deve encerrar a conexão que é gerada entre o cliente e o servidor, definindo como cliente um usuário com uma conexão ODBC para o banco de dados ou um servidor de aplicativos.
Relatórios	
1.77	Permitir a geração de relatórios, de todos os alertas de segurança, nos formatos PDF e CSV.
1.78	Permitir que a escolha da informação seja incluída nos relatórios, com a possibilidade de selecionar os itens.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.79	Capacidade de automatizar a geração de relatórios e sua submissão subsequente por e-mail.
Console de gestão e administração centralizada	
1.80	A solução deve ser gerenciada por uma console de gerenciamento centralizada no formato de appliance (físico ou virtual) da mesma marca dos componentes WAF e DBF, que permite a centralização de políticas, relatórios, revisão de auditoria, monitoramento, eventos de segurança, gerenciamento de os diferentes componentes da solução e o monitoramento de seu status, desempenho, etc.
1.81	Os consoles de gerenciamento devem ter pelo menos as seguintes características (quando forem físicos):
1.81.1	Tem duas (02) 100/1000 interfaces Ethernet Base-TX para gerenciamento off-band.
1.81.2	Ter um mínimo de 16GB de RAM.
1.81.3	2 TB de disco rígido.
1.81.4	“Rackável” em gabinete de 19 "com o respectivo suprimento de acessórios.
1.82	A solução deve incluir um servidor de administração central no qual o software de administração e os arquivos de log gerados pelos diferentes componentes da solução residem.
1.83	O equipamento de administração deve fazer backup diário em forma automática de todas as informações nele armazenadas, incluindo as configurações de todos os módulos gerenciados e ter a capacidade de transferi-los automaticamente para um servidor remoto usando os protocolos SCP e FTP.
1.84	Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração.
1.85	A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um protocolo seguro com mascaramento e/ou tokenização e autenticação por usuários locais, incluindo a possibilidade de usar certificados digitais.
1.86	A solução de administração deve permitir a atribuição de perfis de administração pelos usuários e esses perfis devem permitir a separação das funções de gerenciamento e monitoramento.
1.87	Fornecer uma visão centralizada dos logs, entendida como tal, a unificação dos logs de todos os componentes da solução.
1.87.1	Ser capaz de ser transferido para o servidor de administração.
1.87.2	Ser capaz de ser transferido para o servidor de administração ao mesmo tempo em que é gerado, sem atrasar o início da transferência.
1.87.3	Capacidade de ser exportada do servidor de administração para um formato SYSLOG ou SNMP TRAPS, para poder usar ferramentas de análise de terceiros.
1.88	Os logs de todos os componentes da solução devem atender às seguintes características:

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
1.88.1	As equipes devem poder armazenar os logs localmente, nos casos em que houver problemas na comunicação com o servidor central.
1.88.2	A solução de gerenciamento permitirá a visualização em tempo real dos logs de atividades das equipes da solução e as modificações de configuração que os administradores podem fazer.
1.88.3	Permitir que um usuário da solução defina quais transações serão registradas.
1.89	A solução de administração permitirá, no mínimo:
1.90	Adicionar, excluir ou modificar a configuração em um ambiente gráfico.
1.90.1	Modifique as regras dos diferentes equipamentos.
1.90.2	Execute a configuração dos componentes da solução.
1.90.3	Visualize registros de auditoria, alertas de segurança e eventos do sistema.
1.90.4	Gerar relatórios ajustáveis pelo usuário.
1.90.5	Permitir a geração de relatórios, de toda a atividade registrada nos logs, nos formatos PDF e CSV.
1.90.6	Permitir que a escolha da informação seja incluída nos relatórios.
1.90.7	Capacidade de automatizar a geração de relatórios e sua submissão subsequente por e-mail.
1.90.8	Suportar a geração de eventos de segurança, incluindo o aplicativo do usuário, se isso realmente tiver sido registrado.
1.90.9	Identifique os resultados de autenticação em formulários e seja capaz de impedir ataques de dicionário contra formulários.
A-2	SUPORTE TÉCNICO E GARANTIA
2.1	São previstos como serviços de SUPORTE TÉCNICO, manutenção e apoio:
2.1.1	Manutenção Preventiva: Compreende visitas mensais periódicas, in loco no ambiente da contratante, programadas a fim de verificar a saúde do equipamento e mitigar riscos devido ao uso continuado dos serviços, incluindo:
2.1.1.1	Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
2.1.1.2	Realização de inspeções nos equipamentos, componentes, dispositivos e softwares de configuração gerenciam a solução.
2.1.1.3	Verificação mensal com vistas a manter sua plena funcionalidade e saúde dos equipamentos.
2.1.1.4	Análise de logs de sistema e sugestão de mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da CONTRATANTE decidirá sobre a aplicação ou não das recomendações.
2.1.1.5	Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.
2.1.1.6	Executar procedimentos e resolver problemas relacionadas com configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento da solução de segurança previstos no processo e deverá fazer o ajuste fino (tunning) e as customizações de configuração de toda a solução deste processo, adequando-a ao ambiente do MEC.
2.1.1.7	Definir e implantar as rotinas de backup de todos os equipamentos componentes da solução de segurança. Nesse sentido, será responsabilidade da CONTRATADA o backup realizado pela própria.
2.1.2	Manutenção Corretiva: Compreende visitas pontuais, a partir de abertura de chamados advindos do contratante, a fim de atuar em incidentes ou problemas identificados que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada do fabricante, incluindo:
2.1.2.1	Reinstalação de hardware e softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços por ele prestados.
2.1.2.2	Reparar, corrigir, remover, refazer ou substituir, no todo ou em parte, os serviços, peças ou materiais em que se verificarem imperfeições, vícios, defeitos ou incorreções, dentro dos prazos estabelecidos nos demais subitens contratados.
2.1.2.3	Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências do MEC, de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes.
2.1.2.4	Substituir eventuais equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos.
2.1.2.5	Detectar problemas e limitações de desempenho da solução de DAM relacionados a software e/ou firmware instalado nos elementos que fazem parte do objeto desta contratação, substituindo-os por nova versão que implemente suas correções.
2.1.2.6	Substituir software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação por nova versão eventualmente lançada, quando esta implementar correções a possíveis problemas ou limitações de desempenho das SOLUÇÕES.
2.2	Os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser prestados pela empresa contratada na forma on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento das soluções
2.3	Todos os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser executados por técnicos qualificados e com certificação comprovada pelo fabricante da Solução, pertencentes ao quadro de funcionários da CONTRATADA, sem custos adicionais para o CONTRATANTE, durante todo o período de garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual.
2.4	A comprovação de validade da certificação e comprovação de vínculo empregatício deverão ser apresentados juntamente com o cronograma anual de visitas programadas ou sempre que o técnico credenciado for substituído, podendo ainda, ser solicitada a qualquer momento pela CONTRATANTE.
2.5	Os serviços de Suporte Técnico Especializado, Manutenção e Apoio, quando presencial deverá ser prestado no endereço local do CONTRATANTE ou outro indicado por ele. Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário devem ser substituídos pela CONTRATADA, sem nenhum custo adicional a CONTRATANTE.

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
2.6	Para a prestação dos serviços de Suporte Técnico Especializado, Manutenção e Apoio a CONTRATADA deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pelo MEC, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros. Quando a intervenção implicar interrupção da solução ADC, mesmo que parcial, o MEC poderá determinar que a CONTRATADA a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional ao MEC.
2.7	É expressamente vedada a desativação de hardware, software ou quaisquer recursos computacionais da CONTRATANTE, sem prévio conhecimento e autorização expressa do CONTRATANTE. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais do MEC, a CONTRATADA deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato. Em caso da necessidade de retirada do equipamento, o MEC poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional.
2.8	Havendo necessidade de substituição de hardware (equipamentos), a CONTRATADA deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o CONTRATANTE, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:
2.8.1	Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias.
2.8.2	Caso ocorram problemas recorrentes no mesmo hardware, seja na restauração ou na substituição de peças, assim considerada como recorrente a repetição de uma mesma falha em um intervalo inferior a 2 (dois) meses.
2.8.3	O(s) equipamento(s) (hardware) empregado(s) em substituição ao(s) equipamento(s) defeituoso(s) deverá(ão) possuir prazo de garantia equivalente àquela prevista no CONTRATO.
2.9	Ao término de cada evento de suporte técnico e manutenção, deverá ser gerado e entregue um Relatório de Atendimento Técnico (RAT) com as seguintes características:
2.9.1	Entregue à equipe técnica da CONTRATANTE em até 5 (cinco) dias após o serviço realizado pela CONTRATADA. A CONTRATANTE dará ciência no documento após análise e aceitação do seu conteúdo,
2.9.2	Indicação do tipo de serviço de suporte e manutenção realizado, bem como toda a verificação realizada.
2.9.3	Registro com a identificação do equipamento (nome/modelo/série).
2.9.4	Descrição clara do (s) problema(s) identificado(s), os procedimentos adotados para a sua resolução e o tempo de resolução para o chamado.
2.10	Mensalmente, deverá ser entregue um RELATÓRIO GERENCIAL indicando todos os eventos de suporte técnico e manutenção atendidos no período, seguidos de todos os Relatórios de Atendimento Técnicos (RAT) elaborados e aceitos. O Relatório Gerencial mensal deverá conter no mínimo:
2.10.1	Identificação individual dos chamados atendidos no período;
2.10.2	Identificação individual do equipamento ou solução;
2.10.3	Identificação individual do tipo de atendimento;
2.10.4	Datas de atendimento (abertura e conclusão);
2.10.5	Descrição dos atendimentos;

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
2.10.6	Procedimentos adotados para a solução do problema.
2.11	Sem prejuízo da entrega do Relatório Gerencial, o CONTRATANTE poderá solicitar, em formato digital, informações analíticas e sintéticas dos chamados técnicos abertos e fechados no período.
2.12	As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso do MEC durante todo período contratual e sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, a última versão vigente na data do término do contrato.
2.13	Caso a CONTRATADA não seja a própria fabricante do equipamento, ela deverá observar, obrigatoriamente:
2.13.1	Apresentar documentação de que adquiriu os componentes da solução por meio de canais oficiais do fabricante, referenciando números de série desses componentes.
2.13.2	Apresentar contrato ou documentação equivalente que comprove que a CONTRATADA poderá recorrer ao fabricante para resolução de problemas, com SLA compatível com a vigência da garantia e os tempos de atendimento exigidos neste Termo de Referência;
2.13.3	Permitir que o MEC acione o fabricante diretamente para chamados de suporte e manutenção dos equipamentos e sistemas que compõem a solução durante a vigência da garantia.
2.13.4	O documento comprobatório deverá ter como signatário representante do fabricante e vir acompanhado de procuração pública ou particular com firma reconhecida, contrato social ou estatuto, atesando que o signatário tem o poder para assinar tal compromisso ou responder pelo fabricante.
2.13.5	O documento comprobatório deverá estar expresso em Português ou, se o documento apresentado tiver sido redigido em outra língua que não seja a língua portuguesa, deverá trazer obrigatoriamente a tradução juramentada do mesmo.
2.13.6	O fabricante signatário do documento comprobatório deverá possuir representação legal no Brasil.
2.14	Para aferição dos níveis de serviço o tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade, bem como se entende por término do reparo do equipamento a sua disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado, e o tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.
2.15	Visando a garantir a disponibilidade e o atendimento dos níveis de serviço a CONTRATADA poderá, às suas expensas e sem custo adicional ao CONTRATO, fazer uso de mais de 2 equipamentos (1 cluster) para garantir redundância de fontes e discos, garantindo o pleno funcionamento de todos os equipamentos, softwares e licenças que compõem a solução.
2.16	Os chamados técnicos deverão ser atendidos e solucionados levando em consideração os itens abaixo, referente aos níveis mínimos de serviço:
2.16.1	Tempo de Atendimento: 2 (duas) horas.
2.16.2	Tempo de Solução: 24 (vinte e quatro) horas
2.16.3	Quando não for possível solucionar o problema no prazo estipulado, deverá ser fornecido outro equipamento de igual configuração ou superior, até a resolução definitiva do problema.
2.17	Durante a execução dos serviços de suporte técnico, somente poderão ser utilizadas peças e componentes novos e originais.
2.18	Durante todo o período da prestação de serviços de garantia e suporte técnico, a CONTRATADA deverá fornecer ao CONTRATANTE um login de acesso personalizado ao sítio internet do fabricante, onde deverá ser possível acompanhar a validade garantia do equipamento e, em área própria para o modelo ofertado, recursos para consulta e download de:

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
2.18.1	Softwares, drivers e firmwares (atualizações e/ou versões completas).
2.18.2	Manuais de usuário e dos equipamentos
2.18.3	Banco de solução para suporte ao software e hardware instalados de fábrica.
A-3	TREINAMENTO
3.1	O TREINAMENTO deverá possuir carga horária mínima de 40:00 (quarenta horas) e deverá ser realizado em Brasília/DF em turma fechada de até 6 (seis) participantes com emissão de certificado de participação, sendo que, a critério do CONTRATANTE, poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação (limitando-se a 4 participantes adicionais do tipo "ouvintes").
3.2	Em sua PROPOSTA, as LICITANTES deverão fazer constar informações quanto à identificação do treinamento e seu conteúdo preliminar, observando o currículo oficial do fabricante da solução. Considerando também que todas as despesas referentes à realização do treinamento ou ao custeio de insumos deverão estar inclusas no preço contratado.
3.3	O CONTRATANTE solicitará a realização do treinamento à CONTRATADA por e-mail ou outro mecanismo de comunicação formal, sendo que este deverá ser iniciado em até 90 (noventa) dias corridos após a solicitação e o período e local de realização informados com antecedência mínima de 30 (trinta) dias da data do evento.
3.4	A CONTRATADA deverá comprovar, previamente à realização do evento, que o(s) INSTRUTOR(ES) selecionado(s) para ministrar o treinamento possuem qualificação condizente com o conteúdo programático a ser ministrado, incluindo certificados ou declaração do fabricante dos equipamentos que integram a Solução de ADC (ou documento equivalente).
3.5	O CONTRATANTE poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca de instrutor ou equipamentos de laboratório. Caso a deficiência não possa ser sanada sem prejuízo para o andamento do curso, esse será suspenso pelo MEC, devendo a CONTRATADA agendar novo curso, sem ônus adicional para o MEC.
3.6	O treinamento deverá, ainda, observar o seguinte:
3.6.1	Possuir o conteúdo do treinamento organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação;
3.6.2	Incluir apostilas e manuais dos equipamentos e softwares necessários para a prática dos exercícios propostos no material oficial do fabricante;
3.6.3	Prover os equipamentos que irão compor o laboratório do treinamento que deverão ser iguais aos adquiridos pelo MEC ou, quando não for possível, por equipamentos similares com as mesmas funcionalidades;
3.6.4	Abranger todas as funcionalidades especificadas nesta especificação técnica;

Item 1: Subscrição de Solução de software de segurança e monitoração de atividades em banco de dados	
3.6.5	Serem fornecidos certificados de participação para cada participante (exceto para aqueles na condição de ouvintes);
3.6.6	Todos os manuais, apostilas e demais documentos devem estar nos idiomas Português (ou Inglês, quando não disponíveis em Português); e os cursos devem ser ministrados no idioma Português.
3.7	Após realização do curso será feita uma avaliação de satisfação junto aos participantes, cujo resultado deverá alcançar a média de, pelo menos, 70% (setenta por cento) de satisfação dentre os critérios avaliados, para validação e emissão do Termo de Aceite Definitivo. Caso não alcance o resultado esperado, o treinamento deverá ser ministrado novamente.

Item 2: Serviços agregados de Operação Assistida	
1	REQUISITOS DE EXECUÇÃO
1.1	As Horas de Serviços Técnicos de Operação Assistida serão utilizadas sob demanda, a critério do CONTRATANTE, para realização das atividades relacionadas às soluções fornecidas.
1.2	O período de execução do serviço de operação assistida dar-se-á imediatamente após o serviço de instalação e ativação da solução de Monitoramento de Atividades de banco de dados. Neste período a CONTRATADA deverá executar atividades relacionadas ao “fine tuning” da solução, aplicando ajustes, correções e customizando as soluções para as necessidades do Ministério da Educação.
1.3	Os serviços de operação assistida incluem no mínimo as seguintes atividades:
1.3.1	Execução de atividades operacionais, utilizando os procedimentos mais adequados e adaptados à realidade do ambiente do CONTRATANTE;
1.3.2	Execução de atividades de rotinas de testes, análises e medidas, utilizando procedimentos que assegurem uma mínima interferência na operação e máxima disponibilidade da solução;
1.3.3	Elaboração de procedimentos especiais ou detalhamento de procedimentos padrão, documentados e adaptados à realidade do ambiente do CONTRATANTE;
1.3.4	Elaboração de relatórios de atividades, detalhando os procedimentos realizados e eventuais ajustes, se necessário.

Item 2: Serviços agregados de Operação Assistida	
1.4	Benefícios esperados:
1.4.1	Garantia de que a solução seja operada seguindo procedimentos de melhores práticas;
1.4.2	Redução da curva de aprendizado e transferência de conhecimento para a equipe do CONTRATANTE;
1.4.3	Melhor performance e disponibilidade da solução;
1.4.4	Redução de impacto de implantação e melhorias, com menores índices de incidentes gerados em função de mudanças;
1.4.5	Padronização de procedimentos, possibilitando que o CONTRATANTE execute as atividades operacionais com sua própria equipe;
1.4.6	Procedimentos em conjunto com o fabricante da solução, para situações em que o ambiente do CONTRATANTE esteja sob ataque, destinado a prover o conhecimento para as medidas necessárias à defesa do ambiente;
1.4.7	Procedimentos de ajuste para manter a solução adquirida pelo CONTRATANTE provendo a melhor utilização de suas funcionalidades.
1.5	Reuniões técnicas, mensais ou a critério do CONTRATANTE, para planejamento e execução de serviços com vistas à melhoria do ambiente instalado.
1.6	Reuniões gerenciais, mensais ou a critério do CONTRATANTE, para avaliação e acompanhamento dos serviços oferecidos.
1.7	Entrega de relatórios ao final do período de operação assistida, contendo informações sobre atividades desenvolvidas e recomendações sobre como melhor utilizar a tecnologia.
1.8	Sempre que necessário, a CONTRATADA deverá efetuar vistoria técnica nas dependências do CONTRATANTE de modo a realizar análise e implementar as alterações necessárias.

Item 2: Serviços agregados de Operação Assistida	
1.9	O serviço de operação assistida deverá ser prestado de forma presencial no endereço local do CONTRATANTE ou outro indicado por ele.
1.10	Para atendimento ao serviço de operação assistida a CONTRATADA somente poderá empregar profissionais capacitados e certificados nos produtos fornecidos.
1.11	O CONTRATANTE oficializará a solicitação deste apoio por meio da emissão de uma "Ordem de Serviço – OS", de acordo com o modelo do Termo de Referência.
1.12	A Ordem de Serviço deverá conter no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados.
1.13	Os serviços prestados deverão estar no mínimo de acordo com as especificações constantes na Ordem de Serviço.
1.14	O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo CONTRATANTE, durante a execução – com o acompanhamento e supervisão de responsáveis do CONTRATANTE, e ao término da execução – com o fornecimento de "Relatórios de Atividade da Operação Assistida" pela CONTRATADA e atesto dos mesmos por responsáveis do CONTRATANTE.
1.15	A partir da emissão da "Ordem de Serviço – OS", a CONTRATADA terá até 05 (cinco) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um atendimento imediato de manutenção corretiva ou prioridade alta do CONTRATANTE;
1.16	O CONTRATANTE comunicará à CONTRATADA quando uma "Ordem de Serviço – OS" estiver sendo elaborada para que a CONTRATADA possa se manifestar no interesse de agendamento de reunião para definição de procedimentos e horas necessárias para execução dos serviços.
1.17	As horas e procedimentos previstos inicialmente quando da abertura da "Ordem de Serviço – OS" serão validados no final das atividades e poderão sofrer adequações para estarem de acordo com o que foi efetivamente executado.
1.18	Este serviço deve estar disponível para acionamento no sistema 24 horas por dia x 7 dias por semana.

APÊNDICE 04 RESUMO DA ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Grupo	Item	Descrição	Catser/Catmat	Unidade	Quantidade	MENOR VALOR		MÉDIA		MEDIANA	
						Valor Unitário	Valor Total	Valor Unitário	Valor Total	Valor Unitário	Valor Total
1	1	Subscrição de solução de software de segurança e monitoração de atividades em banco de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados	24333	Subscrição Anual - Banco de Dados	100	R$89.825,47	R$8.982.547,00	R$99.941,82	R$9.994.182,33	R$95.000,00	R$9.500.000,00
	2	Serviços agregados de operação assistida para a solução de segurança e monitoração de atividades em bancos de dados (*Database Activity Monitoring* - DAM), conforme requisitos especificados	27260	Horas de Serviço Técnico	2.016	R$392,00	R$790.272,00	R$566,54	R$1.142.144,64	R$518,00	R$1.044.288,00
					Valor Global Estimado >>>	R$9.772.819,00		R$11.136.326,97		R$10.544.288,00	

ICP Brasil

Documento assinado digitalmente

ALVARO DA COSTA RONDON NETO

Data: 27/09/2022 14:32:07-0300

Verifique em https://verificador.iti.br