MINISTÉRIO DA CIDADANIA

Histórico de Revisões

Data	Versão	Descrição	Autor
10/09/2021	1.0	Finalização da primeira versão do documento	Juliana Rocha Munita Moreira

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA – DOD

INTRODUÇÃO

Em conformidade com o art. 10 da Instrução Normativa SGD/ME n° 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução.

Referência: Art. 10 da IN SGD/ME nº 01/2019.

PREENCHIMENTO PELA ÁREA REQUISITANTE

1. IDENTIFICAÇÃO DA ÁREA REQUISITANTE

Área Requisitante (Unidade/Setor/Departamento): SE/STI	
Responsável pela demanda: Daniel Portilho Troncoso	**Matrícula/SIAPE: 1775726**
E-mail: daniel.troncoso@cidadania.gov.br	**Telefone: 2030-3056**

2. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE

Nome: Juliana Rocha Munita Moreira	**Matrícula/SIAPE: 1816396**
Cargo: Chefe de Divisão II	**Lotação: SE/STI/CGGTI**
E-mail: juliana.munita@cidadania.gov.br	**Telefone: 2030-3056**

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para
exercer esse papel na Equipe de Planejamento da Contratação.

Brasília/DF, 13 de setembro de 2021.

Juliana Rocha Munita Moreira

3. IDENTIFICAÇÃO DA DEMANDA

Necessidade de Contratação:

Este documento apresenta a necessidade de implementação de uma ferramenta de mascaramento de dados.

Devido ao aumento exponencial da informatização dos processos e do volume de informações e dados pessoais processados atualmente, aumentou também a preocupação com a exposição indevida dessas informações. O vazamento dessas informações pode causar todo o tipo de prejuízo, desde danos à imagem e até mesmo perdas financeiras por multas/indenizações por divulgação de informações sigilosas ou sensíveis dos cidadãos. Além disso, os recentes ataques cibernéticos aumentam o risco de acontecer vazamento dos dados.

Assim, o mascaramento de dados passou a ser um controle fundamental para a segurança dos dados pessoais. Quando ocorre vazamento de informações ou dados pessoais, sem os sistemas apropriados de segurança cibernética, é muito difícil identificar se foi por negligência ou por procedimentos e controles de segurança da informação inadequados. Um dos primeiros passos para aumentar os níveis de segurança é restringir o acesso às informações e dados pessoais. O mascaramento de dados é uma forma de restringir acesso a essas informações, aumentando a segurança de que nenhum dado real seja divulgado ou acessado indevidamente.

3.1 - A contratação pretende substituir contrato vigente? Informar nº do contrato e processo.
Não.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos - Plano Estratégico Institucional (PEI 2019-2022)**
Objetivo Estratégico 2.1	Aprimorar estruturas e mecanismos de governança e gestão.
Objetivo 3.2.	Prover soluções logísticas e tecnológicas integradas, seguras e de alto desempenho.
Meta 3.2.2.	Estabelecer procedimentos de gestão de riscos específicos para processos e projetos de TI.
	Disseminar o uso de ferramentas de TI avançadas no âmbito do

Meta 3.2.3.	Ministério.
Meta 3.2.4.	Estabelecer processos de capacitação para o uso mais intensivo e eficaz de ferramentas de TI pelo corpo técnico do Ministério.

Objetivos Estratégicos da Estratégia de Governo Digital (EGD 2020-2022)	
Item	**Descrição**
Objetivo 10	Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal
Iniciativa 10.1.	Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020.
Iniciativa 10.2.	Estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

Política de Governança de Tecnologia da Informação
Descrição
Contratação alinhada à Política de Governança de Tecnologia da Informação do órgão, instituída pela Portaria nº 162, de 10 de fevereiro de 2017, publicada no Diário Oficial da União em 13 de fevereiro de 2017.

Plano Estratégico de Tecnologia da Informação (PETI 2021-2022)	
Item	**Descrição**
Mapa Estratégico - Resultados	Ampliar e fortalecer a transparência e confiabilidade dos serviços e soluções de TI que suportam os processos de negócio e promover a privacidade dos dados pessoais.
Mapa Estratégico - Processos Internos -	Aprimorar as práticas e os controles de segurança da informação e de proteção de dados pessoais
Eficiência Operacional	Promover a privacidade desde a concepção e durante todo o ciclo de vida do tratamento dos dados pessoais

ALINHAMENTO AO PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO (PDTI 2021-2022)	
ID	**Objetivos Estratégicos**
OETI02	Prover sistemas e soluções de TI alinhadas às necessidades das áreas de negócio
OETI04	Aprimorar as práticas e os controles de Segurança da Informação e de proteção de dados pessoais
OETI10	Promover a privacidade desde a concepção e durante todo o ciclo de

OBJETO	vida do tratamento dos dados pessoais

ID	Necessidade de TI	
NL1 a NL40	Prover licenciamento de ferramentas de apoio às atividades das áreas de negócio	
ID	**Ação do PDTI**	**Meta do PDTI associada**
NL.M1	Adquirir, manter e atualizar os softwares e ferramentas	Elaborar Planejamento das Contratações de TI
		Realizar a contratação dos bens/serviços
		Implantar bens/serviços na infraestrutura de TI
		Executar os serviços de desenvolvimento
		Homologar produtos/entregáveis
		Implantar a demanda em produção
ID	**Necessidade de TI**	
NG5	Aprimorar os processos de gestão de segurança da informação e de proteção de dados pessoais	
ID	**Ação do PDTI**	**Meta do PDTI associada**
NGX.M1	Identificar os ativos de informação que dão suporte aos dados pessoais tratados pela STI	Mapear e inventariar os ativos de informação e dados pessoais
NGX.M3	Implementar e melhorar os controles de segurança da informação e de proteção de dados pessoais	Implementar ou melhorar os controles de segurança da informação e de proteção de dados de acordo com o plano de tratamento dos riscos.

ALINHAMENTO AO PLANEJAMENTO ANUAL DE CONTRATAÇÕES (PAC 2021)	
Item	**Descrição**
849	Mascaramento de Dados

4. MOTIVAÇÃO/JUSTIFICATIVA

Os ativos de informação e os dados pessoais ocupam papel de importância estratégica nas organizações. O uso inadequado desses recursos, portanto, oferece elevado risco de impactos negativos e podem resultar em consequências indesejadas,

tais como: prejuízo financeiro, problemas operacionais, danos à imagem do órgão ou governo, vazamento de informações e dados pessoais, sequestro de dados.

A informação deve ser tratada como um recurso estratégico e econômico devido à crescente valorização da informação e dos dados pessoais como principais ativos de gestão do Estado, além das crescentes transações bilaterais com suporte de TI.

No âmbito da Administração Pública Federal (APF), a manutenção de níveis adequados de segurança da informação e de proteção de dados pessoais é de suma importância para se assegurar o fornecimento adequado de serviços públicos aos cidadãos. Não menos importante, esta manutenção contribui para evitar atos criminosos realizados em ambientes virtuais da APF, e os consequentes danos ao Estado e à Sociedade.

Transações eletrônicas, muitas vezes, implicam na movimentação de expressivas quantias de valores financeiros. Esse fato, entre outros, atrai a atenção de organizações criminosas, cuja atuação pode comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações e dos dados pessoais sob custódia do Estado, gerando impactos negativos, tais como: comprometimento da imagem organizacional, insegurança dos usuários, sequestro de dados, prejuízos financeiros.

Desse modo, tratar de forma correta e eficaz os eventos adversos de segurança cibernética tornou-se um desafio para organizações públicas e privadas, considerando que os dados e informações constituem recursos de extrema relevância para a consecução das suas missões institucionais.

Nesse contexto, o mascaramento de dados é de fundamental importância para mitigar os danos causados por ataques cibernéticos. A implementação de uma ferramenta de mascaramento de dados aumenta o nível de maturidade de segurança da informação, protegendo as informações e dados pessoais de acesso ou divulgação indevidos.

Tratar de forma correta e eficaz a ocorrência de eventos adversos de segurança da informação, portanto, tornou-se uma necessidade tanto para empresas do setor privado, quanto para os órgãos públicos, considerando que o comprometimento ou violação de informações podem acarretar danos a pessoas, organizações e mesmo nações.

A implementação de uma ferramenta de mascaramento de dados tem como objetivo a segurança de dados confidenciais contra acessos não autorizados. Na prática, tal ferramenta cria uma versão de estrutura semelhante aos dados originais, mas sem revelar a verdadeira informação. O formato original mantém-se inalterado, porém os dados apresentados são fictícios. O mascaramento pode ser utilizados em diversos ambientes e não compromete o resultado da análise, mas garante a confidencialidade da informação sensível. Um processo manual para segurança de dados consome muito tempo, recursos humanos e não é eficiente.

Conforme demonstram as informações divulgadas pelo Cert.br, os ataques e incidentes de segurança têm aumentado a cada ano. As organizações, porém, são cobradas no tocante à segurança das informações e da proteção de dados pessoais, quer seja de sua propriedade, quer esteja sob sua custódia. Nesse contexto, a segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade.

Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar grandes prejuízos e falta de novas oportunidades de desenvolvimento e de oferta de serviços à sociedade. A Administração Pública Federal – APF faz parte desta realidade.

Além disso, estar em conformidade com a legislação vigente sobre segurança cibernética e sobre proteção de dados...

FUNDAMENTAÇÃO LEGAL

1. Lei de Acesso à Informação (LAI)

De acordo com art. 23 da Lei, pode ser classificada a informação que, dentre outras:

> "c) coloca em risco a vida, a segurança ou a saúde da população;
> d) causa risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, ou a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
> e) põe em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares."

De acordo com o art. 24, § 5°, da Lei de Acesso, a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerando a gravidade do risco ou dano à segurança da sociedade e do Estado.

A LAI determina que as informações pessoais são aquelas relacionadas à pessoa natural identificada ou identificável. As informações relativas à intimidade, vida privada, honra e imagem das pessoas devem ter seu acesso restrito por até 100 anos (art. 31, §1°, I da Lei nº 12.527), independentemente de classificação, e só podem ser acessadas pela própria pessoa; por agentes públicos legalmente autorizados; por terceiros autorizados diante de previsão legal ou consentimento expresso da pessoa a que as informações se referirem.

2. Lei de Proteção de Dados Pessoais (LGPD)

Em se tratando de dados pessoais, a Lei nº 13.709, de 14 agosto de 2018, que é a Lei Geral de Proteção de Dados Pessoais (LGPD), em que podemos destacar a importância da Segurança da Informação na Proteção dos Dados Pessoais.

A LGDP foi criada com a intenção de proteger os dados pessoais de um indivíduo, com grande destaque para a privacidade. Contudo, a segurança da informação é disciplinada pela LGDP em vários pontos, tais como acesso, tratamento, riscos, incidentes, continuidade, responsabilidades e responsabilização. Assim, a segurança da informação tornou-se uma obrigação específica, deixando de ser um meio, muitas vezes opcional, para ser uma finalidade em si mesma.

Podemos tomar como exemplo o inciso VII do artigo 6º da LGDP, que

estabelece os princípios básicos da utilização e tratamento de dados prevê a segurança de dados como um de seus pilares, da seguinte forma:

> " VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"
> "X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Além disso, não se trata apenas de um princípio, mas de uma obrigação, prevista no artigo 46 da LGPD:

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

O referido artigo é um dos itens a ser considerado pela Autoridade Nacional de Proteção de Dados em caso de sanção administrativa, que calculará eventual pena com base em diversos fatores, entre eles, a adoção de mecanismos de segurança de informação (artigo 52, inciso VIII):

> "VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei".

O Art. 23 da LGPD dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> "I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;"

3. Política Nacional de Segurança da Informação (PNSI)

São princípios da PNSI, conforme Art. 3º:

> "II - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade (grifo nosso) e o acesso à informação;
> VIII - orientação à gestão de riscos e à gestão da segurança da informação;
> IX - prevenção e tratamento de incidentes de segurança da informação;
> X - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;
> XI - dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo

das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

XII - need to know para o acesso à informação sigilosa, nos termos da legislação (Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação – conforme descrito na NC 07/IN01/DSIC/GSIPR);

XIV - cooperação entre os órgãos de investigação e os órgãos e as entidades públicos no processo de credenciamento de pessoas para acesso às informações sigilosas."

Em conformidade com o Art. 4º, são objetivos da PNSI, dentre outros:

"I - contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;

II - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;

VI - orientar ações relacionadas a:

a) segurança dos dados custodiados por entidades públicas;

b) segurança da informação das infraestruturas críticas;

c) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica; e

d) tratamento das informações com restrição de acesso."

De acordo com o Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:

V - destinar recursos orçamentários para ações de segurança da informação;

VII - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais, que comporá a rede de equipes formada pelos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República;

Compete à alta administração dos órgãos e das entidades da administração pública federal a governança da segurança da informação, e especialmente, de acordo com o Art. 17:

"I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

IV - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;

V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

VII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;

IX - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal;

X - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos neste Decreto e na legislação.

§ 1º O planejamento e a execução de programas, de projetos e de processos relativos à segurança da informação de que trata o inciso IV do caput serão orientados para:

I - a utilização de recursos criptográficos adequados aos graus de sigilo exigidos no tratamento das informações e as restrições de acesso estabelecidas para o compartilhamento das informações, observada a legislação;
II - o aumento da resiliência dos ativos de tecnologia da informação e comunicação e dos serviços definidos como estratégicos pelo Governo federal."

As considerações acima expostas caracterizam a necessidade de implementação de uma ferramenta de mascaramento de dados no Ministério da Cidadania.

5. RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

Com o mascaramento de dados é possível aumentar os níveis de segurança da informação, de maturidade na proteção de dados e de conformidade com a legislação vigente. Além disso, um dos principais benefícios é a confidencialidade das informações mascaradas. Ao mascarar os dados, o Ministério da Cidadania demonstra preocupação e responsabilidade pelos dados pessoais dos cidadãos sob sua custódia. Além disso, podemos destacar:

a) A segurança da informação é reforçada contra acessos não autorizados, evitando o vazamento de informações e dados pessoais;

b) Há otimização de tempo ao não realizar o processos de segurança manuais, além de reduzir os riscos de erro humano;

c) Aumento da maturidade de governança de dados, sendo que as soluções de mascaramento funcionam com dispositivos de escaneamento e classificação de dados, descobrindo de maneira automática e programada os campos com dados sensíveis;

d) Aumenta a positividade da imagem institucional demonstrando preocupação e responsabilidade pelas informações dos cidadãos sob a custódia do ministério;

e) Segurança na movimentação de dados, evitando o acesso a dados de informações pessoais por desenvolvedores ou demais usuários com acesso privilegiado.

f) Aumento da 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;

g) Aumento da conformidade com a Lei de proteção geral de dados (LGPD).

6. FONTE DE RECURSOS

Plano Interno (PI) M20004160BY.

ENCAMINHAMENTO

Encaminhe-se ao Subsecretário de Tecnologia da Informação para providências.

Brasília/DF, 13 de setembro de 2021.

Maurício Bucciolli Guernelli

Documento assinado eletronicamente por **Juliana Rocha Munita Moreira, Analista de Tecnologia da Informação – ATI**, em 13/09/2021, às 16:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

Documento assinado eletronicamente por **Mauricio Bucciolli Guernelli, Coordenador(a)-Geral de Governança de Tecnologia da Informação**, em 13/09/2021, às 18:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

Documento assinado eletronicamente por **Daniel Portilho Troncoso, Subsecretário(a) de Tecnologia da Informação, Adjunto**, em 14/09/2021, às 17:32, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

A autenticidade deste documento pode ser conferida no site https://sei.cidadania.gov.br/sei-autenticacao , informando o código verificador **11028822** e o código CRC **A29A6ADA**.

Referência: Processo nº 71000.063315/2021-49 SEI nº 11028822

MINISTÉRIO DA CIDADANIA
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA – DOD

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME n° 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
15/09/2021	1.0	Finalização da primeira versão do documento.	Alessandro Dantas

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

1. AVALIAÇÃO QUANTO AO ALINHAMENTO DA CONTRATAÇÃO AO PDTIC E AO PLANO ANUAL DE CONTRATAÇÕES

Conforme as informações dispostas no Documento de Oficialização de Demanda (SEI nº 11028822), referente à necessidade de implementação de uma ferramenta de mascaramento de dados, a pretensa contratação encontra-se devidamente alinhada aos instrumentos de planejamento no Ministério da Cidadania.

2. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome: Felipe Velter Teles	**Matrícula/SIAPE:** 2862331
Cargo: Analista em Tecnologia da Informação	**Lotação:** STI/CGGDI
E-mail: felipe.teles@cidadania.gov.br	**Telefone:** (61) 2030-1767
Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação. **FELIPE VELTER TELES**	

3. JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS

Não se aplica.

4. ENCAMINHAMENTO

Encaminhe-se à autoridade competente da Área Administrativa, que deverá:

I. Decidir motivadamente sobre o prosseguimento da contratação;

II. Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e

III. Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10.

ALESSANDRO DANTAS
Subsecretário de Tecnologia da Informação

Documento assinado eletronicamente por **Felipe Velter Teles, Integrante Técnico**, em 20/09/2021, às 13:34, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

Documento assinado eletronicamente por **Alessandro Franca Dantas, Subsecretário(a) de Tecnologia da Informação**, em 20/09/2021, às 17:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

A autenticidade deste documento pode ser conferida no site https://sei.cidadania.gov.br/sei-autenticacao , informando o código verificador **11080358** e o código CRC **54221B4B**.

Referência: Processo nº 71000.063315/2021-49 SEI nº 11080358

MINISTÉRIO DA CIDADANIA
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE ASSUNTOS ADMINISTRATIVOS
DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA – DOD

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME n° 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

<As atividades atribuídas à autoridade da Área Administrativa poderão ser realizadas em documentos apartados (como Despacho ou Portaria), e devem ser incluídos no processo administrativo da contratação>.

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

8 - DECISÃO DA AUTORIDADE COMPETENTE

Com base no Documento de Oficialização da Demanda - REQUISITANTE (SEI n º 11028822), a contratação de ferramenta de mascaramento de dados, visando à implementação das disposições da Lei de Proteção de Dados Pessoais (LGPD), foi devidamente analisada pela Subsecretaria de Tecnologia da Informação, que emitiu o Documento de Oficialização da Demanda (STI) (SEI nº 11080358).

Nestes termos, encaminho os autos à Coordenação-Geral de Licitações e Contratos - CGLC para **prosseguimento** da contratação e:

I. Análise quanto à melhor modalidade de licitação;

II. Indicação do integrante administrativo;

III. Elaboração da Minuta de portaria de designação da Equipe de Planejamento da Contratação conforme indicações das áreas requisitante e técnica.

Conforme o art. 29, § 8º da IN SGD/ME nº 01/2019, a Equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato.

Assinado eletronicamente
PAULA NUNAN
Subsecretária de Assuntos Administrativos - Substituta

Documento assinado eletronicamente por **Paula Nunan, Subsecretário(a) de Assuntos Administrativos, Substituto(a)**, em 21/09/2021, às 11:30, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

Estudo Técnico Preliminar 41/2021

1. Informações Básicas

Número do processo: 71000.063315/2021-49

2. Descrição da necessidade

Segundo a IN SGD/ME nº 1/2019, 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 da contratação. Tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

3. Área requisitante

Área Requisitante	Responsável
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO	ALESSANDRO DANTAS

4. Necessidades de Negócio

Identificação das necessidades de negócio

Aprimorar os processos de gestão de segurança da informação e de proteção de dados pessoais.

Permitir 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).

Apresentar cópias de dados reais, com dados sensíveis anonimizados, isolados do ambiente produtivo, garantindo assim a máxima fidelidade e usabilidade dos dados para fins de desenvolvimento, teste, análises de negócio ou qualquer outro caso em que o dado real (todo ou em parte) não seja necessário.

Entregar cópias de dados de forma rápida, econômica e segura, sem a necessidade de realização de operações manuais de gerenciamento de dados, visando a simplificação do processo de disponibilização de dados.

Gerar dados realísticos, como nomes, documentos e endereços nacionais, utilizando outros métodos de anonimização dos dados além das cadeias aleatórias de caracteres.

Permitir identificar e mascarar dados de documentos nacionais, como CPF, CNPJ, RG, RENAVAM, placas veiculares, bem como nomes, endereços, correios eletrônicos, além dos dados mais comuns cobertos pela LGPD, com flexibilidade para inclusão de dados sensíveis ou confidenciais específicos do Ministério da Cidadania.

Manter, ao mascarar dados de documentos nacionais, a consistência de dígitos verificadores ou da estrutura de matriz e filial (no caso do CNPJ).

Possuir flexibilidade de customização, possuindo, além de pacotes específicos para dados mais comuns cobertos pela LGPD, flexibilidade para inclusão de dados sensíveis ou confidenciais específicos do negócio.

Permitir a integração com os principais bancos de dados atualmente em uso no Ministério da Cidadania, bem como com arquivos de dados não estruturados.

Realizar o processo de mascaramento de forma integrada ao processo de distribuição e apresentação dos dados.

Fornecer todas as funcionalidades de forma integrada, sem a necessidade de aquisições avulsas de funcionalidades, permitindo o acesso irrestrito e ilimitado do Ministério da Cidadania à solução, independentemente da quantidade de usuários internos necessários para sua operação ou uso.

5. Necessidades Tecnológicas

REQUISITOS TÉCNICOS E FUNCIONAIS DA SOLUÇÃO

1. Permitir que os usuários obtenham os dados de que precisam, quando precisam, de forma intuitiva, prática, flexível e célere, a ponto de ser realizada por usuários finais, e de forma a consumir o mínimo de espaço possível.

2. Apresentar cópias de dados reais, com dados sensíveis anonimizados, isolados do ambiente produtivo, garantindo assim a máxima fidelidade e usabilidade dos dados para fins de desenvolvimento, teste, análises de negócio ou qualquer outro caso em que o dado real (todo ou em parte) não seja necessário, contemplando minimamente informações referentes aos documentos e endereços nacionais.

3. Possuir interface simples e voltada ao usuário final, não necessitando de conhecimento técnico ou de sistemas operacionais ou de bancos de dados pelos usuários finais, bem como permitir que o usuário final opere sua própria cópia de banco de dados, possibilitando, no mínimo, as seguintes operações: restauração da cópia com dados em ponto-do-tempo e marcação da cópia para restauração em ponto de controle.

4. Apresentar, como resultado final de uma nova cópia de banco de dados, um novo banco de dados aberto e em funcionamento, mascarado ou não, segundo políticas configuradas pelo Ministério, sem necessidade de intervenção direta de administradores de bancos de dados para apresentação ao usuário final.

5. Permitir que sejam criadas cópias de bancos de dados com base em outras cópias já existentes, mascaradas ou não, segundo políticas de acesso, e não apenas baseadas em cópias diretas do banco de dados de produção.

6. Não aumentar o volume inicial de sua origem, qual seja, com campos sensíveis ou confidenciais mascarados ou não segundo políticas determinadas pelo Ministério.

7. Todas as operações descritas nos itens anteriores devem também fornecer a opção de escolher um determinado ponto no tempo a partir do qual a cópia será feita.

8. As operações de provisionamento de cópias e restauração de cópias não devem necessitar de intervenção direta pela equipe de bancos de dados, salvo em casos excepcionais.

9. Permitir a realização do mascaramento concomitantemente ao processo de provisionamento de cópias virtuais de dados, sendo garantido que caso o processo de mascaramento falhe, o provisionamento seja interrompido, revertendo para o último mascaramento bem-sucedido disponível, não permitindo a apresentação de dados parcialmente mascarados, impedindo a distribuição de cópias com dados sensíveis.

10. Ser capaz de permitir o funcionamento de cópias de bancos de dados (mascaradas ou não) mantendo seus arquivos nos discos da própria ferramenta.

11. Apresentar um endereçamento ágil da proteção de dados sensíveis em ambientes não produtivos.

12. Possuir, de forma integrada, as funcionalidades de identificação de dados sensíveis, de mascaramento e distribuição de cópias fiéis de dados, e de anonimização de informações sensíveis ou confidenciais.

13. Cadeias aleatórias de caracteres não serão permitidas como método de anonimização dos dados.

14. Possuir capacidade de identificar e mascarar automaticamente os diferentes tipos de documentos, mesmo quando misturados em um mesmo campo, sem a necessidade de intervenção manual do usuário.

15. Possuir flexibilidade de mascaramento de endereços, sendo possível configurar facilmente através de interface gráfica *Web* quais campos serão alterados ou não (logradouro, bairro, cidade, estado, país, CEP), mantendo consistência dos dados quando for pertinente (por exemplo, gerando CEP e Cidade válidos para um determinado Estado).

16. Apresentar cópias com diferentes níveis de mascaramento, a ser definido pelos perfis de acesso, sem impactar o tempo de apresentação dos dados para o usuário final. Exemplo: para fins de análise de negócio, podem ser mantidos intactos dados

referentes a valores e localização, porém anonimizadas informações pessoais como nomes e documentos. Para fins de desenvolvimento e teste por uma fábrica de software, todos os dados devem ser anonimizados, porém realistas (nome, endereço, documento, valores etc.)

17. Distribuir diversas cópias de dados mascarados sem impacto no tempo de apresentação ou necessidade de realizar o processo de mascaramento novamente.

18. Possuir processos para administração da distribuição e mascaramento integrados e centralizados.

19. Ser capaz de executar o processo de mascaramento repetidas vezes, e de maneira consistente.

20. Ser capaz de proteger dados confidenciais através de mecanismo de tokenização, para fins de backup, réplicas através de redes públicas ou qualquer tipo de transporte de dados.

21. Ter função de replicação e apresentação ágil de cópias protegidas entre diferentes Data Centers e/ou plataformas de nuvem, com graus configuráveis de proteção e anonimização de dados, segundo políticas de segurança definidas pelo Ministério.

22. Prover agilidade e controle de versões dos dados, trazendo para essa camada os conceitos de bookmarks, branches, rollback e compartilhamento.

23. Otimizar a utilização da infraestrutura de tecnologia existente, permitindo maior densidade de dados em menos servidores, com indicadores claros e de comum conhecimento pela área de TI.

24. Permitir a realização do mascaramento irreversível do dado (sobrescrição do dado).

25. Possuir rastreabilidade (na mesma ferramenta) por meio da geração automática de relatórios e alertas para garantir que todos os dados sensíveis foram mascarados.

26. Permitir o envio automático de mensagens eletrônicas ao término da operação de cópia avisando o término da operação.

27. Possuir integridade referencial, que consiste na identificação e mascaramento de dados consistentes entre ambientes de dados heterogêneos.

28. Garantir a integridade referencial dos dados sem a necessidade de declaração de modelo relacional, nem formalização de chaves referenciais.

29. Garantir imprevisibilidade e aleatoriedade da geração dos novos dados através da renovação de chaves criptográficas sob demanda.

30. Criar cópias de bancos de dados sem a obrigatoriedade de aquisição ou utilização direta de outras ferramentas de backup próprias ou de terceiros.

31. Apresentar bancos de dados em poucos servidores, consolidando a infraestrutura de ambientes não produtivos.

32. Permitir que o provisionamento ou atualização de cópias de dados afetem minimamente o desempenho de servidores de produção.

33. Suportar ambientes de dados heterogêneos, provendo a compatibilidade com as diversas plataformas de dados, sem cobrança adicional por conectores.

34. Realizar cópias de dados, estruturados ou não, com eficiência de armazenamento, não devendo um mesmo bloco ser armazenado em disco mais de uma vez, segundo o conceito de desduplicação.

35. Compartilhar dados entre cópias, ou seja, dados comuns entre cópias de dados não devem ser duplicados. O compartilhamento de dados entre cópias significa que cópias idênticas de um mesmo conjunto de dados devem sempre ocupar o mesmo espaço em disco, e não múltiplas vezes o volume de dados (que teriam caso fossem cópias tradicionais).

36. Ter, para qualquer grupo de dados gerenciado pela solução, a funcionalidade de recomposição para um momento de tempo (rollback).

37. Permitir a criação de cópias-mestres (versões de armazenamento temporário), mascaradas ou não, para uso posterior em clone de bases de acordo com as necessidades do usuário.

38. Deve fornecer uma SDK para estender suporte a outras plataformas não especificadas neste documento que o Ministério venha a usar no futuro.

39. Deve eliminar ou reduzir a quantidade de blocos temporários ou vazios, filtrando os dados que serão preservados e otimizando consumo de espaço de armazenamento de bancos de dados nos ambientes gerenciados pela ferramenta.

40. Suportar uma arquitetura de alta disponibilidade e redundância através de replicação dos ambientes de dados.

41. Possuir capacidade de replicar dados mascarados de forma seletiva, sendo possível excluir dados não mascarados.

42. Possibilitar, em caso de indisponibilidade da solução, ordenar o chaveamento para uma réplica pré-configurada de todos os ambientes de dados suportados pela ferramenta.

43. Criar agrupamento lógico de objetos de dados distintos (exemplo: aplicações, bancos de dados e diretórios de arquivos não-estruturados) para apresentação consistente de cópias completas dos dados, no mesmo ponto no tempo, respeitando as regras de proteção de dados estabelecidas.

44. Permitir a execução de rotinas periódicas de cópia, refresh, rewind, mascaramento, entre outras, a nível de objeto ou de grupos de objetos, por meio de agendamentos internos ou externos.

45. Permitir integração aos principais provedores de nuvens públicas e privadas.

46. Permitir replicar os dados de maneira segura e completa ou incremental, entre ambientes geograficamente distantes.

47. Permitir uma replicação seletiva, sendo possível criar uma segregação entre ambientes produtivos e de desenvolvimento, homologação ou testes, para garantir que dados sensíveis não sejam transmitidos para fora de ambientes controlados.

48. Permitir gerar relatórios em tempo real para auditoria e verificação de conformidade dos dados, possuindo perfil específico para gerenciamento por equipes de compliance e auditoria.

49. Possuir funcionalidades de backup e restore completas, com point-in-time recovery, para minimizar janelas de recuperação.

50. Deve manter cópias de dados por diferentes períodos de retenção para backups de banco de dados, bem como o conteúdo do sistema de arquivos.

51. Deve ser capaz de criar automaticamente backups ou pontos de restauração (snapshots) das cópias de dados gerenciadas pela solução.

52. Fornecer acesso por interface de linha de comando, bem como API RESTful, para integração com outros programas utilizados pelo Ministério, como orquestrador de Integração e Entregas Contínuas (CI/CD), automação (DevOps) ou Gerenciadores de Chamados.

53. Expor interfaces para permitir automatizar ou customizar processos, por meio da criação e execução de scripts personalizados antes e ou após determinada ação, como por exemplo após o refresh dos dados ou antes do provisionamento dos dados. Tais scripts devem suportar linguagens comuns de mercado, como Shell Script ou SQL.

54. Possuir interface *Web*, sem necessidade de distribuição e instalação de programa cliente nos computadores dos usuários finais e independente das tecnologias *Java* ou *Flash*, por questão de compatibilidade com browsers modernos.

55. Fornecer interface específica para consumidores finais dos dados (desenvolvedores, analistas de testes, analistas de dados, parceiros, entre outros) gerirem o ciclo de vida de ambientes de dados, sem a necessidade de conhecimento específico da plataforma de dados em uso.

56. Permitir que as fotografias (*snapshots*) do banco de dados sejam feitas pelo consumidor final, sob demanda, de maneira recorrente ou automática, sem necessidade de intervenção ou auxílio de um administrador de bancos de dados.

57. Garantir o uso simultâneo da solução por múltiplos operadores, com controle de perfis e permissões.

58. Exibir estatísticas de uso operacional, limites de capacidade de armazenamento, gráficos de performance e rastreabilidade de operações executadas.

59. Ser capaz de se integrar com qualquer tecnologia de armazenamento (*storage*) já utilizada pela contratante.

60. Suportar modelo de virtualização em *Data Centers* próprios, Nuvens ou modelos híbridos, sem a necessidade de acessos remotos ou componentes externos à rede interna da contratante, salvo em necessidade de suporte técnico remoto, atualizações, ou validação de licenciamento.

61. Ser compatível com no mínimo as seguintes versões de bancos de dados:

- IBM DB2 v. 11 ou posterior
- Firebird v. 3.0 ou posterior
- MySQL v. 5.1.52 ou posterior
- Oracle v. 12 ou posterior
- PostgreSQL v. 8.1 ou posterior
- Teratadata v. 16.20 ou posterior

62. Suportar nativamente a integração com sistema de autenticação LDAP.

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

Demais requisitos necessários e suficientes à escolha da solução de TIC

Metodologia de Trabalho

Todos os serviços deverão ser executados em conformidade com as normas, políticas, metodologias, guias e padrões estabelecidos no âmbito do Ministério da Cidadania.

Legislação

Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências (ainda vigente por dois anos a partir de 01/04/2021).

Lei Federal nº 10.520/2002: Institui no âmbito da União, Estados, Distrito Federal e Municípios, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

Lei Federal nº 14.133/2021: Lei de Licitações e Contratos Administrativos (entrou em vigor em 01/04/2021, e revoga as Lei nº 8.666/1993 10.520/2002 após decorridos 2 (dois) anos da sua publicação).

Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

Decreto nº 7.845/2012: Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Decreto nº 10.024/2019: Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal.

Decreto nº 9.637/2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

Instrução Normativa MPDG nº 05/2017: Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

Instrução Normativa SGD/ME nº 01/2019: 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 e Tecnologia da Informação (SISP) do Poder Executivo Federal.

Segurança da Informação

Deverão ser observadas as normas e diretrizes contidas na Política de Segurança da Informação e Comunicações do Ministério da Cidadania, e suas normas complementares.

Deverão ser observadas as leis, normas e diretrizes de Governo relacionadas à Segurança da Informação (SI), em especial atenção ao Decreto Federal nº 9.637/2018 e à legislação do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSI/GSI/PR)

Ambientais, Sociais e Culturais

A CONTRATADA, no que couber, deverá atender os critérios de sustentabilidade ambiental previstos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Governo Digital, do Ministério da Economia (SGD/ME), e do Decreto nº 7.746, de 05 de junho de 2012.

Os serviços prestados pela CONTRATADA, no que couber, deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo Governo.

7. Estimativa da demanda - quantidade de bens e serviços

Durante a realização dos estudos técnicos preliminares, foi solicitado à Coordenação-Geral de Gestão da Informação (CGGDI), em conjunto com a Coordenação-Geral de Infraestrutura (CGINF), um levantamento do volume de dados de produção mantidos pela STI. Apesar do fato de que existem conjuntos de dados contendo informações pessoais sensíveis mesmo em ambientes não produtivos, um dos objetivos da presente contratação é justamente utilizar a solução contratada para identificar dados sensíveis que possam ser migrados para os demais ambientes de forma anonimizada.

As informações foram extraídas a partir dos principais sistemas gerenciadores de banco de dados do Ministério da Cidadania em atividade, bem como de sistemas de arquivos. Com base neste levantamento e análise das aplicações que tratam dados pessoai, a equipe de planejamento da contratação identificou um volume considerável de bases de dados que devem fazer parte do escopo de uso da ferramenta de mascaramento.

Haja vista este processo de contratação ser público e, devido a isso, haver um risco de exposição indevida de detalhamento técnico do nome das bases de dados, modelo do banco de dados e suas versões, a equipe de planejamento da contratação consolidou um arquivo à parte com os dados detalhados do levantamento e anáise das aplicações e suas bases. Esse arquivo que foi armazenado no processo 71000.067625/2021-32 na estrutura do SEI do MC.

Com base nessa análise, estima-se a necessidade de uso de 16 TB de licenciamento, de modo a atender demandas de bases em ambiente de desenvolvimento/homologação, ambiente de produção, ambiente de análise de dados (ETL e afins) e em arquivos de dados não estruturados.

Além do licenciamento, há necessidade de contratação de serviços técnicos para instalação, configuração, parametrização da ferramenta e implementação de projetos com uso de virtualização e mascaramento. Para execução dos serviços especializados, há necessidade de perfis técnicos para essas atividades listadas e de perfil consultivo para análise de sistemas, bases, atividades, arquivos e documentos que devem ser avaliados quanto à necessidade de tratamento de riscos de não atendimento à LGPD.

Conforme preconiza a Instrução Normativa - SGD nº 1 de 4 de abril de 2019, art. 11 II, a Equipe de Planejamento da Contratação - EPC analisou contratações semelhantes para atender à demandas da LGPD. Mais adiante serão trazidas mais informações, como a análise de valores. Neste movimento, foi observado que a contratação realizada pelo Ministério do Meio Ambiente dimensionou 3 perfis por mês, totalizando 36 perfis por ano, com uso sob demanda para realização de dos serviços citados acima. A partir dessa análise foi estimada a utilização de 4 (quatro) perfis profissionais por mês, totalizando 48 por ano, haja vista o volume do escopo dimensionado para a presente contratação ser maior.

Das características dos serviços a serem executados, é necessário que haja um perfil para a execução de competências técnicas do processo de controle de dados dinâmicos, dos serviços de mascaramento de dados, da criação de scripts customizados visando a integração de soluções por meio de API específica da solução, e outro perfil voltado ao levantamento e análise de bases de dados, sistemas, processos, contratos e outros para implementação das diretrizes da LGPD no âmbito do Ministério da Cidadania.

8. Levantamento de soluções

As necessidades elencadas acima dependem da utilização de ferramentas de software específicas para serem plenamente satisfeitas, não sendo possível somente a utilização de mão de obra especializada. Mesmo se considerarmos a utilização dos serviços terceirizados existentes para construção de tais ferramentas, o fato é que as características dessas ferramentas são típicas

de softwares de prateleira, o que as torna inadequadas para o desenvolvimento por meio das contratações vigentes na casa, voltadas para o desenvolvimento de softwares negociais sob demanda.

Em atendimento ao inciso II do art. 11 da IN SGD/ME nº 1/2019, em 15/08/2021 foi procedida pesquisa no catálogo[1] do Portal do Software Público Brasileiro. No entanto, não foram identificadas soluções que atendam a presente demanda. Também não foram encontradas soluções similares disponíveis em órgãos ou entidades da Administração Pública, ou seja, soluções que pudessem ser aproveitadas por meio de cessão ou transferência de tecnologias. Por fim, em pesquisas preliminares não foi possível identificar um software livre mantido por uma comunidade ativa que atenda a presente necessidade e que pudesse ser utilizado de forma isolada ou combinada com as tecnologias atualmente em uso no Ministério da Cidadania.

Ainda, também não foram encontradas Atas de Registro de Preços (ARP) vigentes, ou certames em andamento em fase de Intenção de Registro de Preços (IRP), que possuíssem alguma similaridade com os serviços em avaliação. Também é importante registrar que, em aderência à IN nº 1/2019 SGD/ME, com redação dada pela IN nº 202/2019 SGD/ME, não verificada a existência de Catálogo de Soluções de TIC com Condições Padronizadas referente aos serviços em tela.

Em suma, devido a impossibilidade de desenvolver uma solução própria e em face da ausência de soluções similares disponíveis em órgãos ou entidades da Administração Pública, não é possível considerar cenários em que seja utilizado a força de trabalho interna do Ministério da Cidadania para configurar uma nova solução ou solução preexistente, sendo necessária a aquisição de ferramentas específicas para atendimento da presente necessidade.

Deste modo, uma vez estabelecida a necessidade de utilização de ferramentas e soluções de TIC para atendimento da presente demanda, a única solução a ser vislumbrada é a aquisição de uma solução de software de prateleira e de serviços subjacentes. Assim, será realizada uma comparação dos modelos de contratação que considerem o licenciamento por subscrição ou perpétuo, a fim de tentar selecionar o cenário mais vantajoso frente à realidade do Ministério da Cidadania.

Com base nos cenários considerados acima, segue abaixo a composição das soluções que serão avaliadas quanto ao atendimento da presente necessidade.

Identificação das Soluções

ID	Descrição da solução (ou cenário)
1	Aquisição de ferramenta no modelo de subscrição de software
2	Aquisição de ferramenta no modelo de licenciamento perpétuo de software

9. Análise comparativa de soluções

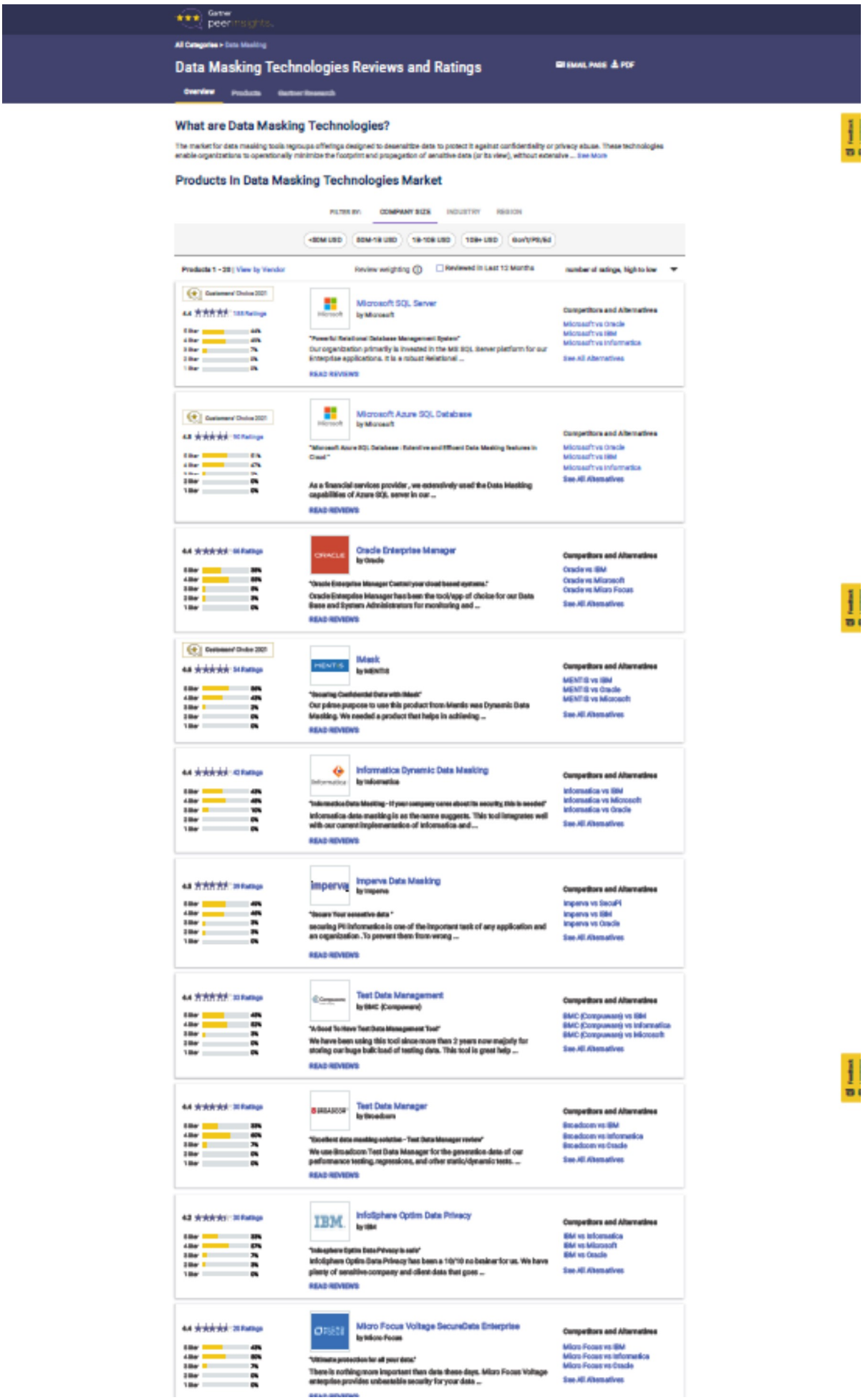
Análise Comparativa de Soluções

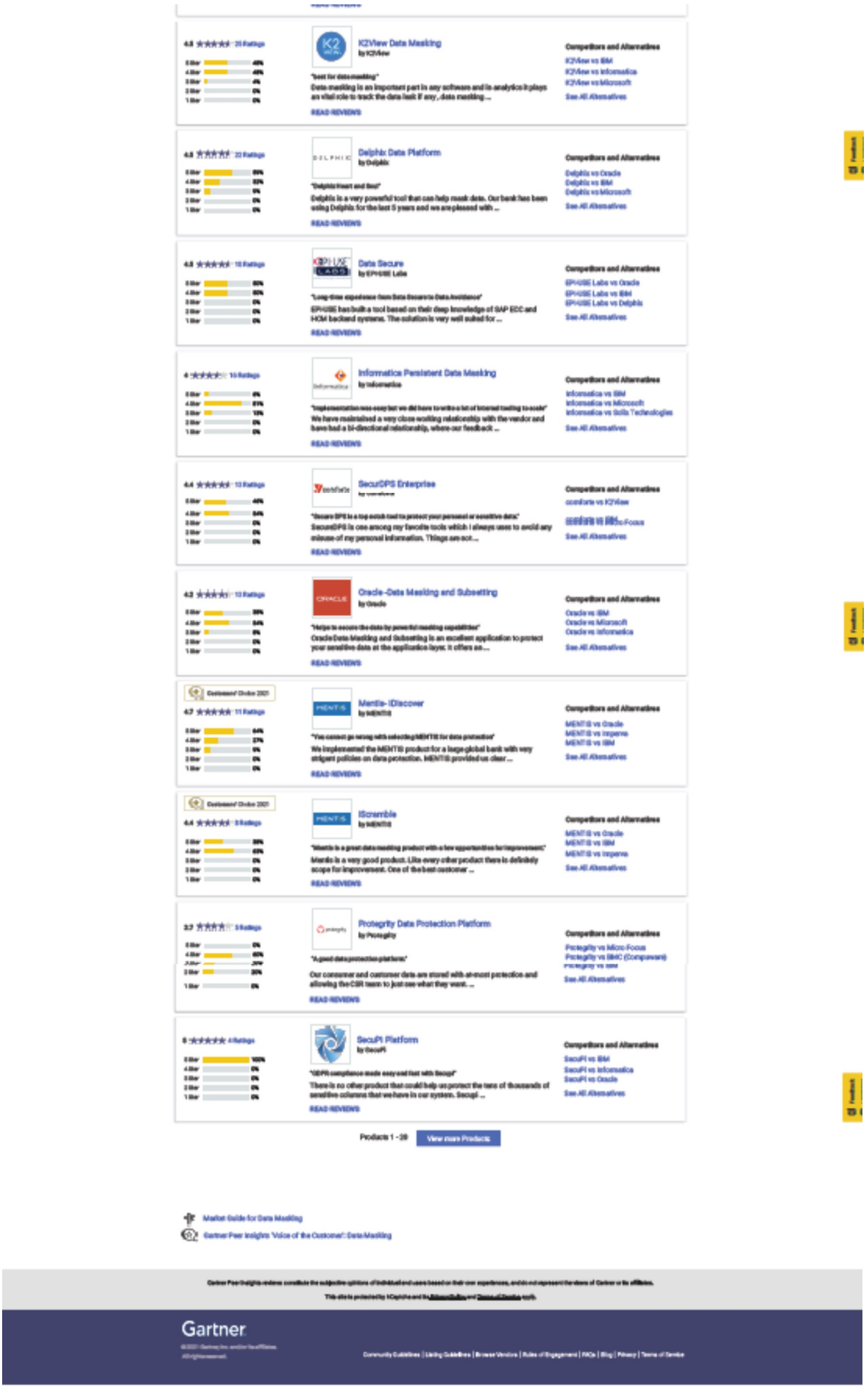
O quadro seguinte consta a comparação de alguns requisitos entre as Soluções identificadas acima:

Requisito	Solução	Sim	Não	Não se a
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1		X[2]	
	Solução 2		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	

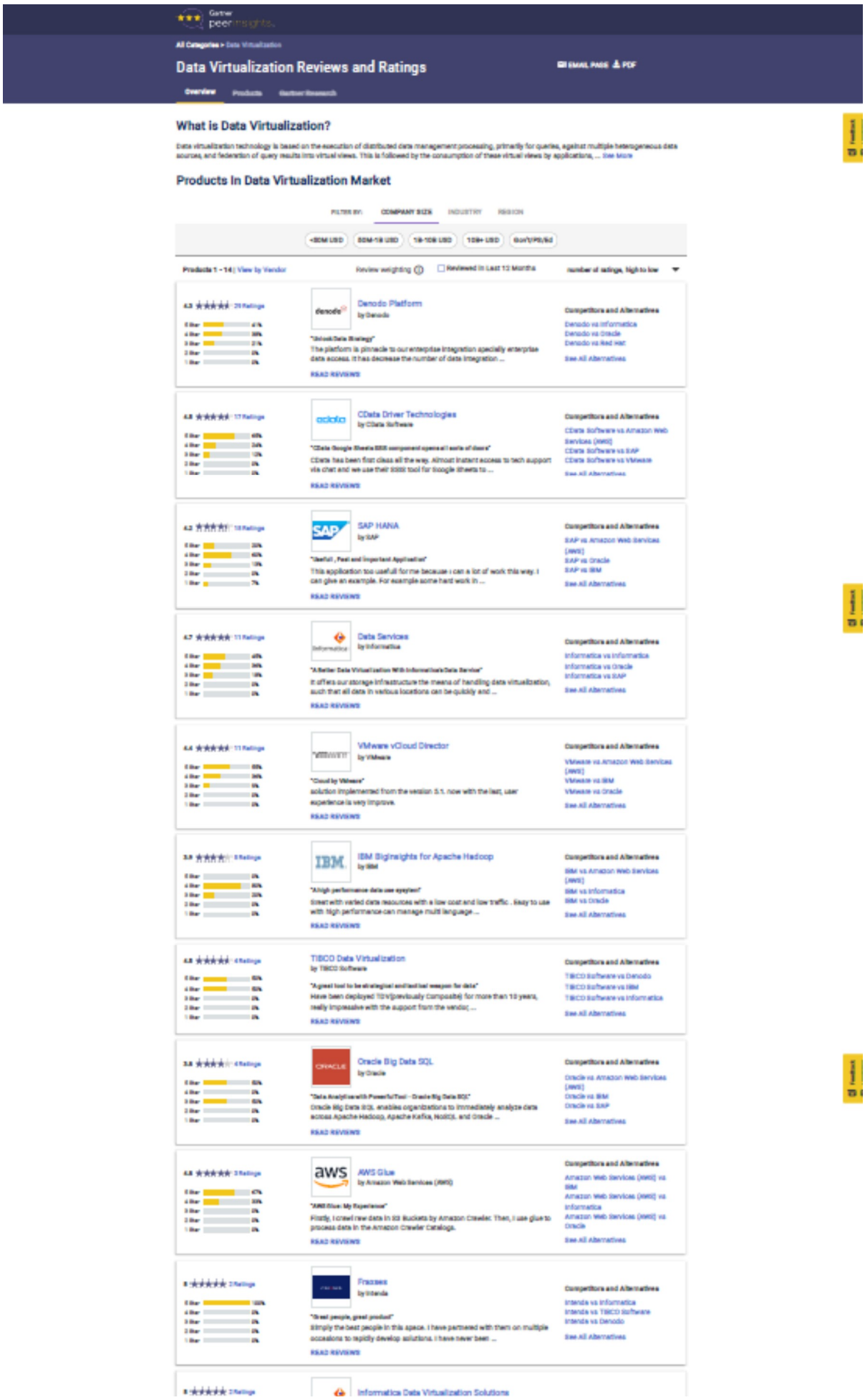
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

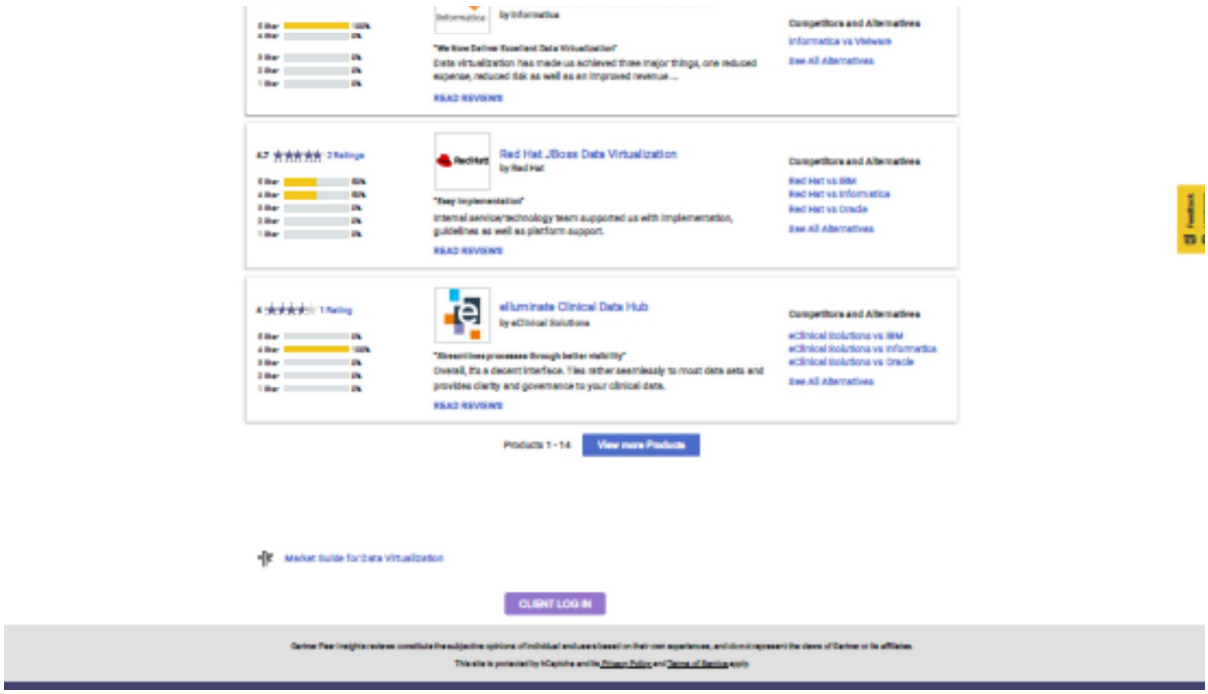
Em pesquisa preliminar no portal Gartner Peer Insights[3], foi possível encontrar uma variada gama de soluções referentes aos casos de uso Data Masking[4] e Data Virtualization[5], sendo possível constatar, inclusive, a existência de fabricantes e soluções que atendem a ambos os casos de uso. Foi verificado que existem soluções de mercado que atendem tanto ao caso de uso de mascaramento de dados quanto ao de disponibilização de cópias virtuais de dados.


Gartner peerinsights.
All Categories > Data Masking
Data Masking Technologies Reviews and Ratings
EMAIL PAGE PDF
Overview
Products
What are Data Masking Technologies?
Products In Data Masking Technologies Market
Microsoft SQL Server
Microsoft Azure SQL Database
Oracle Enterprise Manager
Mask
Informatica Dynamic Data Masking
Imperva Data Masking
Test Data Management
Test Data Manager
InfoSphere Optim Data Privacy
Micro Focus Voltage SecureData Enterprise


K2View Data Masking
by K2View
Competitors and Alternatives
K2View vs IBM
K2View vs Informatica
K2View vs Microsoft
See All Alternatives
READ REVIEWS
Delphix Data Platform
by Delphix
Competitors and Alternatives
Delphix vs Oracle
Delphix vs IBM
Delphix vs Microsoft
See All Alternatives
READ REVIEWS
Data Secure
by EPI-USE Labs
Competitors and Alternatives
EPI-USE Labs vs Oracle
EPI-USE Labs vs IBM
EPI-USE Labs vs Delphix
See All Alternatives
READ REVIEWS
Informatica Persistent Data Masking
by Informatica
Competitors and Alternatives
Informatica vs IBM
Informatica vs Microsoft
Informatica vs Delta Technologies
See All Alternatives
READ REVIEWS
SecurDPS Enterprise
Competitors and Alternatives
See All Alternatives
READ REVIEWS
Oracle Data Masking and Subsetting
by Oracle
Competitors and Alternatives
Oracle vs IBM
Oracle vs Microsoft
Oracle vs Informatica
See All Alternatives
READ REVIEWS
Mentis- iDiscover
by MENTIS
Competitors and Alternatives
MENTIS vs Oracle
MENTIS vs Imperva
MENTIS vs IBM
See All Alternatives
READ REVIEWS
iScramble
by MENTIS
Competitors and Alternatives
MENTIS vs Oracle
MENTIS vs IBM
MENTIS vs Imperva
See All Alternatives
READ REVIEWS
Protegrity Data Protection Platform
by Protegrity
Competitors and Alternatives
Protegrity vs Micro Focus
Protegrity vs IBM (Compuware)
See All Alternatives
READ REVIEWS
SecuPI Platform
by SecuPI
Competitors and Alternatives
SecuPI vs IBM
SecuPI vs Informatica
SecuPI vs Oracle
See All Alternatives
READ REVIEWS
Products 1 - 20
View more Products
Market Guide for Data Masking
Gartner Peer Insights 'Voice of the Customer': Data Masking
Gartner
Community Guidelines | Using Guidelines | Browse Vendors | Rules of Engagement | FAQs | Blog | Privacy | Terms of Service

[4] Data Masking


Gartner peerinsights
Data Virtualization Reviews and Ratings
What is Data Virtualization?
Products In Data Virtualization Market
Denodo Platform
CData Driver Technologies
SAP HANA
Data Services
VMware vCloud Director
IBM Biginsights for Apache Hadoop
TIBCO Data Virtualization
Oracle Big Data SQL
AWS Glue
Frazees
Informatica Data Virtualization Solutions



[5] Data Virtualization

No documento “Market Guide for Data Masking” (Anexo SEI 11175088), 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 (mascaramento e virtualização).

Deste modo, verificamos que existem soluções de mercado aptas a atender as necessidades propostas. Verificou-se que alguns fabricantes, como a Imperva, oferecem ambos os modelos de contratação[6] (licenciamento perpétuo e por subscrição) (Anexo SEI 11175168). Já alguns fabricantes, como a Informatica LLC, têm realizado uma contínua transição de vendas de software perpétuo para software por subscrição[7]. Além disso, fabricantes como a Delphix aparentemente só fornecem o modelo por subscrição[8].

Temos que o licenciamento perpétuo possui a vantagem de permitir a continuidade do uso da solução mesmo após a vigência contratual, porém, em contrapartida, costuma demandar um maior investimento inicial. Um fator determinante a ser observado neste tipo de licenciamento é que os fabricantes costumam lançar novas versões do software e, em geral, param de entregar *patches* de segurança para as versões anteriores. Neste cenário, com o passar do tempo, o cliente é praticamente impelido a adquirir a nova versão, tanto pela segurança da utilização quanto pelos novos recursos disponíveis,do contrário, o produto torna-se obsoleto.

Já o licenciamento por subscrição, em geral, exige um investimento inicial menor e permite que o cliente pague apenas pelo que usar, tendo o software sempre atualizado. Em contrapartida, o uso da solução é encerrado com o fim da vigência contratual. Um fator determinante a ser observado é se a vantajosidade financeira se mantém em relação ao licenciamento perpétuo, e se será criada uma dependência do uso da solução para execução dos serviços após o fim da vigência. Um exemplo clássico desse tipo de dependência é a utilização de formatos proprietários de arquivos que dependem unicamente do software para serem acessados.

Obviamente, a vantajosidade entre ambos os modelos dependeria de uma análise de compras já realizadas no âmbito da Administração Pública. Entretanto, em pesquisas realizadas, não foi possível identificar nenhuma compra pública que tivesse utilizado o licenciamento perpétuo, o que pode ser um indício de que o mercado brasileiro especializado neste tipo de solução não adota esta forma de comercialização, ou que tal modelo de comercialização não se mostrou vantajoso para nenhum órgão público até o momento.

Verificamos que existe uma aparente tendência, para alguns tipos de tecnologias, de ser adotado o modelo de subscrição. Em contratações de licenças Microsoft, por exemplo, foram consultados estudos preliminares de outros órgãos, como o Ministério da Educação (MEC), Agência Nacional de Energia Elétrica (ANEEL) e o Tribunal de Justiça de Mato Grosso (TJMT) que concluíram pela contratação de licenciamento Microsoft pelo modelo de subscrição, frente ao modelo de licenciamento perpétuo.

Assim, a presente análise conclui pela utilização do modelo de licenciamento por subscrição para o projeto em questão, por ser o único modelo utilizado até o momento.

---

[1] https://softwarepublico.gov.br/social/search/software_infos

[2] Existem softwares de mascaramento ou de provisionamento de cópias virtuais de dados contratadas por outros órgãos públicos, mas que não são passíveis de utilização por questões relativas ao direito de uso das licenças/subscrições.

[3] https://www.gartner.com/reviews/home

[4] https://www.gartner.com/reviews/market/data-masking

[5] https://www.gartner.com/reviews/market/data-virtualization

[6] https://docs.imperva.com/bundle/v14.5-dam-administration-guide/page/6717.htm

[7] https://finance.yahoo.com/news/informatica-llc-moodys-announces-completion-154310362.html

[8] https://community.delphix.com/communities/communityhome/digestviewer/viewthread?MID=5519

10. Registro de soluções consideradas inviáveis

Por meio da análise realizada, verificou-se que a utilização da força de trabalho ou das ferramentas existentes no Ministério da Cidadania não seria viável para atendimento da presente necessidade. Com base na análise das atividades dos servidores alocados na Subsecretaria de Tecnologia da Informação - STI e no perfil das atividades descritas no Decreto-Lei nº 200, de 1967, Art. 10 § 7º, conclui-se que os serviços a serem executados devem fazer parte da contratação para que os servidores possam definir as ações estratégicas da utilização da ferramenta. Conforme § 1º do art. 11 da IN 1/2019, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

11. Análise comparativa de custos (TCO)

ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Cálculo dos Custos Totais de Propriedade

SOLUÇÃO VIÁVEL
Descrição
Contratação de licença/subscrição de um novo software, e de serviços subjacentes.
Custo Total de Propriedade – Memória de Cálculo
Com base na Pesquisa de Preços contida no “Anexo B” deste documento, realizada por meio de cotação com fornecedores de mercado, em consonância com o artigo 5º da IN nº 73/2020 SEGES/ME, o valor anual estimado da presente solução foi de R$ 13.632.071,04.

Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

Descrição da Solução	Estimativa de TCO ao longo dos anos		
	2021	2022	2023
Aquisição de ferramenta no modelo de subscrição de software	R$ 13.632.071,04	R$ 13.632.071,04	R$ 13.632.

12. Descrição da solução de TIC a ser contratada

A solução de TIC para atendimento das necessidades levantadas consiste na subscrição de software de identificação e mascaramento de dados sensíveis, em conformidade com as diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD), e de entrega de cópias de dados de forma rápida, econômica e segura para simplificar o processo de disponibilização de dados bem como para impulsionar o desenvolvimento de aplicativos de forma eficiente e de alta qualidade. Além disso, contempla a prestação de serviços especializados de instalação, consultoria, treinamento e apoio na utilização da solução.

Os serviços deverão ser prestados sob demanda, sem dedicação exclusiva de mão de obra, por meio de profissionais devidamente capacitados para tal. No início da execução do contrato, serão necessários os serviços de instalação, configuração e parametrização da ferramenta, e a preparação das bases de dados para que a solução esteja pronta para o mascaramento e o controle de dados por virtualização.

Após a configuração inicial da ferramenta e preparação das bases, há necessidade de serviço técnico continuado que operacionalize as atividades de entrega de projetos que demandem a virtualização, controle e/ou mascaramento dos dados. Esses serviços serão demandados mensalmente de acordo com a necessidade de projetos a serem entregues às áreas de negócio e sisitemas do Ministério. Para isso, a alocação será dinâmica de acordo com essa necessidade, possibilitando o dimensionamento da equipe da contratada com um ou mais perfis por mês, vinculado à entrega de produtos e regulado pela aplicação de níveis mínimos de serviço.

Abaixo segue a divisão em itens dos bens e serviços que compõem a solução:

Item	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade
1	Subscrição de software de mascaramento de dados	16	*Terabyte* (TB)
2	Subscrição de software de controle de dados dinâmicos	16	*Terabyte* (TB)
3	Serviços especializados de consultoria e apoio na utilização da solução	48	Perfil/Mês

Foi possível constatar que o fornecimento de soluções similares é realizado por volume de armazenamento. Considerando que esta unidade de medida é universal, e que sempre é possível medir com precisão o volume dos dados armazenados, foi mantido o modelo de fornecimento por “Terabytes”, a fim de maximizar a possibilidade de comparação de preços.

Modelo de remuneração

Quanto aos serviços técnicos especializados, foi adotado o modelo de remuneração em perfil por mês, vinculado à entrega de produtos. Em síntese, o modelo prevê que a CONTRATADA proverá equipe para prestação de serviços técnicos de instalação,

configuração, consultoria e apoio na utilização da solução somente após emissão de ordem de serviço, e será remunerada após a conclusão dos serviços e entrega dos produtos, uma vez demonstrado a entrega dos produtos e serviços. Cada ordem de serviço será acompanhada do respectivo Plano de Trabalho, pactuado entre as partes antes do início da execução dos serviços, contendo a lista de produtos e serviços a serem entregues, a estimativa de trabalho atribuído a cada produto ou serviço, bem como o prazo de entrega a ser observado. A cada entrega, o CONTRATANTE irá monitorar a execução dos serviços com base no Plano de Trabalho pactuado, com base nos níveis mínimos de serviço de qualidade e produtividade previstos neste documento.

Parcelamento da solução

Decide-se pela contratação em lote único, conforme previsto na legislação porque, conforme citado anteriormente, ao gerar uma cópia virtual de dados mascarados, é imprescindível que se o processo de mascaramento falhar, a disponibilização da cópia de dados também deverá falhar, tornando impossível a apresentação de clones parcialmente mascarados. Nos cenários que contemplam a contratação separada da solução de disponibilização, acesso e controle de cópias virtuais de dados e a solução de mascaramento de dados, não é possível garantir a integração mínima de ambas as soluções a fim de que este requisito seja atendido.

A impossibilidade de realização do mascaramento concomitantemente ao processo de virtualização poderia significar uma falha de segurança, uma vez que demandaria a criação de cópias virtualizadas com informações reais, passíveis de serem acessadas antes do processo de mascaramento. Tais razões implicam na necessidade de perfeita integração entre ambas as soluções, não sendo tecnicamente viável, para fins do presente projeto, a separação desses itens em lotes distintos.

Outra questão relevante para decisão referente ao parcelamento da presente solução é que, conforme verificado nos estudos técnicos preliminares, é possível encontrar soluções de mercado que atendem plenamente aos itens da forma como está sendo proposto acima. Foi constatado na pesquisa 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. Foi constatado ainda 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.

13. Estimativa de custo total da contratação

Valor (R$): 13.632.071,04

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Registro da estimativa do custo da contratação, considerando a Solução escolhida:

Item	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade	Valor Anual (Estimado)	Valor Anual (Estimado)
1	Subscrição de software de mascaramento de dados	16	*Terabyte* (TB)	R$ 436.221,72	R$ 6.979.547,52
2	Subscrição de software de controle de dados dinâmicos	16	*Terabyte* (TB)	R$ 350.034,24	R$ 5.600.547,84
3	Serviços especializados de consultoria e apoio na utilização da solução	48	Perfil/Mês	R$ 21.916,16	R$ 1.051.975,68
TOTAL					**R$ 13.632.071,04**

14. Justificativa técnica da escolha da solução

.

15. Justificativa econômica da escolha da solução

...

16. Benefícios a serem alcançados com a contratação

...

17. Providências a serem Adotadas

Não há providencias a serem adotadas

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Viável

19. Responsáveis

JULIANA ROCHA MUNITA MOREIRA
Analista de Tecnologia da Informação – ATI

FELIPE VELTER TELES
Integrante Técnico